电脑报 总策划

黑客攻防36计

谋略·技巧篇

生死博弈

王勇 徐杰 仲治国 编著

揭秘36计经典谋略 黑客攻防完全精通

外面的世界很无奈
狙击IE恶意插件
黑暗中的眼睛
免杀木马打造与防范
伸过你的网络我的手
远程控制任我行
黑客攻击前奏曲
手把手教你玩转扫描入侵
局域网中的猎犬
让嗅探入侵更彻底
动态中的秘密
ASP网站攻防经典案例剖析
旁门左道玩系统入侵
DLL攻击与防范详解
揭开无线入侵的面纱
无线网络安全攻防

精彩光盘

- 正版软件超值赠送
- 漏洞扫描工具
- 木马防范工具
- 数据加密工具
- 系统优化工具
- 黑客攻防技法电子书

电脑报电子音像出版社
CPCW Electronic & Audiovisual Press

黑白攻防36计

谋略·技巧篇

生死博弈

王勇 徐杰 仲治国 编著

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

内容提要

黑客强敌诡计多端，安全防范刻不容缓。本手册专门为黑客攻防与网络安全爱好者量身定制，剖析与黑客斗智斗勇的36个经典案例，以提供安全防范有效技法和措施。手册内容涵盖IE恶意插件、免杀木马打造与防范、远程控制、扫描入侵、嗅探入侵、ASP网站攻防、DLL攻击与防范、Cookie漏洞、无线网络安全、手机入侵与防范等领域，全面解析黑客攻击过程，详尽介绍防范操作步骤，帮助你快速掌握黑客攻防的谋略与技巧，提高安全防护能力。

光盘要目

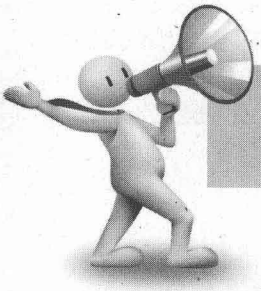
- 《可牛杀毒软件》电脑报专用版
- 漏洞扫描工具
- 木马防范工具
- 数据加密工具
- 系统优化工具
- 黑客攻防技法精选电子书

声明：使用网络技术攻击他人计算机属于违法行为，读者切勿用本手册内容对他人计算机进行恶意攻击，否则后果自负！

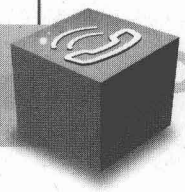
黑客攻防36计

编　　者：王　勇　徐　杰　仲治国
责任编辑：马　声
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：四川省蓥山数码科技有限公司
文本印刷：重庆科情印务有限公司
开本规格：787mm×1092mm 1/16　18印张　300千字
版　　号：ISBN 978-7-89476-481-2
版　　次：2010年10月第1版 2010年10月第1次印刷
定　　价：35.00元(1CD+手册)

前言



揭秘黑客谋略与兵器精髓



这是一套全面指导黑客入门与实战的黑客图书
这是一套深刻解析攻防工具及应用的黑客图书
这是一套完全精通攻防谋略与技巧案例的黑客图书

网络就是战场、安全就是用兵。

战场上硝烟弥漫，鲜血迸溅；网络中针锋相对，明争暗斗！

黑客世界的刀光剑影总让人感到神秘莫测。

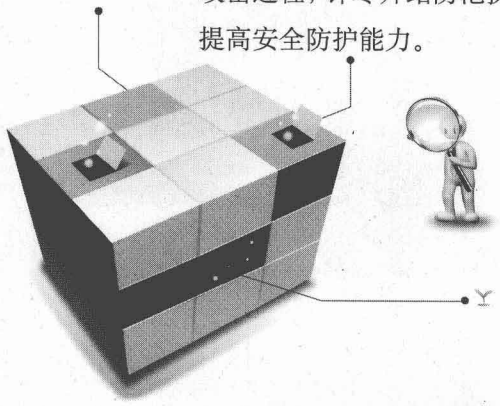
正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

一名技艺高超的黑客无非体现在以下三方面：其一是掌握常见的黑客攻防手法，其二是娴熟的黑客工具应用，其三是独到的谋略技巧施展。本系列图书正是围绕以上三方面的黑客攻防必备技能为读者全面展开并详细解读。

《黑客入门与成长秘技 108 招》：通过 108 招攻防技巧，由浅入深地为大家讲解了黑客成长必备的技能，让大家快速步入黑客之门。

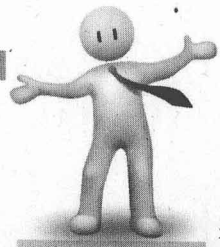
《黑客 88 种兵器全解析》：精选了黑客最常用的 88 种攻防工具，通过工具的实战操作帮助读者快速领悟黑客攻防手段。

《黑客攻防 36 计》：剖析了与黑客斗智斗勇的 36 个实战案例，全面解析黑客攻击过程，详尽介绍防范操作步骤，帮助你快速掌握黑客攻防的深度谋略与技巧，提高安全防护能力。



编 者

2010 年 9 月



光盘精彩导航

实用功能

本光盘可自启动电脑，并进入 Windows PE 系统，进行系统维护、杀毒等。还可通过 Ghost 软件进行系统一键备份，系统还原等操作。该光盘功能完善、实用，是你维护电脑的随身宝典。

数据加密工具

360保险箱
Dr.Web CureIT
超级巡警账号保护神
金山密保
网游保镖
账号保险箱

系统优化工具

360网吧还原系统保护器
pcAnywhere
quickip8.3
UltraVNC
WinVNC
波尔远程控制
美萍网管大师10.1
网吧管理助手
网络人(Netman) V5.30
网维大师icafe

漏洞扫描工具

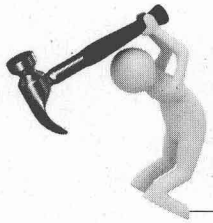
ESET NOD32安全套装
Microsoft Baseline Security Analyzer
Windows系统漏洞扫描专家
超级巡警漏洞检测
光华系统漏洞修护工具
卡巴斯基病毒清除工具

木马防范工具

360恶意网站屏蔽器
360时间保护器
360文件粉碎工具
360系统诊断工具
Norman_Malware_Cleaner
U盘免疫器V1.5
超级巡警文件删除工具
超级巡警之机器狗专杀
肉鸡检测器
网络保镖

黑客攻防技法精选电子书

第1计 启动有“礼”——让小菜都能轻松发现安全隐患
第2计 寻找李鬼——进程打黑轻松行
第3计 外面的世界很无奈——浏览器的攻防
第4计 菜鸟的QQ自卫反击战——QQ及相关服务攻防
第5计 见招拆招——网吧入侵与防范
第6计 黑暗中的眼睛——木马原理与攻击防范
第7计 风光暗箭——用0day漏洞入侵PHP网站Webshell
第8计 XP密码连连看——系统密码破解全攻略
第9计 伸过你的网络我的手——远程控制任我行
第10计 速度与激情——巧用IIS 6.0漏洞入侵网站
第11计 攻击前奏曲——手把手教你玩转入侵检测
第12计 局域网中的猎犬——让嗅探入侵更彻底
第13计 动态中的秘密——网站挂马经典案例剖析
第14计 入侵中的旁门左道——DLL攻击与防范详解
……



目录 CONTENTS

生死博弈
黑客攻防36计

第1计 启动有“礼” 让小菜也能查隐患

第2计 寻找李鬼 进程打黑轻松行

第3计 外面的世界很无奈 浏览器的攻防

第4计 菜鸟的自卫反击战 QQ及相关服务攻防

第5计 见招拆招 网吧入侵与防范

第6计 黑暗中的眼睛 木马原理与攻击防范

第7计 风光暗箭 用0day漏洞入侵PHP网站

第8计 XP密码连连看 系统密码破解全攻略

第9计 伸过你的网络我的手 远程控制任我行

第10计 速度与激情 巧用IIS 6.0漏洞入侵网站

第11计 攻击前奏曲 教你玩转入侵检测

第12计 局域网中的猎犬 让嗅探入侵更彻底

第13计 动态中的秘密 网站挂马案例剖析

第14计 入侵中的旁门左道 DLL攻击与防范详解

第19计 揭开无线入侵的面纱 无线网络安全攻防

第20计 直击核心 数据库攻防

第21计 脚本漏洞的秘密 透过脚本玩入侵

第22计 黑客焦点 手机入侵与防范

第23计 开源系统攻防 Linux入侵与防范

第24计 突破的魅力 软件破解绕开限制

第25计 致命一击 注册表入侵与防范

第26计 桌面系统秒杀 Windows XP与Vista攻防

第27计 千防万护总难全 服务器入侵与防范

第28计 浅探设备攻防 网络交换设备的安全配置

第33计 密码风云 加密与解密

第34计 网络暴力 拒绝服务攻击

第35计 城门失火 殃及池鱼 常用工具也防黑

第36计 快乐身后的杀手 游戏攻击与防范

第1计 启动有“礼” 让小菜也能查隐患

很多恶意程序都会很不客气地加入到系统的启动项中，进而导致了系统变慢、数据被窃取等问题涌现。那么，这些恶意程序都是怎样成为启动项目的？怎样才能把这些不懂礼貌的家伙赶出去？在本谋略中，将为读者们剖析 Windows 中的启动安全配置策略。

一、要搞破坏很简单

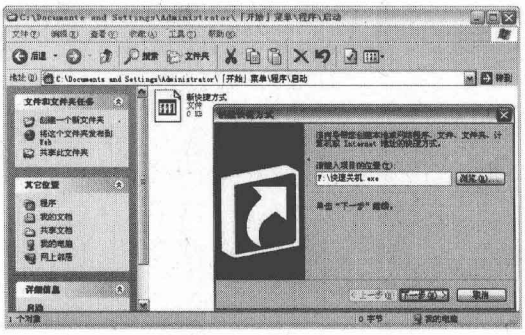
我们经常会遇到木马等不请自来的恶意程序，这些恶意程序都是如何在系统中搞破坏的？最方便的方法就是在系统启动时由系统进行调用。这样，每次系统运行后，恶意程序就会自动“接管”系统或悄悄地进行破坏。比方说，有的木马可以在系统启动过程中自动把安装的杀毒软件禁用掉。也就是说，可以对系统调用杀毒软件这个过程加以破坏，一旦杀毒软件无法使用，系统的安全性无疑则是雪上加霜。

下面，让我们来做一个测试，这个测试将实现的效果是：将恶意程序添加到“开始”→“程序”→“启动”中，在重启动系统并进入桌面后，系统将会在数秒内自动关机。

为了方便测试，需要先在“http://hshy9.ys168.com”或“http://e.ys168.com/?hshy9”的“测试程序”目录中下载“快速关机 .exe”这个可执行文件。接着，假设当前登录的账户名为 Administrator，那么，需要依次执行如下操作：

在资源管理器窗口中打开“X:\Documents and Settings\Administrator\「开始」菜单\程序\启动”（X：是指 Windows 目录所在分区）文件夹，在右侧窗格中单击鼠标右键，并在弹出的右键菜单中依次选择“新建”→“快捷方式”项。

在自动弹出的“创建快捷方式”对话框中，单击“浏览”按钮把下载的“快速关机 .exe”添加进来。



添加程序

单击“下一步”按钮，在出现对话框时，单击“完成”按钮结束快捷方式的创建。

依次单击“开始”→“程序”→“启动”，在展开的菜单中可以看到添加的程序。

现在，就可以重启系统并在重新进入桌面数秒后，在无任何提示（包括不显示关机界面）的状态自动关机了。显然，在启动项目中如果存在一些恶意程序的话，对于毫无排除经验的电脑用户来说，就会是一个较大的麻烦。

其实，要解决这个问题也是非常容易的，我们至少可以使用三种方法来解决问题：

方法一：在进入桌面后快速打开资源管理器窗口，并依次进入“X:\Documents and Settings\Administrator\「开始」菜单\程序\启动”文件夹，将其中恶意程序对应的快捷方式删除即可。

方法可行性程度：低。原因：操作所需要时间往往超过加载启动程序的时间。

方法二：在启动时当 Windows XP 滚动条界面消失时，立即按下 Shift 键不放直至系统桌面和右下角的系统托盘图标均出现为止，这样，也可以阻止启动项自动运行。

方法可行性程度：中。原因：容易忘记。

方法三：如果根本没时间进入“X:\Documents and Settings\Administrator\「开始」菜单\程序\启动”文件夹，那么可以使用 WinPE 启动光盘进入系统，即可轻松删除此文件夹下的任意文件。

方法可行性程度：高。原因：几乎无限制。

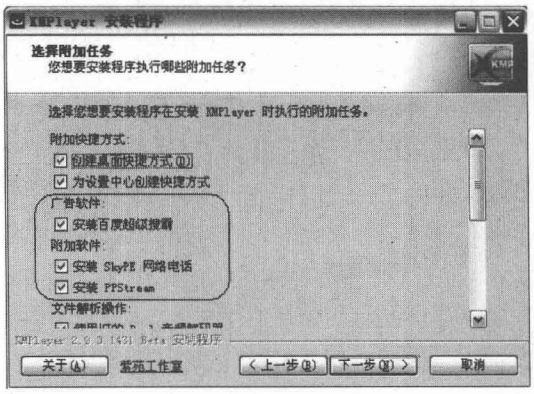
二、黑客会怎么做？

除非已经明确判断目标用户在安全技术掌握程度上是“菜鸟”级别，否则黑客通常不会使用上述的“入门”级启动项目添加方法，因为太容易被有经验的电脑用户发现和清除了，他们通常会使用如下两种比较隐蔽的方法：

1. 在注册表中添加

对于没有丰富经验的电脑用户来说，注册表的内容总是让人看得眼花缭乱，更别说还要从中找到恶意程序的藏身之所了。所以，在注册表中进行启动项目的添加显得较为“安全”。

向注册表的启动项中添加恶意程序的方法有很多种，但效果最好、使用量最大的方法还是通过在应用程序中内挂恶意程序来实现。

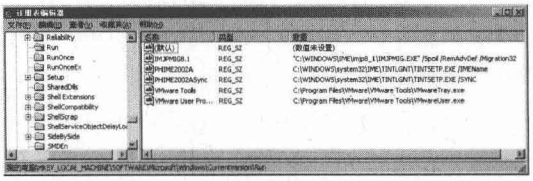


内置恶意插件

通过在应用程序中捆绑恶意程序，可以非常容易地在系统中实现恶意代码的植入，如篡改注册表的启动项，等等。由于杀毒软件在用户允许应用程序安装后，通常不会再进行深入干涉，所以，这样的恶意代码植入显得防不胜防。

在使用“Regedit”命令打开“注册表编辑器”窗口后，其中主要的启动分支包括如下几个：

* 在[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]和[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]中均可以添加启动项。



启动项

* 在[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]和[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]项下，也可以添加启动项。如果没有 Explorer 和 Run 项，可以自行添加。

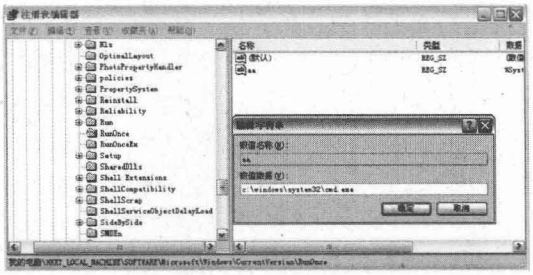
* 在[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]和[HKEY_LOCAL_MACHINE\Software\

Microsoft\Windows\CurrentVersion\RunOnce]项中可以添加只执行一次的程序，而RUN项下的程序则会在每次系统启动时都执行一次。

针对Run和RunOnce项中的键值，Windows XP的处理原则是：

首先，在以安全模式登录系统时会忽略Run和RunOnce项。但RunOnce项下的键值，可以通过在键值名称前添加一个星号（*），强制安全模式下也运行。

其次，RunOnce项中的程序运行后，对应的键值就会被删除。在删除方式上，可以使用如下两种方法：一是将感叹号（!）添加到RunOnce项中的键值名称前，这样对该键值的删除操作将延迟到程序（或命令）运行之后执行；二是如果没有感叹号作为前缀，键值将会在运行命令之前即被删除，如图7所示。



属性

如果某个键值没有正确地运行，则下一次系统启动时就不会要求运行对应的程序，所以说它是一次性的。

将如下代码保存为任意名称的reg文件并双击，在向系统中写入后，即可在RunOnce中添加一个启动项目，它的调用程序为“cmd.exe”（命令提示符）。

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce]
"zhong"="c:\\windows\\system32\\cmd.exe"
```

在重启系统并在出现桌面图标之前就会自动运行cmd.exe程序，并直至用户关闭此程序后，才会出现桌面图标。试想，如果我们运行的是一个伪装巧妙的恶意程序，系统将会遭受怎样的麻烦。

提示 ATTENTION

如果不想书写此代码，可以至“http:// hshy9.ys168.com/”或“http://e.ys168.com/?hshy9”的“测试程序”目录中下载“开机时只执行一次.reg”文件直接使用源代码。

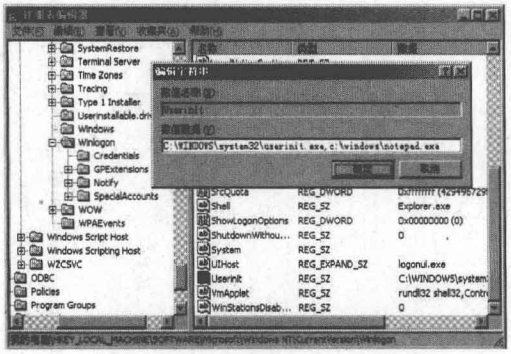
* [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]和[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]中的程序会在用户登录之前及其他注册表的启动项加载前“潜在”、自动执行一次。

* [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]和[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices]中的加载项，是继RunServicesOnce之后启动的程序。

* [HKEY_CURRENT_USER\\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]和[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx]是Windows XP/2003特有的自启动注册表项。

* [HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CRRENTVERSION\WINLOGON]项中，双击打开Userinit键值，其默认“数值数据”为“C:\WINDOWS\system32\userinit.exe,”，在半角逗号后面可以添加一个或多个要执行的程序，如图所示中添加的“c:\windows\notepad.exe”表示要调用“记事本”程序，这个键值会随着系统

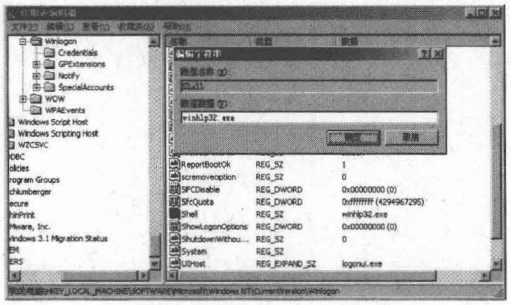
启动而每次自动执行。



注册表

* [HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows] 项中，设置 load 键的值为任意程序即可，这里的“C:\WINDOWS\system32\cmd.exe”表示启动 cmd.exe 这个文件。

* [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] 项中的 Shell 键，其值默认是 Explorer.exe。如果恶意程序将其更改为自身，那么在启动 Windows XP 时，桌面环境将不再出现，而是只出现恶意程序的运行界面。



键值

如果希望既出现桌面环境，又能运行恶意程序，那么只需将值改为“Explorer.exe %WINDIR%\System32\cmd.exe”这种形式就可以了。

要解决这个问题，只需按下“Ctrl+Alt+Delete”键打开“Windows 任务管理器”，并依次单击“文件”→“新建任务（运行…）”菜单。

在弹出的“创建新任务”对话框中输入“Regedit”，在打开“注册表编辑器”窗口后，再将 Shell 键的值更改为“Explorer.exe”即可。

* [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler] 和 [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad] 项中，可以添加后缀名为 dll 的木马程序。

2. 在计划任务中添加

我们来模拟一个场景，黑客在入侵一台目标计算机后，希望目标计算机每次启动时都能自动执行植入的远程控制程序（通常为木马）服务端，特别是使用动态 IP 的目标用户，也许这次碰巧入侵成功了，下次就再没机会遇到了。让目标计算机能每次启动时，都自动联系黑客。那么，这种需求该怎么满足？答案之一就是使用计划任务功能！

所谓“计划任务”，就是指在指定的时间、在指定的计算机系统中，由指定的账户运行指定的程序。使用计划任务的优势在于：可以自动定时运行，程序执行具有不容易被人发现的特点。

黑客针对目标计算机执行的计划任务都是使用 DOS 命令实现的。下面，以几个实例讲解一下远程进行计划任务制订、列出和取消的方法。

（1）制订远程计算机计划

通常，黑客在登录目标计算机后，就会在目标计算机中创建执行木马等程序的计划。也就是说，要在目标计算机中执行计划任务相关的操作，前提就是获得相应的操作权限，如管理员账户。

假设，现在需要让 192.168.1.8 这台远程计算机在 9:00 执行“srv.exe”这个程序，那么需要执行如下操作：

步骤 1

使用“CMD”命令打开“命令提示符”窗口。

步骤 2

输入命令“Net use \\192.168.1.8 /user:"administrator" 780316”，这里的 administrator 是账户名，780316 是密码。它们用于登录到 192.168.1.8，192.168.1.8 中必须事先有这个账