新天创作联盟 曲鼎 王岗 编著

PC 实用之道

病毒与黑客攻防

洞悉黑客攻防之道
深析网络安全技术
玩转主流杀毒软件
打造安枕无忧系统

修补Windows下可能出现的各种漏洞，曝光最新的黑客攻防技巧
掌握各种防黑防毒软件的操作，确保数据与信息的安全
打造更加稳定可靠的电脑系统环境

清华大学出版社

新天创作联盟 曲鼎 王岗 编著

PC实用之道

病毒与黑客攻防

洞悉黑客攻防之道
深析网络安全技术
玩转主流杀毒软件
打造安枕无忧系统

修补Windows下可能出现的各种漏洞，曝光最新的黑客攻防技巧
掌握各种防黑防毒软件的操作，确保数据与信息的安全
打造更加稳定可靠的电脑系统环境

清华大学出版社
北京

内 容 简 介

本书内容丰富，简明通俗，实用性强。全书共分为12章，详细讲解了黑客攻防技术学习平台的搭建、计算机攻防的基础知识与必备常用命令，从计算机漏洞、计算机密码、聊天软件以及对木马攻防的常用的攻击手法进行演示揭密，并指出相应的防范措施。本书还对时下流行的跨站注入、SQL注入、代码攻防进行了实例讲解，让读者可以快速学习网站攻防技术。在网络病毒横行的时代，本书特别针对病毒的基础知识与初级分析、各类病毒的攻击与防范进行了讲解，最后对数据的备份与恢复，以及病毒与系统安全防护进行了详细的实例讲解。

本书通过在虚拟实验环境中进行技能训练的方式，带领读者系统、全面地完成计算机黑客与病毒等神秘内容的学习和演练。本书适合于对网络安全及黑客攻防感兴趣的读者，特别适用于普通大众读者，增强网民的安全防范意识，减少计算机与网络的安全隐患。

图书在版编目（CIP）数据

PC实用之道——病毒与黑客攻防/新天创作联盟，曲鼎，王岗编著. —北京：清华大学出版社，2006.9
ISBN 7-302-13247-X

Ⅰ. P…　Ⅱ. ①新…②曲…③王…　Ⅲ. 电子计算机-安全技术　Ⅳ. TP309

中国版本图书馆CIP数据核字（2006）第068107号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
组稿编辑：田在儒
文稿编辑：林都嘉
印 刷 者：北京市清华园胶印厂
装 订 者：三河市新茂装订有限公司
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：22.5　**字数**：557千字
版　　次：2006年9月第1版　2006年9月第1次印刷
书　　号：ISBN 7-302-13247-X/TP·8371
印　　数：1～4000
定　　价：35.00元

前　言

在 Internet 高速发展的今天，网络作为一种重要的信息传递手段，对经济的发展和人们之间的交流起着越来越重要的作用。近几年，我国的网络建设突飞猛进，中国互联网用户已经跃居世界第二，成为世界网络大国。网络已经进入我们的日常生活，它与我们的工作、学习、生活息息相关。在网络建设蓬勃发展的同时，网络安全问题也到了令人堪忧的地步。

我们常常考虑，到底是什么阻碍了 Internet 在社会生活和经济中的广泛应用，是什么原因使我们仍然不敢也不愿意通过 Internet 进行交易，以及为什么在为企业架设网络时总是要问一个类似的问题：这个和 Internet 连接的计算机网络会不会被黑客利用。是的，随着网络技术的发展，黑客的攻击手法已经超过计算机病毒的种类，总数达近千种，计算机与网络最大的威胁就是“安全”。在网络上的大多数人都或多或少地知道计算机安全的概念，哪怕是没有接触过计算机的人也能够通过电视、报纸等媒体知道诸如黑客、病毒，木马之类的名词。虽然其中大多数人的计算机可能不曾感染过病毒，也可能他们的计算机资料没有被窃取过，但是所有利用互联网进行工作、生活和学习的人都会担忧网络的安全问题。

为了解决读者对黑客攻击与防范、病毒以及网络安全整体防范的强烈需求，为了提高广大网络爱好者的安全防范意识，排除计算机与网络的安全隐患，我们特此推出此书，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进行相应的防范，为大家打造一个安全放心的网络环境。

本书由新天创作联盟、曲鼎、王岗、王洁、黄艳共同创作，感谢胡鹏先生在本书的策划和创作过程中给予的宝贵意见和大力帮助，由于他的不懈努力和一丝不苟的敬业精神，使得本书在质量上有了质的飞跃。

从本书中可以学到什么？

- 黑客攻防技术学习平台的搭建
- 计算机攻防的基础知识与必备常用命令
- 计算机漏洞、计算机密码、聊天软件、计算机木马的攻防实战技术
- 跨站注入、SQL 注入攻防与代码安全
- 病毒基础知识与初级分析技术
- 各类病毒（冲击波、QQ 病毒、邮件病毒、VBS 病毒）的攻防
- 数据备份与恢复
- 病毒与系统安全防护

目　录

第 1 章　构建黑客测试平台

黑客攻防技术中，每一种技术都只能针对存在该种对应漏洞的主机才能有效实施，也就是说，没有万能的入侵与防范技术，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，以及平台所需的虚拟硬件、虚拟系统、虚拟工具，最后为大家介绍 ASP、PHP、JSP 环境平台的打造与典型配置等内容。

本章所学到的内容：

- 如何打造黑客攻防测试平台
- 攻防测试平台的建立与安装
- 虚拟网络环境的配置
- ASP、PHP、JSP 平台的搭建

“万丈高楼平地起”，这句话说明了基础平台的重要性，同样，它也适用于黑客攻防技术。作为安全技术的前沿，黑客攻防技术十分强调实践性和灵活性，实践性即操作的条理性，按照既定的某些步骤，就可以达到意想不到的效果；灵活性就不同了，按照既定的步骤，如果更换一个操作系统，测试的结果可能就完全不一样了。这也是喜爱攻防的人们常常感到困惑的一个问题。可见，安全测试环境千变万化，如果不能把握平台特点，在安全实践中就会寸步难行。因此，黑客测试平台是整个安全工作中的一个重要组成部分。

1.1 打造第一个黑客测试平台

万事开头难，做一个技术精湛的黑客也是如此。黑客需要经常进行各类测试，如系统的漏洞测试、网络的远程连接测试、最新黑客软件的功能测试等。很明显，这些测试都需要复杂的网络环境，完全依靠单机网络环境是不可能实现的。因此，必须利用有限的资源，打造一个完全属于自己的测试平台。

1.1.1 为什么需要黑客测试平台

在学习安全技术的过程中，经常会出现这样的现象：很多安全爱好者都喜欢关注最新的安全漏洞和最新的安全文摘，但遗憾的是面对一些高手所公布的漏洞他们却往往一筹莫展。

例如：打开绿盟科技平台的“安全公告”或“安全漏洞”页面，就经常可以看到各种不同操作系统的漏洞消息，但是如果要实际操作的话，会存在很大的难度。

仔细分析，出现这样困惑的根源在于：没有一个完整的平台来完成这些安全漏洞的编译和测试。因为这些最新的安全漏洞囊括了各种各样的平台，随便打开一个最新的漏洞描述页面，再打开中间的“所有系统”下拉菜单即可看到（图 1－1）。

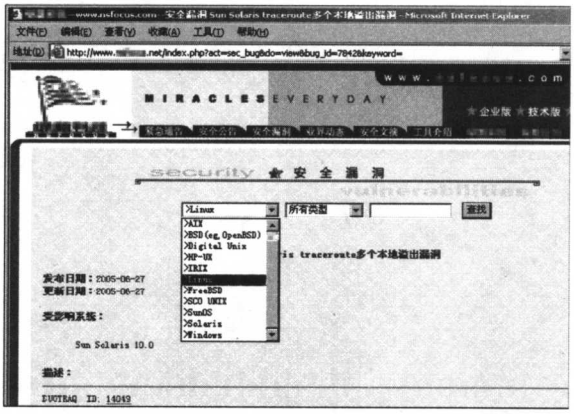

图 1－1 各种各样的漏洞操作平台

面对图 1－1 中种类繁多的测试环境，如果仅限于当前的 Windows 系统，就显得有些捉襟见肘了。难道要自己准备 10 多台机器来完成这些任务吗？如果我们玩腻了 Windows 操作系统，想学习一下 Linux，却害怕 Linux 的重新分区，怎么办？如果已经安装了多个操作系统，可是需要切换操作系统的时候难道只能重新启动吗？

其实，只要使用 VMware 公司出品的 VMware 虚拟机，一切问题都可以迎刃而解。说得通

俗一些，VMware 虚拟机是一款软件，可以模拟出无数个计算机操作系统。与“多启动”系统相比，VMware 不需要重新开机就能在同一台计算机中使用多个操作系统。它可以将计算机上的一部分硬盘和内存进行组合，虚拟出若干台机器，每台机器拥有自己独立的 CMOS（互补金属氧化物半导体）、硬盘和操作系统，可以像使用普通机器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。

所谓虚拟机，就是在一台真实计算机上虚拟出一台计算机，同时运行两个或更多的操作系统。它以原有的操作系统为基础，使用额外的硬盘空间创建一个虚拟的计算机。“虚拟机”只是一个程序，由于一切操作都是虚拟进行的，因此可以在虚拟机上尝试一些危险的操作，当然这一切都是安全的。

本章将结合最新版本的 VMware 5.0，为安全技术爱好者打造一个完美的测试平台。VMware 虚拟机的下载地址为 http://www.vmware.cn。

1.1.2 虚拟硬件基础知识

在虚拟平台的测试过程中，VMware 需要一个操作系统作为最基本的平台，即 HOST OS（主操作系统），在 HOST OS 上运行的其他系统都叫 GUEST OS（子操作系统或客户操作系统）。除此之外，还需要一些基本的虚拟硬件，下面简单介绍几个最常见的虚拟硬件设备。

- 网卡。虚拟网卡用于 HOST OS 和 GUEST OS 之间的通信，它可以建立标准的 TCP/IP 或 NETBEUI（网络基本输入输出系统增强型用户接口）桥梁。在虚拟机中，网卡品牌很大众化，Windows 系统和 Linux 系统都能自动识别并驱动。
- 显卡。VMware 将显卡模拟为一种叫 VMware SVGA（FIFO）的型号，并自带了这种显卡的驱动程序，安装之后能让虚拟系统的分辨率和颜色数增加。
- 驱动器。软驱和光驱的虚拟比较简单，基本上就是和主操作系统共用，将光盘放进去就可以读取了。
- 硬盘。IDE 设备有 Virtual DISK 和 Existing PARTITION 两种方式。使用 virtual DISK 方式时，在真正的硬盘上建立一个大文件作为虚拟机的整个硬盘。在虚拟机中的任何操作都在这个大文件中进行，不会影响真正系统的数据。这种方法的好处是安全，不用担心数据问题。如果采用 Existing PARTITION 方式，那就是开放真实的分区给虚拟机使用，好处是已有的系统可以直接运行，坏处是如果不小心可能会影响硬盘上的有用数据。
- 声卡。声卡在虚拟机中一律模拟为兼容性较好的一种型号，几乎所有操作系统都能自行识别并驱动。至于虚拟机中的声音指令如何通过真实的声卡和音箱来发声，这一系列转换都由 VMware 来完成。

从以上可以看出，在虚拟机中的设备和实际的设备完全不一样，VMware 为了保证系统的兼容性和稳定性，将现有的设备都虚拟成为标准的、兼容性最好的设备，所以尽量不要试图按照自己的实际硬件情况来配置系统。除此之外，在虚拟机中不用也不能安装任何驱动程序。

1.1.3 建立虚拟系统

建立虚拟系统前首先要安装 VMware 软件，这个过程十分简单，下载完毕后一直单击 Next 按钮即可完成安装。

安装完毕 VMware 后会发现多了两块虚拟网卡，在 VMware 下可以使用虚拟网卡进行联网设置及试验。虚拟机如同真实的计算机一样，可以进行网络连接和 IP 设定。几台虚拟机一起进行网络连接，即可构成一个小型的局域网，对做网络实验非常有效。

接下来看看如何建立虚拟系统：

(1) 首先新建虚拟机。通过单击“新建虚拟机”图标，根据提示选择一种要安装的操作系统（一般选择典型设置），然后直接单击“下一步”按钮即可（图 1－2）。

(2) 进行虚拟机的启动。这个过程和 PC 的启动过程没有什么不同。当虚拟机进行开机自检时，按 F2 键可以进入 BIOS（基本输入输出系统）设置（图 1－3）。

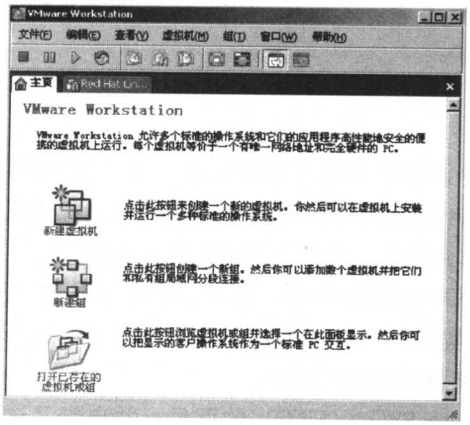

图 1－2　VMware Workstation 操作界面

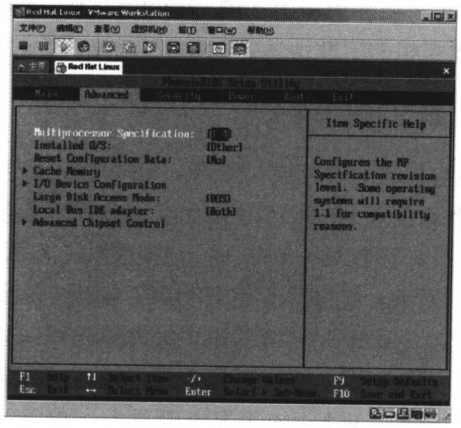

图 1－3　VMware Workstation 的 BIOS 设置界面

每一台虚拟机都有自己的 BIOS，一般为 PHOENIX BIOS，在其主界面中包括 Main（主菜单）、Advanced（高级）、Security（安全）、Power（电源）、Boot（启动）以及 Exit（退出）几个菜单项，通过方向键结合 Page Up/Page Down 键可以对各个项目进行设置。

(3) 虚拟操作系统的安装。将安装光盘放入光驱并在 BIOS 中设置从光盘启动，然后即可根据提示在虚拟机中安装操作系统，其安装过程和平常安装系统的过程完全相同。下面是 Red Hat Linux 的安装界面（图 1－4）。

选择虚拟机操作界面上方左边工具栏中的“打开电源”键，如同按下了一台计算机的电源开关。工具栏中的其他按钮分别是关机、挂起、重启按钮，其中挂起方式可以让虚拟机记录下当前状态，下次可以用 Resume 重新恢复选择挂起时的运行状态，以便可以接着上次的任务进行工作。

进入虚拟平台后，它会屏蔽主机系统的所有鼠标或键盘操作，使用过程中，可以按 Ctrl＋Alt 组合键返回主机系统。安装好操作系统的虚拟机，同样需要通过“开始”菜单关机，而不能强制关闭虚拟机电源。

1.1.4　虚拟机工具的安装

完成 Red Hat Linux 系统虚拟安装后，在 VMware 软件的左下角有一个“你没有安装 VM-

ware Tools”的提示，接下来的工作就是进行虚拟机工具的安装。

(1) 登录系统。启动虚拟计算机中的 Linux 系统，并以 root 身份登录进入 Linux，然后按 Ctrl + Alt 组合键，切换到真实的计算机系统。

如果是用 ISO（国际标准化组织）文件安装的操作系统，最好重新加载该安装文件并重新启动系统，这样系统就能自动找到 VMware Tools 的安装文件。

(2) 单击“虚拟机”菜单中的“安装 VMware 工具”选项，这时系统将自动跳出安装文件(图 1－5)。

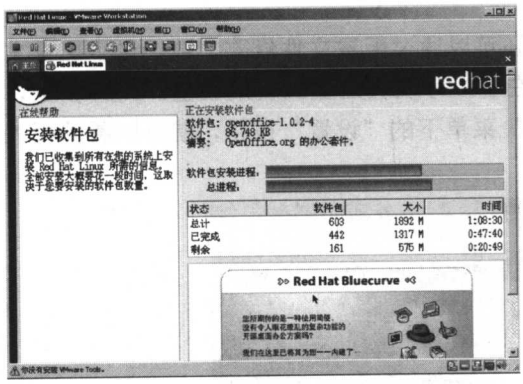

图 1－4 Red Hat Linux 的安装界面

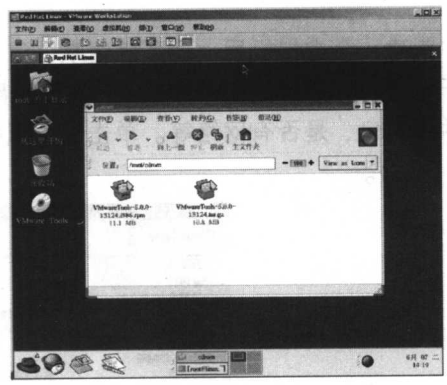

图 1－5 VMware 工具安装包文件

(3) 右击 VMwareTools－5.0.0－13124.tar.gz 文件，在弹出的菜单中选择“打开方式”选项下的 File Roller，这是一个和 WinRAR 比较类似的文件。

(4) 选择需要解压的文件包，单击“解压缩”按钮，在目的文件夹窗口中，选择解压到“/root/VMTools”目录（图 1－6)。

(5) 解压缩完毕，打开启动栏上“系统工具”下的“终端”，输入 cd /root/VMTools 命令，进入 /root/VMTools 目录，可以看到解压出来的安装文件。现在，安装文件解压到了 vmware-tools-distrib 这个目录下。

(6) 输入 cd vmware-tools-distrib 命令，进入 vmware-tools-distrib 目录。其中，有一个 vmware-install.pl 安装文件，在命令行模式下，输入 ./vmware-install.pl 命令（图1－7)，就可以开始安装 VMTools 了。

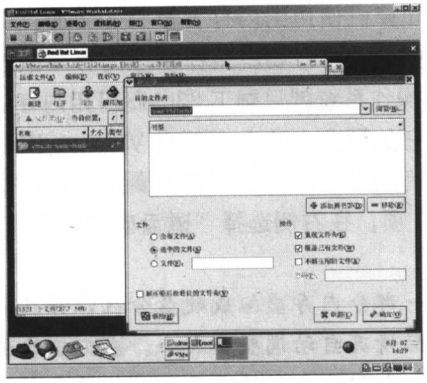

图 1－6 选择 VMware 工具安装包的目的文件夹

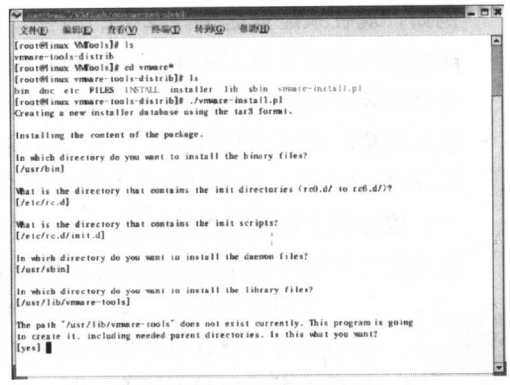

图 1－7 VMware 工具安装界面

现在系统将会提示是否备份现有的文件和链接，建议使用默认选项，直接按回车键，使用默认的安装参数设置。操作完毕，重新启动系统。以上文件名只供参考，安装时可以自行命名安装文件夹。

安装 VMware Tools 之后，再次登录 Red Hat Linux 系统，对比分析，就会发现操作系统在图像色彩和声音质量上都有很大的提高。同时鼠标可以在虚拟机、宿主机之间随意移动、切换。

1.1.5 虚拟设备和文件

新建一个虚拟机后，除了使用默认值，还可以通过配置文件修改参数。这个配置文件相当于一台新计算机的“硬件配置”，其作用在于：可以决定虚拟机的硬盘、内存多大，是否有并口串口、是否有网络等。单击“虚拟机”菜单下的“设置”按钮，就可以看到相关参数(图 1－8)。

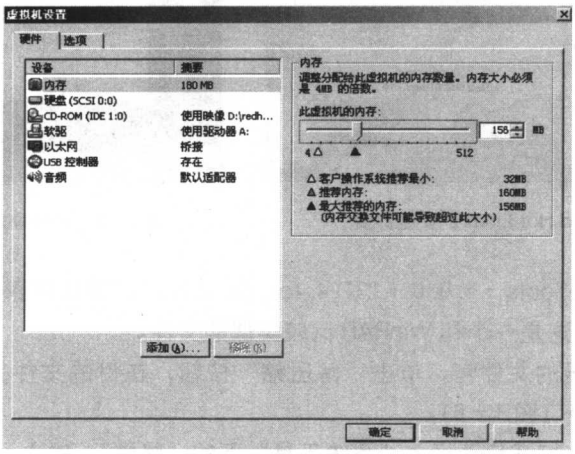

图 1－8 虚拟机参数设置界面

- 内存设置。是指从真正的内存中，分配给这台虚拟机器多少内存。

小知识

所谓虚拟内存，就是将硬盘上的一部分空间模拟成内存，实现在较小的内存下运行较大的程序。虚拟内存即虚拟机启动时占用的内存数，因此要得到一个性能卓越的虚拟机，物理内存必须足够大。

例如，现在来配置虚拟计算机的内存，如果计算机使用的内存容量为 392MB，而在此配置的内存容量为 129MB。当启动虚拟的计算机时，它要占用掉物理内存中的 156MB 来运行要安装的 Linux，这时现在正在运行的操作系统就只剩下 236MB 可用内存。

- 硬盘设置。虚拟机专门开辟了一个空间作为它的硬盘，这个文件在 VMware 安装目录的 VMS 目录下，大小将随着实际数据的增加而增加。真实的硬盘需要定期整理磁盘碎片，虚拟机上的硬盘也是如此。选中“硬盘”项，在右侧选择“磁盘碎片整理”按钮，软件就会开始整理虚拟机硬盘上的碎片。

小知识

所谓虚拟硬盘，就是通过软件将一部分内存虚拟成硬盘分区，并且采用先进的动态管理技术，根据使用者的实际情况自动调整其大小。虚拟机的硬盘就如同刚刚买回的新硬盘一样，只管放心大胆地分区格式化，对你的真实系统不