电脑報 总策划

搞定黑客当好网管

仲治国 编著

网管 VS 黑客终极大练兵

想当网管，先做黑客 知己知彼，方能百战百胜！

- 黑客是主动的 网管是被动的
- 黑客就像是怪盗 网管就是侦探
- 黑客能变成网管 网管也能变成黑客

暗战！恶战！！决战！！！

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

搞定黑客 当好网管

编著：仲治国

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

内容提要

黑客是主动的，网管是被动的。

黑客就像是怪盗，网管就是侦探。

黑客能变成网管，网管也能变成黑客。

做一个好网管，先从做一个小黑客开始，这是被普遍认可的信条。

网管的职责之一是维护网络的安全、防范黑客的攻击，当网络出现问题时及时采取措施补救，确保网络正常运作。但这毕竟是比较被动的做法，高水平的网管应当通晓黑客攻击的各种方式，主动发现网络存在的漏洞，及时修补漏洞，化被动为主动。

虽然黑客攻击的方式层出不穷，但归结起来不外乎以下几类：获取口令、放置木马、WWW欺骗技术、电子邮件攻击、通过一个节点来攻击其他节点、网络监听、寻找系统漏洞等。一个合格的网管应该精通黑客攻击的原理，这样才能更好的防御黑客的攻击，做到知己知彼，百战百胜。

本手册就是从黑客攻击的角度出发，以实例为基础，让读者深度了解黑客攻击的各种手法与手段，从而在日常管理工作中做到处变不惊，从容面对并迅速处理各类突发事故。

警告：本手册涉及到的黑客相关知识，仅供读者学习之用，如用于非法用途，后果自负。

光盘要目

1.IP工具
2.服务器工具
3.密码工具
4.系统安全工具
5.网络安全工具
6.网络控制工具
7.网络监测工具

书　　名：搞定黑客，当好网管
编　　者：仲治国
责任编辑：李　志
技术编辑：黄　斌
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
对外合作：(023)63658933
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：重庆华林印务有限公司
开本规格：787mm×1092mm 1/16　21.5印张　400千字
版　　号：ISBN 978-7-89476-120-0
版　　次：2009年4月第1版　2009年4月第1次印刷
定　　价：38.00元(1CD+配套手册)

基础篇

第1章 网络安全与黑客攻击

第2章 黑客常用兵器谱

第3章 黑客与网管必知DOS命令

应用实战篇

第4章 黑客VS网吧网管

第5章 黑客VS企业网管

第6章 黑客VS网站网管

第7章 黑客暴力攻击与网管防御

第8章 黑客控制与网管反控制

第9章 黑客嗅探与网管监控

网管防线篇

第10章 严密部署权限防线

第11章 账户的安全管理

第12章 远程访问安全配置

第1章

网络安全与黑客攻击

无论是个人PC，还是各种网络中的服务器与工作站，都无法对“安全”这个话题进行回避。特别是随着网络用户的不断倍增、黑客工具与病毒的泛滥，更是让网络中的安全问题日趋严重——当邮件的内容被偷窥、经商创业的内容被窃取、即时通信中附带病毒、影音娱乐中内藏木马、辛苦编就的文件被恶意删除、电脑应用变得没有安全保障时，人们开始“谈网色变”。

网络应该是为电脑添加了腾飞的翅膀，进而成为生活中的一种时尚。可是，安全问题的悄然来临，让我们的生活与工作产生诸多不和谐的因素。没有人喜欢用电脑时还有一双眼睛在远程监控你，没有人愿意自己的电脑慢如蜗牛，没有人会同意自己的电脑被别人如入无人之境……

在网络环境中，各种安全隐患是屡见不鲜、防不胜防，无数的网管员都在为之头疼。对于很多初、中级网管员来说，如果哪天无人求救，那天才是真正的休假。否则，很多休假的日子也会被一个个电话召了回去。

在本章中，将以中小网络网管员的角度，谈谈如何面对各种常见的安全问题，以便让复杂的安全问题条理化，让脆弱的防御策略堡垒化！让大家对黑客和网络安全有个全面的认识。

1.1 网络安全隐患所在

十几年前，我们使用的网络大部分是同轴电缆组成的网络，网络出现的问题不外乎就是网络不通。网管要做的任务就是花上几分钟整理一下网线或是网络协议。可是，如今的网络环境早已经是日新月异：双绞线、光纤、具有网管功能的交换机、操作复杂的路由器、设置繁琐的网关、功能迥异的服务器，要求熟练运用的技术太多。在这一切已经足以让初、中级网管员头痛的时候，防不胜防的黑客和病毒却又如潮水般涌来……棘手的问题一个接一个，怎是一个“烦”字能说得清？

很多个人电脑用户在谈到网络安全时都不能理解：为什么我只是一个普通的个人电脑用户，却会有这么多莫名其妙的“黑客”对我感兴趣？

其实原因很简单：现在网络上泛滥的黑客工具使任一个网民都可以随手而得。很多新手喜欢使用扫描类工具对某一 IP 地址段进行大规模的端口扫描，利用这些工具来发现网络上的具有安全隐患的主机，然后再逐个进行入侵或攻击。其实他们在进行扫描之前根本就不知道你究竟是谁。这也就是为什么个人电脑用户屡屡发生安全问题的根本原因。

那么，为什么企业也会有各种各样的安全问题呢？这是因为企业的“出口”太多，每一台电脑都开放了 N 个端口，都在不停地进行着各种应用，这些都会或多或少地与网络安全“挂上钩”。例如，某台电脑中了蠕虫病毒后，当他将电脑中的文件发送给局域网中的同事时，同事的电脑就会被感染，如图 1-1 所示。

图1-1 网络中的每一台电脑都可能是病毒的传播者

当然，稍微“高级”些的病毒就会自动在网络中进行自身的传播——这种“无色无味”的“毒药”基本上是中者必失。所以，网络管理员应该对网络中的每一台电脑都进行把关，例如，要求每一台电脑都要安装杀毒软件等等。一般来说，网络主要面临如下几点安全隐患：

1.病毒的感染

俗话说得好：“病来如山倒，病去如抽丝。”如果电脑感染了病毒，轻则软件“发烧感冒”，重则连硬件都会遭受破坏。病毒让电脑来个“一病不起”的事儿已是屡见不鲜！

病毒一般具有隐藏性、潜伏性、传染性、破坏性等特征，通常条件好的网络会使用硬件级病毒过滤设备，如图 1-2 所示。

图1-2 网关过滤设备

一般性的网络则会依靠网络版杀毒软件来完成病毒的防御任务，如图 1-3 所示。因为网络规模有多种，所以，网络版杀毒软件也会分为好几种版本，不同版本的杀毒软件不仅设计理念不一样，在功能上、使用上都有很多的不同之处。

图1-3 网络版杀毒软件

2.黑客的入侵与攻击

与病毒程序相伴相随的就是黑客程序了，它的出现虽然要比病毒程序晚许多，其盛行只是近几年随着计算机网络的普及才开始的，但是它的威胁性和破坏性比病毒更大。

黑客一般会使用三种方法入侵目标电脑，一是使用各种方法向对方电脑植入木马程序，只要

对方上线自己就会立即知道并进行遥控，如图 1-4 所示。

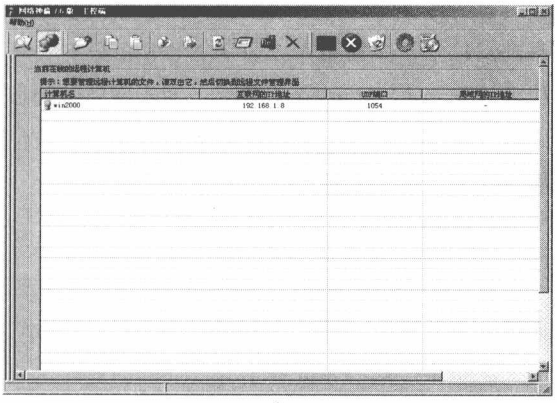


图1-4 服务器端上线

二是扫描目标电脑是否存在什么漏洞，如果存在漏洞——网络中的电脑如果不经过专门的漏洞修补的话，基本上每一台电脑都会存在问题，如图 1-5 所示。

图1-5 Windows XP单机中的常见漏洞列表

很多企业的网管员只在服务器上进行漏洞修补，却忽略了单机的漏洞问题，让黑客有机可乘，这也是安全管理体系上的一个不足。

三是目前攻击效果仍是排在前列的 DDoS（分布式拒绝服务攻击），这种攻击方法是持续使用大量的数据包攻击目标，目的是使目标主机的被访问能力严重下降，如图 1-6 所示。

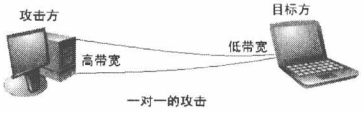


图1-6 DoS攻击方式

在网络中，只有服务器会受到这种攻击，单机一般不会受到这个问题的困扰。但是，由于服务器和单机是使用同一个 Internet 接口，所以，当 Internet 带宽受到严重影响时，单机的 Internet 应用自然也会受到影响。

网络解决这个问题的方法，一般有两种：一是购买硬件防火墙，如图 1-7 所示。

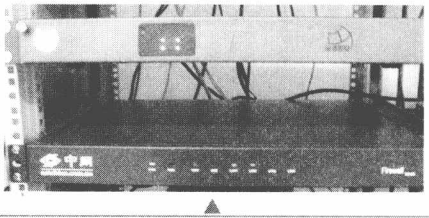


图1-7 硬件防火墙

二是使用软件防火墙，把监测到的攻击 IP 地址屏蔽掉，即丢弃这些发来的数据包，这样也可以起到一定的防御作用，但是效果一般。

事实上，黑客入侵有两种方式，一种网络入侵，还有一种就是本地入侵。后者的使用量甚至还要大于前者，而且也较前者更容易入侵成功。例如，本地入侵中的“输入法漏洞”，就可以让黑客轻松获得 Vista 系统的管理权限。所以，网管员不仅要对网络通道严加防范，还应对机房的使用人员进行相应规章的制定。

病毒程序的设计目的大多数都是搞破坏，黑客程序的设计目的则是“深入敌后”，把目标电脑的控制权拿下来，以便获得各种所需的资料。因此，黑客行为或工具一般不具备破坏性，因为把系统破坏了，自己也就没得用了。

3.账户密码设置不当

对于一台电脑来说，账户就是它的主人姓名，密码就是主人的钥匙。账户是必需存在的主体，密码虽然可有可无，但是没有密码就表示给了黑客一把万能钥匙——推开系统的大门就可以了。这样的电脑安全性毫无保障，即使安装了强大的防黑杀毒的软件也无济于事。所以，默认状态下，在 Windows XP/2003 等系统的组策略中已经禁止使用“空密码”进行远程登录了，如图 1-8 所示。

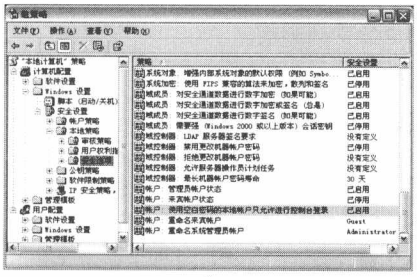


图1-8 组策略设置

4.权限设置不当

所谓“权限”（Permission），是指用户对于对象的访问限制。例如，能否新建、读取、删除对象。对象的种类包括文件、文件夹、分区、磁盘和打印机等等，如图 1-9 所示。

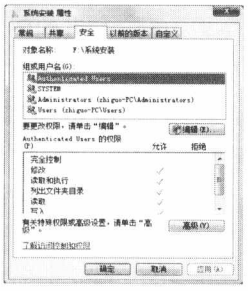


图1-9 权限设置列表

设置权限是以对象为基础，即“设置某个对象有哪些用户可以拥有相应的权限”，而不能是以用户为主，即“设置某个用户可以对哪些对象拥有权限”。这就意味着“权限”必须针对“对象”而言，脱离了对象去谈权限毫无意义——在提到权限的具体实施时，“某个对象”是必须存在的。

以文件夹与文件的权限为例，依据是否被共享到网络上，其权限可以分为 NTFS 权限与共享权限（Shared Permission）两种。对于网络管理员来说，要清楚地知道权限在网络访问通道中的位置、作用与常见问题。

5.邮箱被破解或邮件被拦截

对于企业网络来说，邮箱被破解或邮件被拦截都是一个属于“严重”级的问题，如图 1-10 所示。因为邮箱中一般有合同样本等重要的商业秘密或者是个人隐私。这些资料是不能外泄的，否则可能会给企业的运作上带来被动。

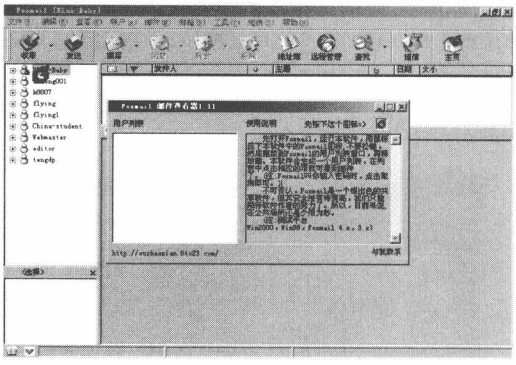


图1-10 Foxmail的邮箱被破解

网管员应该从多个角度对邮箱问题进行防范，有条件的可以通过硬件设备过滤一些包含木马等病毒的邮件，否则可以从软件角度上进行一些防范，如使用 PKI 技术等。

6.操作系统漏洞

有很多企业网管员只对服务器的系统漏洞加以重视，却忽略了单机的系统漏洞。其实，很多时候面向公众的服务器里提供的反而是不重要的普通资料，有些高级企业管理人员私人电脑中的资料才是企业运行的“核心”内容。因此，对于网管员来说，最好是使用域环境对整个网络的电脑进行统一管理，如统一安装补丁，等等。

什么是系统漏洞？系统漏洞就是 Windows 本身因设计缺陷产生的安全问题。系统漏洞是一个永远不会终结的问题，我们不要期望系统的漏洞能彻底修补好，因为系统漏洞永远是“此补彼现”，如图 1-11 所示。

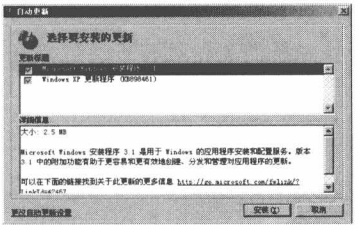


图1-11 检测到的系统漏洞

7.文件的非法访问

在电脑中进行的一切数据处理操作都是以文件为基础的。例如，用 Word 编辑了一份文档文件，用“录音机”录制了一个声音文件，用摄像头拍了一幅图像文件，等等。

在企业环境中，有很多数据（如编写的商业合同文件）是不希望被别人随意查看内容的，对于这样的文件可以使用加密的方法进行保护。因此，网管员应熟悉文件夹、文件、克隆文件等重要数据的常见加密与解密方法，并对 EFS 这些系统加密功能加以了解。

8.交换设备设置不当

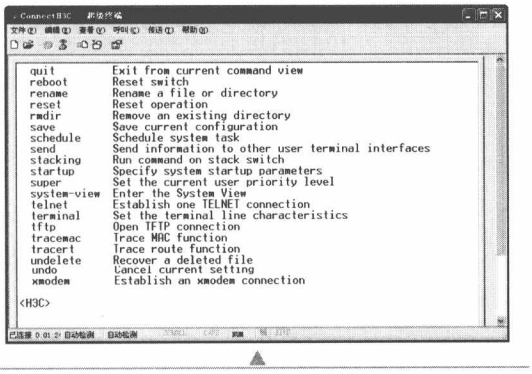


图1-12 通过终端配置交换机

在网络的中央节点设备中，路由器和交换机等都是具有网管功能的，对于没有彻底掌握含义的功能最好不要乱设置，因为一不小心把默认的标准策略设置为宽松策略，那么网络就可能面临入侵等糟糕的问题，如图 1-12 所示。

9.数据存储介质损坏、丢失或维修时泄密

数据可能会因很多原因泄密，其中硬盘、光盘、优盘等存储介质出现损坏、丢失和维修现象时，最容易泄密。特别是对硬盘进行维修时，维修的时间往往需要等待几天，在这个过程中很容易就把数据弄丢或被复制。要解决类似的问题，需要对重要的数据进行加密和备份，并且最好能在有实力、有信誉的维修处目睹维修过程，慎防数据被恶意拷贝。

10.第三方程序漏洞，如Serv-U、网站程序等

除去了操作系统外，网管员经常需要在电脑中安装第三方软件，并使用它们（如 Serv-U）与 Internet 进行数据交互，此时，就要谨防这些软件带有安全问题——没有百分百安全的操作系统，也不会有百分百安全的软件。

那么，系统漏洞和应用软件漏洞有什么不一样？要弄明白这一点，需要先搞清楚软件的分类。在电脑软件中，软件可以分为系统软件和应用软件两大类。所谓应用软件（俗称“应用程序”），是指专门为解决各类实际问题而开发的程序，比如，Word 可以提供文字编辑功能，WinRAR 可以提供压缩与解压缩功能，迅雷可以帮助用户从网络中高速下载软件，等等。

那么，如 Windows XP/2003、Vista 之类的操作系统是应用软件吗？答案是：NO！这是因为 Windows XP/2003、Vista 是属于“系统软件”类。一台没有安装软件的电脑通常被称之为“裸机”，裸机需要安装操作系统来运行。操作系统可以完成一系列底层硬件的基本调度，以及提供一些基本功能，例如，开机与关机功能、电影与音乐的播放、文字输入与打印，等等。

但是，由于这些功能都比较简单，所以很多时候为了满足更多的需求，我们就需要为电脑安装一些专业的应用程序来协助工作。例如，由于Vista中的文本编辑功能只支持简单的文本编辑，所以，可以通过安装专业的文本编辑软件Word来完成复杂的文档编辑。

通过裸机、操作系统和应用程序形成的三层结构，就可以实现电脑中各种各样的功能调用了，如图1-13所示。

图1-13 硬件、操作系统与应用软件的结构

显然，裸机是操作系统的平台，而操作系统则可以看成是应用软件的平台。其中，应用程序处于最上端，它离开了操作系统和裸机将无法使用。这就好比演员与舞台的关系，演员必须在平稳的舞台上才能表演，而应用程序也必须在稳定的操作系统中才能执行安装和运行。

通常，在购买个人电脑时第一件要做的事情就是安装Windows XP、Vista等操作系统。操作系统是所有软件中最重要的组成部分，它为软件与硬件之间“搭”起了一座交流的“桥”。作为电脑中的软件平台，黑客工具和安全软件都需要操作系统的支持才能运行。

系统漏洞与软件漏洞通常互相影响，例如，系统出现了漏洞，黑客并籍此控制了电脑，那么电脑中的一切应用软件的控制权自然也就拱手送人。

1.2 认识黑客

在这个瞬息万变的效率时代，我们与高科技产物——电脑的接触越来越多，在电脑为我们带来高效运作的同时，无所不在的黑客也同时带来了大量的安全隐患。

什么是黑客？首先要说的是，黑客（Hacker）技术其实是网络安全技术的一部分，是一种从操作系统安全分析的角度进行系统完善的技术。所以，从正面来看可以认为黑客就是研究网络安全技术的一个技术群体，他们大多都是程序员出身，对于操作系统和编程语言都有着深刻的认识，乐于探索操作系统的奥秘且善于通过探索了解系统中的漏洞及其原因所在，他们恪守这样一条准则：“Never damage any system”（永不破坏任何系统）。他们近乎疯狂地钻研更深入的电脑系统知识并乐于与他人共享成果，他们一度是电脑发展史上的英雄，为推动计算机的发展起了重要的作用。例如，Linux就得益于很多黑客的不懈努力才有了今天的成就。

显然，“黑客”一词原来并没有丝毫的贬义成分。直到后来，少数怀着不良企图的人，他们技术或许很好，也可能只是对技术一知半解，他们专以非法侵入他人网站、恶意破坏电脑中的数据为乐。这类群体就是被人们所了解、所警惕的“Cracker”一族，也就是“骇客”技术。本书中如果有“防范黑客破坏”等用语，其实指的就是这类伪黑客，并非是针对专心研究网络安全技术的黑客而言。

1.3 认识病毒

在网络中，网管员每天都可能与之打交道的安全隐患有三种，即：病毒、木马和恶意代码。对于网管员来说，病毒是头号大敌！病毒（Virus）是六亲不认的，不论是谁都有可能“与毒共舞”。如果是电脑不巧碰上了病毒（这种机会基本上是人人有份，决不落空），用户通常就会手忙脚乱，不知所措。国内用户认识病毒大多始于1989年初“大连市统计局的计算机上发现有小球计算机病毒”的报道，如图1-14所示。从此以后，计算机病毒以极其迅猛之势在中国大陆蔓延。

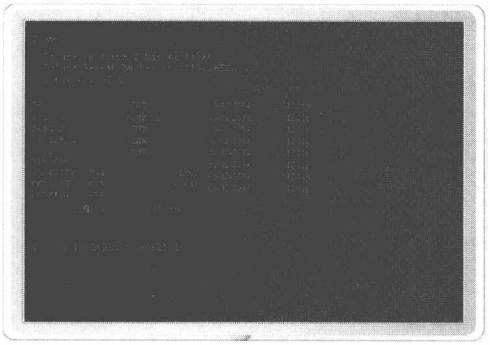
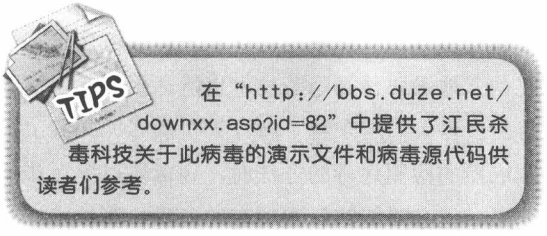


图1-14 小球病毒演示



那时，大家都在使用 DOS 操作系统（“DISK Operation System”，中文译为“磁盘操作系统”）。由于杀毒软件尚未普及，造成了小球等病毒的大量传播。后来，又有了中央电视台都报道过的 CIH，使得全国计算机用户都对病毒有了一定的了解。

1.3.1 病毒能做什么

病毒究竟是什么？其实病毒也是一种软件（程序），只不过它的功能是搞破坏罢了。那么，为什么称其为病毒？首先，它与医学上的“病毒”有着本质的区别，它不是天然存在的，而是某些计算机程序员利用计算机软、硬件所固有的脆弱性，编写的具有特殊功能的程序。由于它与生物医学上的“病毒”同样有传染和破坏的特性，因此这一名词是由生物医学上的“病毒”概念引申而来。病毒一旦进入计算机并得以执行，它会搜寻符合其传染条件的程序或存储介质，确定目标后再将自身插入其中，达到自我繁殖的目的。

那么，病毒究竟能做什么呢？下面，列举了病毒常会去完成的“任务”：

（1）大量占用磁盘的可用空间。

（2）大量占用 CPU 和内存的可用资源。

（3）让系统发出其特定的声音和显示特定的图像等。

（4）让 Windows 无法启用或是正常使用。

（5）疯狂删除系统及各类文件，让系统崩溃或让用户丢失重要数据。

（6）传播自身或其他病毒。

（7）盗取用户账号及密码等信息。

（8）破坏硬件，如大名鼎鼎的 CIH 病毒。

（9）将杀毒软件破坏掉，以便让黑客程序进驻。

（10）恶意修改用户的各种设置，如 IE、注册表……

显然，病毒能做的事儿还真就不少。其实，病毒并不可怕——只要我们肯练好查毒和杀毒的“基本功”，就一定能将病毒赶出系统。当然，只要感染了病毒，或多或少系统都会有点损失，例如，数据被恶意删除、系统文件被恶意更换、IE 和注册表被胡乱修改了等等。所以说，最好不要中毒，一旦中了毒，就别老想着“出病毒而不染”——如果病毒能如此善良，那它也别叫病毒了。

1.3.2 病毒的四个特性

计算机病毒是能够通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活，从而对计算机资源进行破坏的程序或指令集合。它具有四个基本特性，即：破坏性、传染性、潜伏性和隐蔽性。

1.破坏性

80% 以上的病毒具有破坏性，例如，可以自动格式化硬盘、删除系统核心文件等等。象 CIH 等病毒还可以对硬件进行影响，所以，与病毒打交道，要以预防为主，杀除为辅。因为有些文件一旦被感染，就不能再轻易地恢复了，通常只能

使用新的文件进行替换。

例如，“熊猫烧香”等病毒可以终止大量的反病毒软件和防火墙软件进程，会强行删除扩展名为“gho”的文件，使用户无法使用 Ghost 软件恢复操作系统。

2.传染性

98% 以上的病毒具有传染性，如臭名昭著的 Funlove 、熊猫烧香病毒就会瞬间感染系统中所有符合感染条件的文件，在如图 1-15 所示中可以看到感染了“兔宝宝”病毒后，所有的 exe 文件图标就会都变成兔子图标。

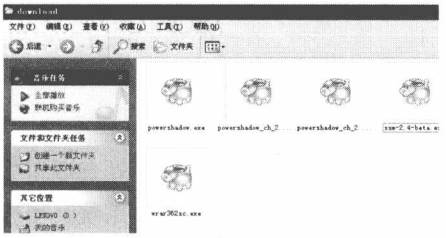


图1-15 感染“兔宝宝”病毒后

病毒具有“传染性”，这意味着它只要有机会就会到处进行传播。是否具传染性，是判别一个程序是否为病毒的最重要条件。

3.潜伏性

“潜伏性”也是病毒的基本特性之一，目的就是让人们不易发现它。我们可以将其视为“定时炸弹”，因为病毒随时都可能因为某个条件被满足而爆发——病毒使用的触发条件主要有以下三种：一是利用主板上的时钟提供的时间作为触发器，这种触发条件被许多病毒采用，触发的时间有的精确到百分之几秒，有的则只区分年份。二是利用病毒自带的计数器作为触发器，病毒利用计数器记录某种事件发生的次数，一旦计数器达到某一设定的值，就执行破坏操作。三是利用计算机内执行的某些特定操作作为触发器，特定操作可以是用户按下某种特定的组合键，也可以是执行格式化命令，或是读写磁盘的某些扇区，等等。

有些病毒还可能会悄悄地在系统中发生作用，只是我们很少会轻易地觉察到。例如，有的木马病毒会先把杀毒软件 KILL 了，让其表面上还处于运行状态，实际上已经不起作用，进而满足“潜伏”的需求。

4.隐蔽性

计算机病毒刚刚开始出现时，由于人们对这种新生事物的认识不足，所以，计算机病毒不需要刻意地采取什么隐蔽技术也能达到广泛传播的目的。当人们越来越了解计算机病毒，并有了一套成熟的检测病毒的方法时，病毒要想广泛传播开来，就必需能够躲避现有的病毒检测技术，以便不被人们发现。例如，弹出一个图片让你欣赏时，病毒在悄悄传播。不经过程序代码分析或计算机病毒代码扫描，病毒程序与正常程序是不容易被区分的。

通常，在遇到上述的这些情况时，不管杀毒软件是否报警，都要警惕系统中是否有病毒在运作。

不驻留内存的病毒是一种立即传染的病毒，每执行一次带毒程序，就主动在当前路径中搜索，查到满足要求的可执行文件即进行传染。该类病毒不改动系统的任何状态，因而很难区分当前运行的是一个病毒还是一个正常的程序。驻留型病毒的不同在于它常驻在内存中，它先窃取系统控制权，接着等待系统运行其他程序时进行感染。

设计完善的病毒往往会很好地隐蔽自己，从而可以争取较长的存活期并造成大面积的感染、造成大面积的伤害。例如，有的使用汇编语言编写的大型病毒仅仅只有 2KB 不到，这使得它更容易地在硬盘等存储介质、内存中隐藏自己，甚至