电脑报 总策划

电脑报 编

MY FIRST WORK SECURITY HANDBOOK

我的第一本网络安全手册

真能上手

轻松掌握黑客攻防技法

超值光盘

98元黑客攻防视频教程
全防范及漏洞检测软件
彩黑客电影及壁纸欣赏

●菜鸟必须熟悉的**安全规则**，必须要了解的**攻防细节**；●初学者**查漏补遗**，探秘各种**攻防技巧**，掌握**安全命门**；●资深黑客自述的**闯关宝典**，解密黑客入侵缘何**势如破竹**；●安全专家撰写的防御手册，精确剖析，**抵御入侵**。

电脑报电子音像出版社
CPCW ELECTRONIC & AUDIOVISUAL PRESS

MY FIRST NETWORK SECURITY HANDBOOK

我的第一本网络安全手册

真能上手

轻松掌握黑客攻防技法

电脑报 编

电脑报电子音像出版社
CEAP ELECTRONIC & AUDIOVISUAL PRESS

内容提要

本手册采用实例的形式为大家详细解析了黑客的各种攻防手段与要领，通过细致的步骤讲解，让大家特别是初学者能很好上手，对于各种安全问题能迎刃而解。其内容包括病毒木马、端口进程、漏洞攻防、网页挂马、信息搜集、QQ防盗、嗅探欺骗等。选材全面主流，涉及安全攻防的方方面面，对于入门新手来说，不再是枯燥叙述与技术分解，趣味性、互动性让学习、理解更加轻松。

光盘要目

● 50款安全防范必备软件 ● 价值98元黑客攻防视频教程 ● 10部经典黑客电影介绍 ● 精美壁纸欣赏

警告：文中涉及到的黑客攻防相关内容，仅供读者学习之用，如用于非法途径，后果自负。

真能上手——我的第一本网络安全手册

编　　者：电脑报
技术编辑：钟　卫
版式设计：杨　亚
出版单位：电脑报电子音像出版社
地　　址：重庆市双钢路3号科协大厦
邮政编码：400013
服务电话：(023)63658888-13117
发　　行：电脑报经营有限责任公司
经　　销：各地新华书店、报刊亭
CD生产：苏州新海博数码科技有限公司
文本印刷：重庆日报印务有限公司
开本规格：787mm×1092mm 1/16 20印张 190千字
版　　号：ISBN 978-7-89476-329-7
版　　次：2010年4月第1版 2010年4月第1次印刷
定　　价：35.00元(1CD+手册)

前言 PREFACE

随着互联网的不断发展，信息交流也变得更为高效、快捷，但与此同时，网络的安全隐患却时时威胁着大家的学习与生活。水能载舟，亦能覆舟，网络就像一把双刃剑，在促进经济发展、推动社会进步和提高人们生活质量的同时，也爆发着很多危险信号。账号泄漏、资料被盗、硬件被损，其问题日趋严重，需引起每一位电脑用户的重视。

时下越来越多的关键应用已经迁移到网上，网络应用的安全性已经成为各机构的重要挑战。知己知彼，方能百战不殆。要杜绝这种损失，只有从根本上了解网络应用程序中存在的可被利用的漏洞和攻击者所采用的攻击方法，才能更有效地确保网络安全。

考虑到初学者的理解程度，本手册内容深入浅出，特意将一些原本枯燥乏味的理论知识通过更形象的方式表述出来，适合新手第一次学习网络安全知识。手册从网络安全技术的基础知识入手，到进阶的黑客工程学，内容包罗万象。无论是常用的漏洞进程、盗取账号等雕虫小技，还是嗅探欺骗、网页挂马等瞒天过海招数，通过大量的实例，以生动活泼的形式，呈现在广大读者面前。

本手册内容翔实、通俗易懂，实例丰富、步骤详细，图文并茂、生动有趣，版式精美、阅读轻松，其配套光盘更有丰富的软件与视频供大家学习研究。本手册定位于有一定电脑知识的用户，可供在校学生、电脑技术人员、各种电脑培训班学员以及不同年龄段想了解网络安全技术的电脑爱好者学习参考。

黑客不再高深，菜鸟也可以扮大师，网络安全攻与防，你我都能轻松上手。

编者

目录 CONTENT

我的第一本网络安全手册

THE FIRST NETWORK SECURITY HANDBOOK

CH1 病毒木马篇

CH2 端口进程篇

CH3 漏洞攻防篇

CH4 网页挂马篇

CH5 信息搜集篇

CH6 账号密码篇

CH7 嗅探欺骗篇

CH8 QQ防盗篇

CH9 远程控制篇

病毒木马篇

NETWORK SECURITY

第1回 巧借虚拟机环境与病毒零距离接触

一、计算机病毒及其分类

1.计算机病毒的概念

小张首先发问了：“最近两年计算机病毒特别多，经常都听朋友说电脑中病毒了，王教授，到底什么是计算机病毒呢？”王教授略有所思，然后回答道：“简单地说，其实计算机病毒就是一段恶意程序，能达到编写者的某个目的，比如破坏你的数据、恶作剧、窃取资料等。当然，按照国家有关条例的规定的准确含义是‘计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。’”

王教授将这一准确定义背出来让小张听呆了，小张不得不对王教授另眼相看了，佩服有加！怀着无比尊敬的心情，小张再次发问：“王教授，那计算机病毒可以分为哪些类别呢？”

2.计算机病毒的分类

王教授笑了笑，“计算机病毒分类很复杂，按照不同的分类标准，会有不同的分类，这里我只做简单的介绍，说多了也记不住啊！”

“按入侵方式可以分为：源码型病毒、入侵型病毒、操作系统型病毒、外壳型病毒；按破坏性可分为：良性病毒、恶性病毒，其中良性病毒没有危害，而恶性病毒则是有一定的危险性，甚至有的非常危险；按病毒算法还可以分为：伴随型病毒、寄生型病毒、蠕虫型病毒等。病毒的分类方式很多，大家只需要简单了解一下即可。”

小张点了点头：“分类是有些复杂，不过这些不同种类的病毒都是通过什么方式传播的呢？有的时候我没有上网，怎么也会感染病毒呢？”

3.计算机病毒传播途径

王教授笑了笑，“这个问题就涉及到病毒的传播方式了，除了当前大家所熟知的互联网传播病毒外，其实还有多种病毒传播方式，比如现在大家使用比较广泛的U盘、移动硬盘就是一个传染源，所以即使没有上网也可能在拷贝文件的时候传染病毒。此外，局域网传播、光盘传播也是大家容易忽视的，以后一定要引起高度重视。有的病毒，在局域网中一台电脑感染了，可能导致整个局域网全部中毒，甚至所有机器全部瘫痪，这是非常可怕的。下表是今年五一黄金周病毒排行前10名，感染数量之大，不得不让我们高度重视。”

病毒名称	感染电脑台数（台）
Ani 漏洞下载器（RISK.Exploit.Ani）	201123
ANI 漏洞生成器 （Win32.Troj.ExpAni.a）	63449
病毒生成机（Win32.VirInstaller.Delf）	30364
罐金（Worm.Viking.gm）	15507
Win32.Troj.OnLineGames.nb	12885
Win32.Troj.ZSKill.tf.88569	8913
传奇木马 （Win32.Troj.Mir.t）	8827
Win32.Troj.TianLongBB	8627
Win32.Troj.OnLineGamesT.ob	8357
灰鸽子 （Win32.Hack.Huigezi.cz）	6941

二、什么是虚拟机

听了上面的讲解，小张对病毒有了基本的认识，总觉得还是很害怕，不过小张心中也有不少疑问："这些病毒应该如何防范和查杀呢？另外，制造病毒的作者如何测试这些病毒的威力，难道用他们自己的电脑做实验？有的病毒危害性非常大，谁敢把病毒放自己机器上做测试呢？"

王教授点了点头，说道："很好，这说明你非常用心去思考了。计算机病毒的查杀方法这里我们暂且不讲，因为不同病毒查杀方法是不同的，而用杀毒软件查杀的方法大家都知道了，非常简单，非常傻瓜化的操作。这里我主要探讨你提出来的第二个问题，就是病毒的测试平台问题，由于很多病毒危害性很大，病毒制作者和病毒研究者很多时候都是在虚拟机中进行测试的。"

"什么是虚拟机？"小张打断了王教授的话。王教授顿了顿："别着急，这就是我下面要讲的。简单地说，虚拟机就是借助软件来实现在你的一台机器上同时模拟出多台机器，这些虚拟机用起来几乎和真实的机器一模一样，它们有自己的BIOS，有一套完整的硬件设备、有自己的操作系统，可以在里面运行软件，总之，跟我们常用的电脑没有大的区别。唯一不同的是，在虚拟系统崩溃之后可直接删除而不影响本机的电脑系统，这就为这些病毒开发者和研究者的高危操作提供了一个安全可靠的平台，让他们尽情测试危险操作，而不会影响其电脑。虚拟机在学习技术方面能够发挥很大的作用。"

听到这里，小张又发问了，"那么，有哪些软件可以实现虚拟机的功能呢？"王教授回答道："这类软件目前并不多，常用的有VMware、Virtual PC、Xen、Parallels、Virtuozzo等，但最常用的当属VMware和Virtual PC了。"

"王教授，那就教教我如何使用这神奇的虚拟机器吧！"王教授回答道："好的，没问题，不过先来简单了解一下虚拟机的几个概念。"

小知识Tips

（1）主机：主机即用户在真实环境中使用的计算机，主机被称为Host OS，在使用虚拟机时，也被称为"宿主机"。

（2）客户机：客户机就是安装在主机中的虚拟系统，包括虚拟的硬件，如CPU、内存、硬盘、光驱等。客户机又被称为Guest OS。

（3）虚拟机光驱：虚拟机将主机中的光驱当作自己的光驱，如果用户在Windows环境中，也可以使用虚拟光驱来做虚拟机的光驱。

（4）虚拟机内存：虚拟机将主机中的内存划分一部分作为自己的内存，要流畅使用虚拟机，大容量内存是必要的。

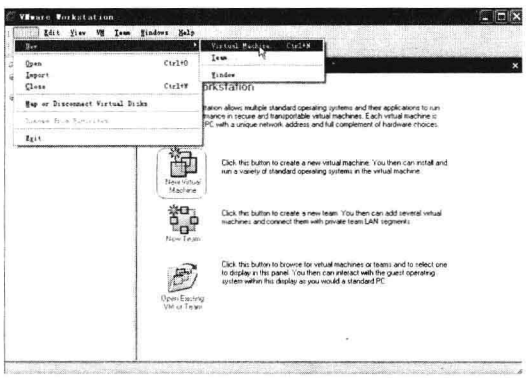
三、第一次搭建虚拟机环境

“了解虚拟机的基本概念后，下面我们一起来看看如何搭建一个虚拟机环境。”王教授开始讲解虚拟机安装配置方面的知识了。

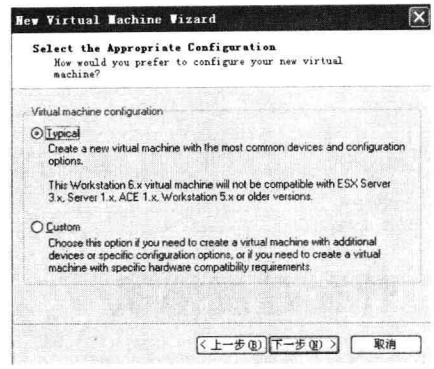
1.安装操作系统前的初始配置

这里以使用非常广泛的VMware虚拟机软件为例，首先安装好这个软件。在使用虚拟机安装操作系统之前，首先要对模拟系统作必要的配置，包括对虚拟内存、硬盘、光驱等设置，然后才能像在真实主机中那样，在虚拟机中安装虚拟操作系统。

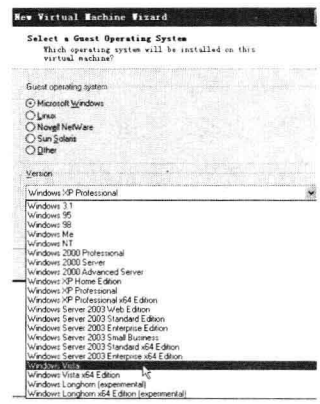
首先打开VMware程序，单击“File→New→Virtual Machine”菜单，或者单击主界面上的“新建虚拟机”图标，弹出新建虚拟机的配置向导对话框。



单击“下一步”按钮进入虚拟机配置对话框，在此对话框中有两种虚拟机配置“典型（Typical）”和“自定义（Custom）”，在没有特殊设备或配置的情况下，我们一般选择“典型（Typical）”配置。



单击“下一步”按钮，进入“选择客户机操作系统”对话框。用户根据实际需要在“客户机操作系统”组合框中选择操作系统种类，然后在“版本”下拉列表中选择版本。



单击“下一步”按钮进入“虚拟机命名”对话框，输入本虚拟机名称和安装在主机中的位置。