黑客技术典型应用系列

154分钟
DVD多媒体
讲解视频

黑客攻防实战解析

武新华　段玲华　等编著

- 图文并茂地再现黑客入侵和主体防御的全过程，帮助读者达到知己知彼。
- 条理清晰地描述各类网络运行环境和攻防实战技巧，多年实践经验倾囊相送。
- 分门别类地提供多段多媒体讲解视频，直观再现操作步骤，全力弥补读者知识断层。

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

黑客技术典型应用系列

黑客攻防实战解析

武新华　段玲华　等编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书着眼于计算机、网络安全等方面的典型应用，从黑客攻防实战角度解析各种操作技巧与实例，从系统漏洞的查补到网络恶意入侵，从 QQ、MSN 账号保卫到木马攻防实战，从系统进程隐藏到系统间谍清理，筛选出典型案例和有效的解决方案，使读者能够循序渐进地了解黑客入侵的关键技术与方法，进而提高安全防护意识和网络管理水平。

本书内容实用，案例典型，图文并茂，适用于网络管理员及网络安全从业者，也可作为广大网络安全爱好者提升能力的参考用书。

图书在版编目（CIP）数据

黑客攻防实战解析/武新华等编著. —北京：中国铁道出版社，2009.5

（黑客技术典型应用系列）

ISBN 978-7-113-10106-0

Ⅰ.黑… Ⅱ.武… 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（2009）第 082902 号

书　　名：黑客攻防实战解析

作　　者：武新华　段玲华　等编著

策划编辑：严晓舟　荆　波

责任编辑：苏　茜　　**编辑部电话：**（010）63583215

编辑助理：惠　敏　　**封面制作：**白　雪

封面设计：付　巍　　**责任印制：**李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）

印　　刷：北京鑫正大印刷有限公司

版　　次：2009 年 7 月第 1 版　　2009 年 7 月第 1 次印刷

开　　本：787mm×1092mm　1/16　　**印张：**23.25　　**字数：**558 千

印　　数：4 000 册

书　　号：ISBN 978-7-113-10106-0/TP・3333

定　　价：45.00 元（附赠光盘）

前　言

网上黑客工具的肆意传播，使得即使是稍微有点计算机基础的人，都可以使用简单的工具对网络中一些疏于防范的计算机进行攻击，并在入侵成功之后对其中的数据信息为所欲为。进而使得用户在发现密码被盗、资料被修改删除、硬盘变做一团空白之时，想亡羊补牢，却为时已晚。可以想象，如果不了解入侵者的手段并采取必要的防御措施，关键时刻出现问题而导致重要数据丢失，将会多么令人扼腕痛惜。

因此，应广大读者的要求，我们根据自己多年的亲身体验，在总结系统网络中广为使用的入侵、防御技术的基础上，针对广大网管以及网络爱好者编写了此书，希望能够有助于大家从多个角度了解网络安全技术，从而更加有效地维护网络安全。

本书写作的目的主要是通过解析黑客攻防实战，使读者能够循序渐进地了解黑客入侵的关键技术与方法，进而提高安全防护意识。此外，本书还从黑客入侵防护应用角度给出了相对独立的论述，使读者对建构黑客入侵防范体系有一个基本概念和思路，为读者的安全防护系统建设方案提供一些有益的参考和借鉴。

本书通过常见入侵手段的比较和分析，让读者更深入地了解入侵的原理和过程，并提供相应的防御措施和解读方案。长达 154 分钟的多媒体讲解视频，帮助读者更直观地了解入侵痕迹的清除、防范工具的安装和完善的安全设置。

为了节省用户宝贵的时间，提高用户的使用水平，本书在创作过程中尽量体现以下特色：

- 循序渐进，由浅入深地讲解，使初学者和具有一定基础的用户都能逐步提高，快速掌握黑客防范技巧的使用方法。
- 注重实用性，理论与实例相结合，并配以大量插图和配套光盘视频进行讲解，力图使读者能够将知识融会贯通。
- 介绍大量小技巧和小窍门，提高读者的学习效率，节省读者宝贵的摸索时间。
- 重点突出、操作简练、内容丰富，同时附有大量的操作实例，读者可以一边学习，一边在电脑上操作，做到即学即用、即用即得，让读者快速掌握所学知识。

本书由武新华、段玲华等编著，其中武新华编写第 1 章，李防编写第 2 章，李秋菊编写第 3 章，陈艳艳编写第 4 章，杨平编写第 5 章，段玲华编写第 6、11 章，张克歌编写第 7 章，刘岩编写第 8 章，王英英编写第 9 章，孙世宁编写第 10 章，最后由武新华统稿。本书在编写过程中得到了许多热心网友的支持，参考了大量来自网络的资料，并对这些资料进行了再加工和深化处理。在此对这些资料的原作者表示衷心的感谢，没有大家的共同努力，本书是不可能完成的。

我们虽满腔热情，但水平有限，书中难免有疏漏之处，欢迎广大读者给予批评指正。意见反馈请发邮件至 jb18803242@yahoo.com.cn

编　者

2009 年 4 月

声明：

本书目的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。希望读者在阅读本书后不要使用文中介绍的黑客技术对别人的主机进行攻击，否则后果自负。切记切记！

目 录

第 1 章　安全的测试环境

本章精粹

本章在讲述虚拟硬件基础、建立虚拟系统及安装虚拟工具的基础上，重点讲述在虚拟机上架设 IIS 服务器和安装网站及相关组件的方法，并对入侵前的自我保护方法进行剖析，有助于读者更好地了解入侵者的特点，实现更好的防护。

重点提示

- 创建安全测试环境。
- 入侵测试前的自我保护。

所谓黑客或许是网络中沿着庞杂的线路潜行的杀手，又或许是在侵入别人系统之后仅仅留下一纸建议便飘然离去的侠士。无论是“杀手”还是“侠士”，黑客实施入侵的目的都是对远程主机实施控制，他们在攻击别人之前，往往会创建一个安全的测试环境进行一下实验。

1.1　创建安全测试环境

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，在操作方式及操作步骤不变的情况下，更换一个操作系统进行测试的结果可能就完全不一样。这也是很多学习黑客技术的朋友常常感到困惑的一个问题。

安全测试环境有很多因素存在，如果不能把握平台的特点，在安全实践中就会寸步难行。因此，一个好的安全测试平台是整个安全工作中的一个重要组成部分。

1.1.1　安全测试环境概述

通常情况下，网络爱好者在浏览安全技术的网页时，总是特别关注一些最新的安全漏洞和安全文摘，但却不能学以致用，原因就在于这些网络爱好者没有或无法同时兼顾多台计算机环境进行试验，没有一个完整的平台来完成安全漏洞技术的编译和测试，自身的操作系统远远达不到最新安全漏洞所需要的各种各样的平台，任意打开一个最新的漏洞描述页面，即可发现存在的多种平台需求，如图 1-1 所示。

当然，有问题就会有相应的解决方法，要想同时操作多种操作系统，唯一的办法就是运用虚拟机软件，通过虚拟的环境实现安全检测，这就是所谓的安全测试环境，该环境一直以来深受众多网络爱好者的好评，为更深一步地掌握安全技术提供了有力保障。

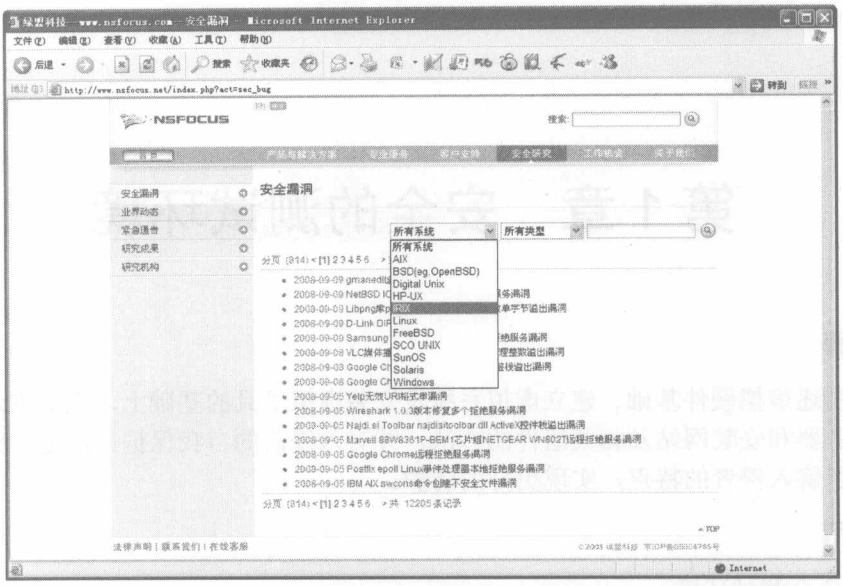

图 1-1　多种操作系统中的漏洞描述

1.1.2　虚拟机软件概述

所谓虚拟机软件是一种可以在一台本地计算机上模拟出若干台计算机的运行软件，只要本地计算机的 CPU 计算能力及硬盘容量足够强大，模拟出来的若干计算机就可以单独运行各自的操作系统而互不干扰，真正实现同时运行几个操作系统的目的，必要时还可以将几个操作系统连成一个内网网络。

下面对比较流行的几款虚拟机软件进行一些简要的介绍。

1．VMware

VMware 在实业界比较有实力，有着最完整的产品线：

- esx server：企业服务器版，面向企业用户，功能强大。esx 是一个独立的操作系统，集成了一个 Linux 作为控制台，但 esx 并不运行在 Linux 上。esx 有自己的兼容硬件列表，对硬件需求高，同时必须作为专用服务器。
- gsx server（推荐）：服务器版，面向小型企业、教育科研机构和开发人员。gsx 作为系统服务运行在 Windows 和 Linux 上。
- work station：工作站版，面向个人用户。work station 作为应用程序运行在 Windows 和 Linux 上。

2．Virtual PC

Virtual PC 因为被微软收购而成为 MS Virtual PC，包括如下几个版本：

- Virtual server：面向企业用户的系统平台迁移，运行于 Windows 2000/2003 server 系统，必须在 host 上安装 IIS 服务支持，界面不及 gsx。
- Virtual PC（推荐）：定位类似 VMware work station。
- Virtual PC for mac：Mac OS 9 和 Mac OS X 上虚拟 x86 系统。
- Virtual PC for os2：5.x 中有过这样的版本。

- Virtual PC 提供了最好的兼容性，号称凡 x86 系统均可运行。

3．Virtuozzo

sw-soft 出品。采用了和 VMware/Vpc 完全不同的技术，Virtuozzo 并没有虚拟硬件，而是采用一种称为“虚拟化”的技术，把 guest 作为 host 的副本运行。要求对 guest 的操作系统作特别的修改，不支持与 host 不同的操作系统。

Virtuozzo 的效率甚至高于 VMware，其特性非常适合于构建群集（大概也只能做这个了）。Virtuozzo 运行在 Linux 系统下，仅支持 Windows 2003 操作系统。

4．Xen

开源软件，受到众多 Linux 厂商和硬件厂商的支持。与 Virtuozzo 类似，Xen 也是采用虚拟化技术，也要对 guest 系统作修改，也不能运行和 host 不同的系统，也具有十分高的效率。Xen 目前仅支持 Linux。

5．Two OS two 和 Svista

这两个软件的界面十分类似，虚拟硬件、磁盘格式几乎完全相同，都采用了和 VMware 十分相似的虚拟方案，像极了 VMware work station 的精简版。Two OS two 和 Svista 运行于 Windows 2000（SP2）/XP/2003 操作系统，效率略低于 VMware，和 Virtual PC 相当。

6．Bochs

历史悠久的开源软件，仿真 P75/P3 计算机，带硬件调试，适合开发操作系统。速度慢，界面控制不方便，没有太多实用性。Bochs 有 Linux 和 Windows 两种版本。

7．Qemu（推荐）

开源软件，在 Bochs 的基础上开发而成。Qemu 模拟了 Pentium III，速度有很大提高，几乎可以和 Vpc 相比，Linux 版本更是带了一个加速器。

Qemu 目前有 Linux、Windows 和 Mac OS 版本，除了 x86 之外，还可以模拟 powerpc、sparc、adm64 和 arm；并且仍在开发模拟更多的 CPU 和更多的发行版。Qemu 需要通过命令行设置启动配置，也需要通过命令行更换光盘，使用极为不便。不过，已经有了两种第三方开发的 GUI（图形界面），使用不便的问题终于可以解决了。

8．Dosbox

在 Windows 2000/XP 下虚拟了一个纯 DOS 环境，怀旧 DOS 游戏的最佳选择。

Windowse/Windows4linux/Dosmenu

在 Linux 下虚拟了 Windows 程序的运行环境，更像是 dos4gw 的现代版。

9．Cygwin/Windowslinux

作为开源软件的同时兼且体积庞大，提供在 Windows 下的完整的 UNIX 环境和开发。可以通过 Cygwin 在 Windows 下运行 Linux 程序，也可以编译 Linux 源程序。Cygwin 编译出来的是可在 Windows 系统中直接运行的可执行文件，是 Linux 软件向 Windows 移植的利器，Bochs、Qemu、Pearpc 的 Windows 版本都是这样做的。

Cygwin 支持 Windows 2000/XP/2003 操作系统，可以视为 UNIX 的 Windows 内嵌版本。Windowslinux 和 Cygwin 十分类似，是 Linux 的 Windows 内嵌版本。

10．Beos

Beos 是一个基于多媒体的操作系统，而其他操作系统都是基于文本的。

11. Colinux

Colinux 是开源软件，提供 Windows 下的 Linux 系统的模拟，需要对 Linux 系统作修改。

12. Simics

可以用来模拟最多的系统，包括 x86、amd64、ia-64、alpha、powerpc、68000 系列、sparc、arm 等，可以在 Windows/Linux 下运行。在当前的虚拟机软件中，比较常用的有 VMware 和 Virtual PC 两种虚拟机软件，在虚拟平台的测试过程中，VMware 需要一个操作系统作为基本平台，即 HOST OS（主系统），在 HOST OS 上运行的其他系统都叫 GUEST OS（子系统或客户系统）。

下面简单介绍一下几个在 VMware 虚拟机中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 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 将显卡模拟成了 VMware SVGA（FIFO），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。使用第一种方式时，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，不会影响到真正系统的数据。采用第二种方式就需要开放真正的分区给虚拟机使用，优点是已有的系统可以直接运行，缺点是有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。

由此看来，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，将现有设备都虚拟成为标准、兼容性最好的设备，所以尽量不要试图按照实际硬件情况来配置系统，并且在虚拟机中也不能安装任何驱动程序。

1.1.3 用 VMware 创建虚拟系统

利用 VMware 可以在一台计算机上将硬盘和内存的一部分拿出来虚拟若干台计算机，每台计算机可以运行单独的操作系统而互不干扰，这些“计算机系统”各自拥有自己独立的 CMOS、硬盘和操作系统。用户可以像使用普通计算机一样，对其进行分区、格式化、安装操作系统和应用软件等操作，还可以将这些系统联成一个网络。

1. 安装 VMware 软件

VMware 软件与其他普通软件一样，在使用之前需要先进行安装，具体操作步骤如下：

步骤 1 双击下载的安装文件即可自动安装，并同时弹出一个信息提示，如图 1-2 所示。

步骤 2 单击“确定”按钮，打开“安装向导”对话框，如图 1-3 所示。

步骤 3 单击 Next 按钮，打开“安装模式”对话框，系统提供 Typical（典型）和 Custom（自定义）两种安装模式，用户可根据实际情况选择相应的模式，如图 1-4 所示。

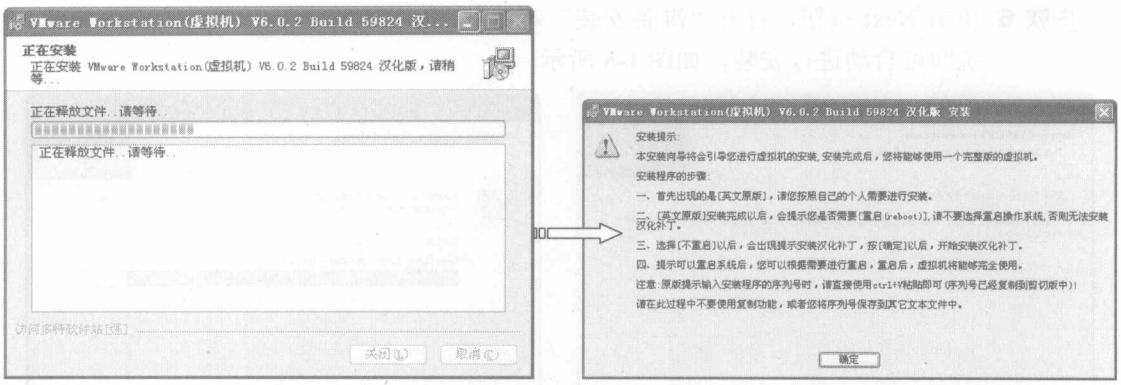

图 1-2　信息提示

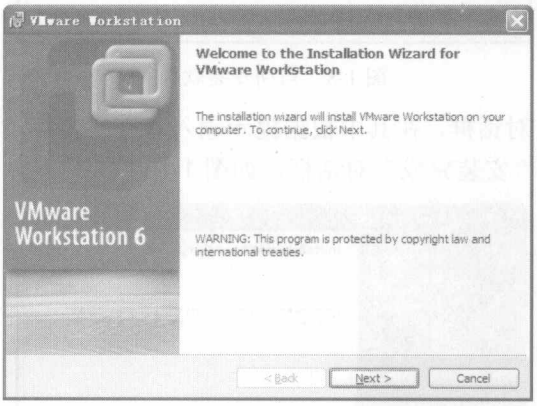

图 1-3　安装向导对话框

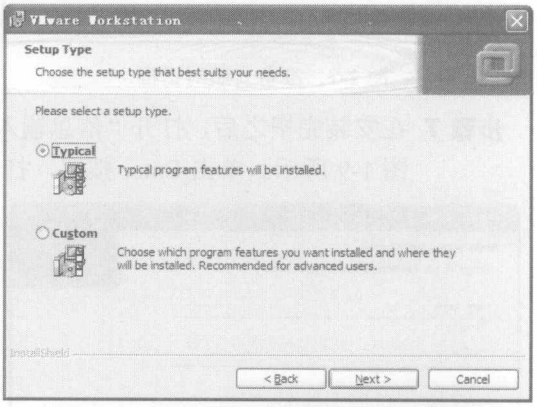

图 1-4　安装模式对话框

步骤 4 单击 Next 按钮，打开“选择安装路径”对话框，用户可以选择系统默认的路径，也可以单击 Change 按钮，从打开的对话框中重新选择要安装的路径，如图 1-5 所示。

步骤 5 在路径选择完毕之后，单击 Next 按钮，打开“选择快捷方式”对话框，根据实际需要选择相应的复选框，如图 1-6 所示。

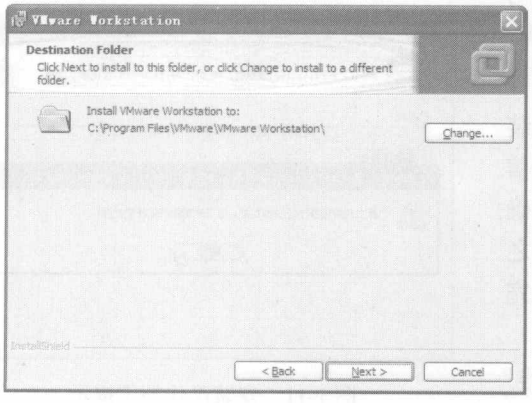

图 1-5　选择安装路径对话框

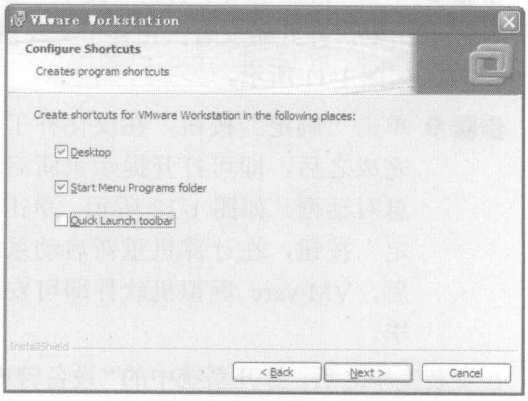

图 1-6　选择快捷方式对话框