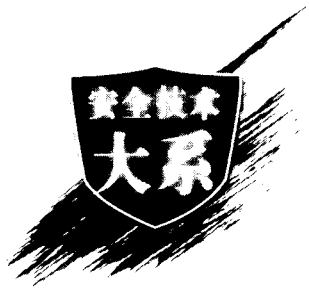
Broadview
www.broadview.com.cn

安全技术大系

黑客攻防实战详解

邓 吉 柳 靖 编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn



黑客攻防实战详解

邓 吉 柳 靖 编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。本书共分 3 篇共 11 章，系统地介绍了入侵的全部过程，以及相应的防御措施和方法。内容主要包括基于认证的入侵及防御、基于服务器软件漏洞的入侵及防御、基于 Windows 操作系统漏洞的入侵及防御、基于木马的入侵及防御、入侵中的隐藏技术、入侵后的留后门及清脚印技术、本地入侵及防御，以及防火墙技术和 BAT 编程。本书用图解的方式对每一步入侵步骤都进行了详细的分析，以推测入侵者的入侵目的；对入侵过程中常见的问题进行了必要的说明与解答；并对一些常见的入侵手段进行了比较与分析，以方便读者了解入侵者常用的方式、方法，保卫网络安全。本书是《黑客攻防实战入门》的姊妹篇。

本书适合于网络技术爱好者、网络系统管理员阅读，并可作为相关专业学生的学习资料和参考资料。

图书在版编目（CIP）数据

黑客攻防实战详解 / 邓吉，柳靖编著. —北京：电子工业出版社，2006.3
（安全技术大系）
ISBN 7-121-02221-4

Ⅰ. 黑… Ⅱ. ①邓… ②柳… 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 002901 号

责任编辑：毕 宁 bn@phei.com.cn
印 刷：北京智力达印刷有限公司
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
经 销：各地新华书店
开 本：787×1092 1/16 印张：30.5 字数：817 千字
印 次：2006 年 3 月第 1 次印刷
印 数：6000 册 定价：49.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

前　言

《黑客攻防实战入门》一书自面世以来，得到了广大读者的肯定与好评，笔者在此深表感谢。本书作为《黑客攻防实战入门》一书的姊妹篇，读者定位与其基本相同，主要针对那些对网络安全技术感兴趣的初学者，同时，本书更深入、细致地剖析了黑客技术，系统性更强，以期满足那些已有一定技术基础的读者的需要。此外，值得一提的是，笔者始终以“授之以鱼，不如授之以渔”为基本出发点来展开本书的内容。也就是说，本书的主要目的是向读者介绍黑客攻防技术的思考方法，而不是单纯地介绍某个工具的使用方法。总之，本书是一本介绍为什么，而不是单单介绍怎么做的一本黑客入门及提高书，这一点是本书区别于其他黑客类书籍的根本特征。

关于黑客

长期以来，由于诸多方面的因素，“黑客”这个字眼变得十分敏感，不同的人群对黑客也存在不同的理解，甚至没有人愿意承认自己是黑客。有些人认为，黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；有些人认为，黑客只是一群拥有技术，但思想简单的毛头小伙子；还有些人认为黑客是不应该存在的，他们是网络的破坏者。这里，我们没有必要对这个问题争论不休，也无须给“黑客”加上一个标准的定义，但从客观存在的事实来看，黑客这类群体往往存在着以下几个共同点。

① 强烈的技术渴望与完美主义。驱动他们成长的是对技术的无限渴望，获得技术的提高才是他们最终的任务。

② 强烈的责任感。只有强烈的责任感才能使他们不会走向歧途。责任感告诉他们不要在任何媒体上公布成功入侵的服务器；不要对其入侵的服务器进行任何的破坏；在发现系统漏洞后要马上通知官方对该漏洞采取必要的修补措施，在官方补丁没有公布之前，绝对不要大范围地公开漏洞利用代码。一方面，黑客入侵可能造成网络的暂时瘫痪，另一方面，黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

为什么写作本书

不容乐观的事实是，一部分人歪曲了黑客的本质，被不良动机所驱使，进行各种入侵活动，威胁网络的健康发展。对于我国来说，形势尤为严峻。我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后，在几次跨国黑客大战中，国内网站的弱口令、漏洞比比皆是，这种现状实在令人担忧，值得我们深思和反省，从中也可以看出国内传统的计算机、网络教学远远没有满足实际的需要。可能出于安全等原因的考虑，传统教学往往只教授简单的应用，避开了一些敏感的技术。设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，

那么他如何对自己网站的缺陷了如指掌？如何能够及时地获知最新漏洞而提前做好抵御？如果以上都做不到，那就更不要谈日常的系统更新、维护和打补丁了。然而，国内精通入侵的网管又有多少呢？长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。可以想像10年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括你的手机、家电、汽车，等等。因此，在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵。

出于以上原因，笔者通过多年的研究与实践，系统地总结了目前广为使用的入侵、防御技术，并针对广大网管以及对网络感兴趣的在校学生编写了本书。希望大家能够从多个角度来了解网络安全技术，至少做到知己知彼。

本书主要内容

本书以深入剖析入侵过程为主线来展开全书内容，向读者介绍入侵者如何实现信息的收集，如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵），如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日志防止目标服务器发现入侵痕迹。此外，书中还详细地介绍了入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。全书会对每一个入侵步骤做详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，此外，还会对几种常见的入侵手段进行比较与分析。

本书按照难易程度分为“入门篇”、“实战篇”和“提高篇”，3篇共11章，每章的主要内容如下。

第1章“一次完整的入侵”通过一个完整的入侵实例来介绍入侵的一般手法。使读者对入侵手法有个初步的认识。

第2章“信息收集”系统地介绍了入侵之前的准备工作。这一阶段也是经常被忽略的部分。

第3章“基于认证的入侵”介绍了如何入侵基于用户名+密码认证方式的远程主机。

第4章“基于服务器软件漏洞的入侵”介绍了入侵者是如何通过服务器软件的漏洞来实现入侵的目的。

第5章“Windows操作系统漏洞”介绍了入侵者如何通过Windows操作系统漏洞来实现入侵的目的。

第6章“基于木马的入侵”介绍了入侵者如何通过种植木马程序来实现入侵的目的。

第7章“隐藏技术”介绍了入侵者在入侵的时候所使用的一些隐身手法，通过该章读者能够了解为何难以发现入侵者的足迹。

第8章“留后门与清脚印”介绍了入侵成功后，入侵者如何抹去入侵痕迹。

第9章“本地入侵”介绍了如何入侵物理上可以接触的计算机。

第10章“防火墙技术”介绍了防火墙的原理，以及入侵者如何穿透防火墙实现入侵。

第 11 章“BAT 编程”介绍了 BAT 编程的一般方法。在入侵中，入侵者经常编写一些 BAT 程序来简化繁琐的入侵过程。

笔者将书中提到的所有相关软件整理为一个说明文件（提供了这些软件的下载地址和简单介绍），读者可到 http://www.broadview.com.cn/html/resource/hack.rar 下载这个文件。

需要声明的是，**本书的目的绝不是为那些怀有不良动机的人提供支持，也不承担因为技术被滥用所产生的连带责任；本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。**

限于水平，加之时间仓促，书中错漏之处难免，敬请批评指正。

意见反馈请发邮件至 editor@broadview.com.cn 或 jsj@phei.coml.cn。

读者与作者技术交流，可上书友论坛 http://forum.broadview.com.cn。

目　录

入 门 篇

实 战 篇

提　高　篇

入 门 篇

本篇通过一个完整的入侵实例，介绍如何搭建虚拟局域网来构建自己的入侵测试环境，如何在入侵之前获取目标主机的关键信息，以及如何实现最基本的入侵。

通过本篇的学习，读者会对网络安全技术有一个初步的认识，并且能够独立地搭建各种入侵测试环境以完成后续章节的学习。

第 1 章　一次完整的入侵

黑客技术与计算机领域其他技术的一个显著区别是黑客技术的非公开化，因此很少看到对黑客技术进行大范围公开宣传。从隶属关系的角度来看，黑客技术是计算机安全领域内的一个分支。因此，正确理解黑客技术的内涵对学习黑客技术是十分重要的。

很多人认为黑客技术很神秘，这主要是由于对黑客技术的不了解造成的。还有一部分人认为黑客技术就是用于入侵系统的技术。黑客技术确实离不开入侵，但黑客技术的应用绝不单单是入侵系统。在矛与盾的斗争中，没有绝对的胜者，为了做出更好的“盾”，仔细了解“矛”的特点是十分重要的。

本篇是全书的开篇，本篇中将着重介绍基础知识，同时通过一个入侵实例使读者对黑客技术有一个初步的了解，有助于读者后边的学习。

1.1　搭建局域网

本节中提及的局域网并不是物理上的局域网，而是指使用虚拟机搭建起来的虚拟局域网。该虚拟局域网可以供那些没有网络环境的读者来测试、实践书中所介绍的入侵与防御技术。

使用工具：VMware。

➘ 工具介绍

VMware 是一个“虚拟机”软件。它可以实现在一台机器上同时运行两个或更多的操作系统。

与“多启动”系统相比，VMware 采用了完全不同的概念。一台主机在正常安装多系统后同一时刻只能运行一个系统，需要进行系统切换时必须重新启动计算机，而 VMware 则是真正“同时”在主系统的平台上运行多个操作系统，实现像标准 Windows 应用程序那样切换。

此外，使用 VMware 可以实现在一台计算机上架设一个局域网。可以在这个虚拟的局域网中进行网络测试。

➘ VMware 的获取

可以到 VMware 的官方网站“http://www.vmware.com/”下载最新版本的 VMware，并在官方网站上注册获得一个免费使用三十天的序列号。

➘ VMware 的安装

本节中以 VMware workstation 4.0.5 为例介绍 VMware 的安装过程。

双击安装文件后会弹出如图 1-1 所示的窗口。

单击“Next”按钮，显示如图 1-2 所示。

选择接受许可后，单击“Next”按钮，会弹出如图 1-3 所示的窗口。

如果不想安装在默认路径下，可以单击“Change”按钮更改。选定路径后，单击“Next”按钮，如图 1-4 所示。

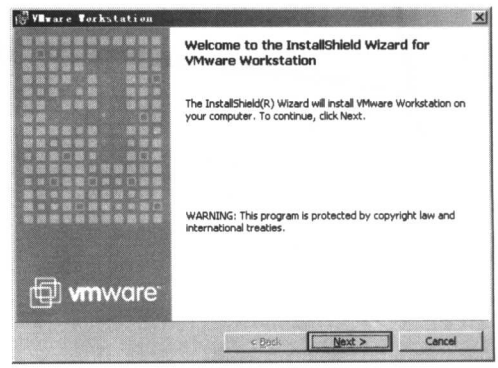


图 1-1

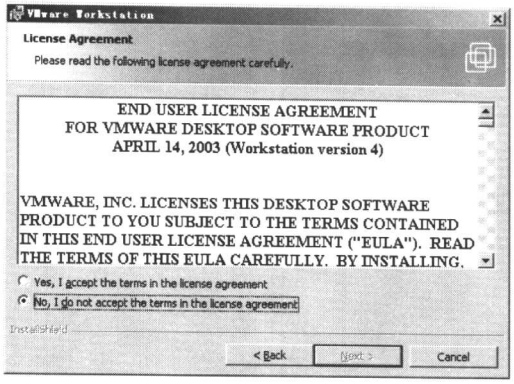


图 1-2

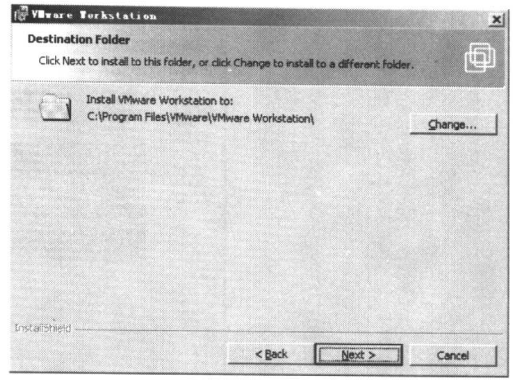


图 1-3

如果设置都正确，可以单击“Install”按钮进行安装了。

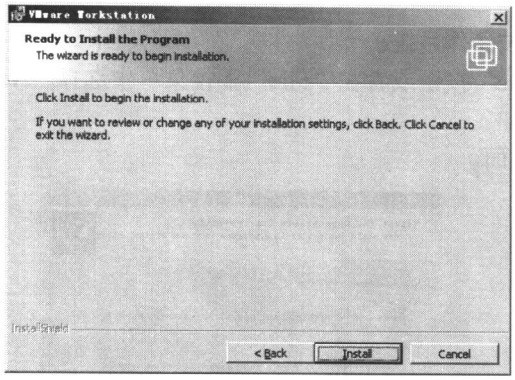


图 1-4

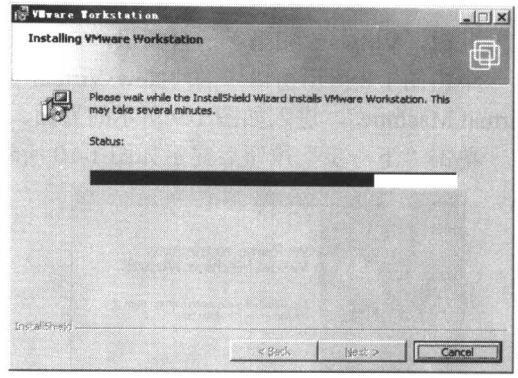


图 1-5

拷贝文件完成后，会要求输入序列号，如图 1-6 所示。

输入序列号后，单击“Enter”按钮，显示如图 1-7。

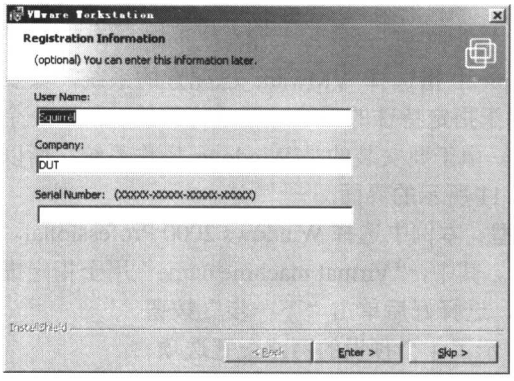


图 1-6

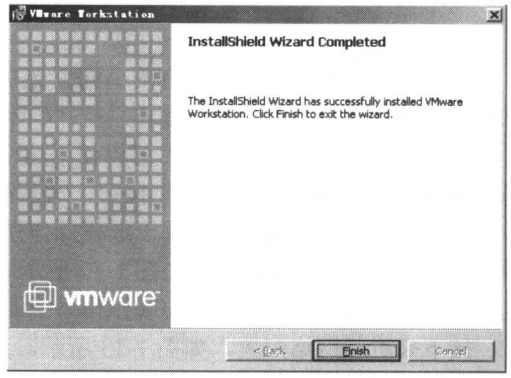


图 1-7

单击“Finish”按钮完成 VMware 的安装。

VMware 的配置与使用说明

首次运行 VMware 显示如图 1-8 所示的界面。

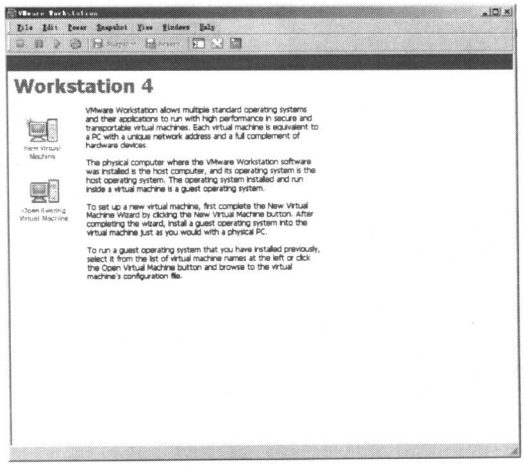


图 1-8

此时，VMware 相当于一台裸机，需要为其安装操作系统。

单击图 1-8 所示窗口中的“New Virtual Machine”按钮或者在“File”下拉菜单中选择“New Virtual Machine”，进入如图 1-9 所示的界面。

单击“下一步”按钮后显示如图 1-10 所示的界面。

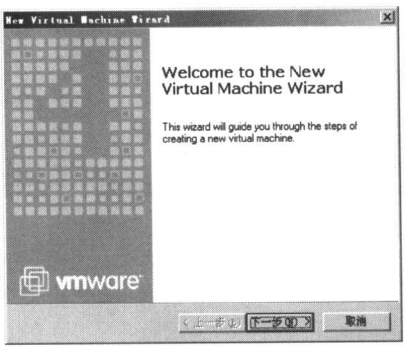


图 1-9

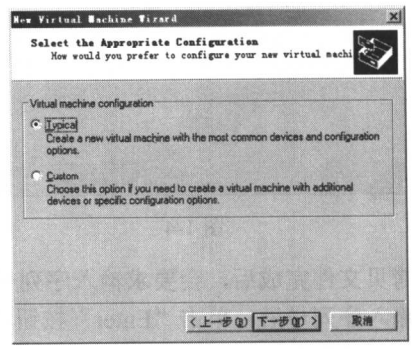


图 1-10

在图 1-10 所示的窗口中有两个配置选项：Typical 指选择 VMware 已配置的系统，如安装 Windows 操作系统或者 Linux 操作系统；Custom 用于指定特殊的系统配置或特殊的功能，一个新开发的操作系统需要进行测试时可以使用这个选项。由于要安装的是 Windows 操作系统，所以选择 Typical。然后单击“下一步”按钮，进入如图 1-11 所示的界面。

“Guest operating system”用于选择操作系统类型。本例中选择 Windows 2000 Professional。然后单击“下一步”按钮，进入如图 1-12 所示的界面。其中，“Virtual machine name”用于指定虚拟机的名称，Location 用于指定安装操作系统的位置，选择好后单击“下一步”按钮。

接下来进行网络配置，如图 1-13 所示。其中显示了 4 个预设的网络配置选项。

- Use bridged networking：虚拟机直接连接外部网络，需要为虚拟机设定独立的 IP 地址。
- Use network address translation：虚拟机通过主系统连接到外部网络，这种设置下，虚拟给与主系统使用相同的 IP 地址。
- Use host-only networking：将虚拟机连接到一个架设在主系统之上的虚拟局域网中，为架设虚拟局域网并且不希望虚拟机连接到外部网络时，可以选择此项。