

黑客攻防36计

谋略·技巧篇

王勇 徐杰 仲治国 编著

生死博弈



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

DDoS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

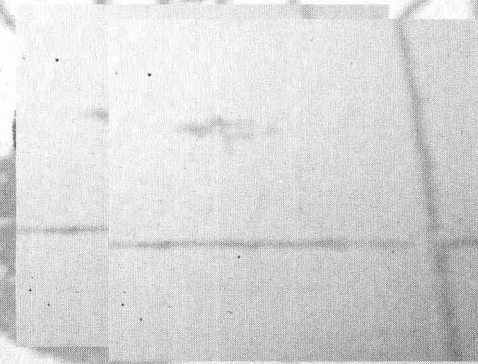
黑 夜 攻 防 36 计

谋略·技巧篇

王勇徐杰仲治国编著

生死
博弈

TP393.08
W432



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

- 《牛牛杀毒软件》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

版权所有 盗版必究

未经许可 不得以任何形式和手段复制和抄袭

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

C D 生产：四川省釜山数码科技有限公司

文本印刷：重庆科情印务有限公司

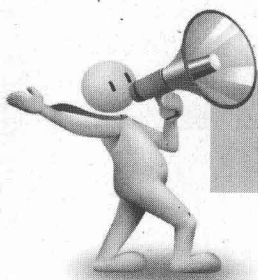
开本规格：787mm×1092mm 1/16 18印张 300千字

版号：ISBN 978-7-89476-481-2

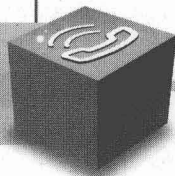
版次：2010年10月第1版 2010年10月第1次印刷

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。

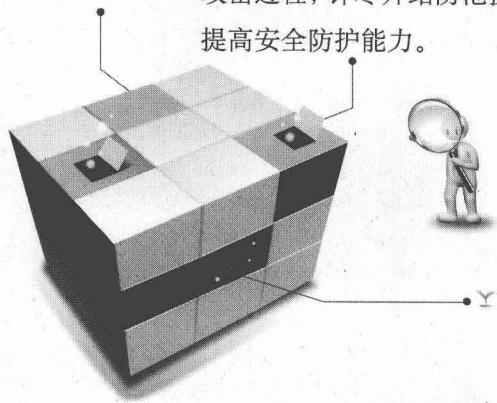
正所谓兵来将挡，水来土掩。只要我们抱着“勿恃敌之不来，恃吾有以待之”的精神，必能将各种危机化解于无形！熟读兵书三百遍，不会用兵也能防。

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。

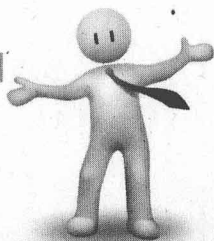
《黑客入门与成长秘技 108 招》：通过 108 招攻防技巧，由浅入深地为大家讲解了黑客成长必备的技能，让大家快速步入黑客之门。

《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

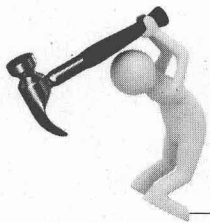
- ESET NOD32安全套装
- Microsoft Baseline Security Analyzer
- Windows系统漏洞扫描专家
- 超级巡警漏洞检测
- 光华系统漏洞修补工具
- 卡巴斯基病毒清除工具

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Oday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

- 一、要搞破坏很简单.....001
- 二、黑客会怎么做?.....002
 - 1. 在注册表中添加.....002
 - 2. 在计划任务中添加.....004
- 三、如何禁止恶意启动项运行?.....006
 - 1. 系统配置实用程序.....006
 - 2. 组策略管理器.....007
 - 3. 使用专业的管理程序.....009

第2计

寻找李鬼 进程打黑轻松行

- 一、进/线程是干什么的?.....011
- 二、分析、关闭和重建进程.....014
- 三、杀死黑客植入的隐藏进程.....015
- 四、黑客是如何查看远程进程的.....016
- 五、如何杀死病毒进程.....016
- 六、删除发起进程的恶意程序.....019
- 七、查看木马进程对应的服务.....019
- 八、进程的高级管理.....020

第3计

外面的世界很无奈 浏览器的攻防

- 一、IE攻防.....022
- 二、0Day漏洞攻防.....022
 - 1. 漏洞简介.....022
 - 2. 漏洞利用代码实测.....023
 - 3. 木马的利用.....023
 - 4. 漏洞的防范.....024
- 三、常见的篡改恢复.....024
 - 1. 注册表编辑器被锁定.....024
 - 2. 禁止修改IE主页.....024
 - 3. 禁止查看“源文件”.....025
 - 4. 修复IE标题栏.....025
 - 5. 修复IE几个重要的URL.....025
 - 6. 修复IE右键菜单.....026
 - 7. 删除工具栏上多余的按钮.....026
 - 8. 疯狂打开窗口.....026
- 四、恶意插件攻防.....026
 - 1. IE的“插件”有什么用?.....026
 - 2. 插件是如何绑架IE的.....027
 - 3. 解救IE.....027

第4计

菜鸟的自卫反击战 QQ及相关服务攻防

- 一、黑客为什么喜欢QQ.....029

二、本地盗号实战	030
三、QQ登录保护	031
1. nProtect技术与破解	031
2. 登录环境选择	032
3. 使用密保卡	033
四、聊天记录防范	034
五、强行聊天防范	035
六、恶意链接防范	036
七、木马的查杀	038
八、加密相册破解实战	039

第5计

见招拆招 网吧入侵与防范

一、剖析网吧安全环境	040
1. 安全问题一览	040
2. 初识防护技术	041
二、突破网吧限制	042
1. 手工突破限制	042
2. 利用工具破解	043
三、网络攻击与防范	044
1. 局域网攻击原理	044
2. 局域网终结者	045
四、溢出入侵网吧主机	046
五、网吧之安全上网	047

第6计

黑暗中的眼睛 木马原理与攻击防范

一、创建“沙盘”	048
二、木马入侵原理	049

1. 修改图标	050
2. 捆绑文件	050
3. 定制端口	051
4. 文件夹惯性点击	051
5. 下载欺骗	051

三、木马使用 051

1. Xrat木马实战	051
2. 灰鸽子	052
3. Wolf木马	053

四、免杀木马 055

五、轻松测试EXE文件 056

第7计

风光暗箭 用0day漏洞入侵PHP网站

一、搭建测试环境	057
1. 配置PHP支持环境	057
2. 在IIS中启用PHP的支持	058
二、提供MySQL支持	060
三、安装PHPCMS	061
四、入侵与防范	062

第8计

XP密码连连看 系统密码破解全攻略

一、初识系统密码	064
二、密码是如何被攻破的?	066
三、恢复、重设和清除密码	070
1. 密码恢复功能	070
2. 通过ERD Commander重设密码	071
3. 清除密码	072
四、密码的安全管理	072
1. 设置密码的最小长度	072

- 2. 设置密码的复杂性要求 073
- 3. 强制不能再用旧密码 073

第9计

伸过你的网络我的手 远程控制任我行

- 一、远程控制概述 074
- 二、多用户远程桌面 075
- 三、PsTools实战 077
 - 1. 远程登录 078
 - 2. 执行命令 079
 - 3. 传送文件并执行 079
 - 4. 执行远程命令并显示 079
 - 5. 查看远程进程并杀除 080
 - 6. 查看硬盘空间 081
 - 7. 关闭服务 081
 - 8. 检查远程机是否有木马 082

第10计

速度与激情 巧用IIS 6.0漏洞入侵网站

- 一、网站与服务器概述 083
- 二、利用漏洞入侵论坛 085
- 三、利用漏洞制作私密网站 087

第11计

攻击前奏曲 教你玩转入侵检测

- 一、知己知彼，百战不殆 092
 - 1. 入侵的定义 092
 - 2. 入侵检测的起点 093
 - 3. 入侵检测基本模型 093
 - 4. 按照信息源的分类 094

二、用X-Scan扫描目标主机 094

三、用IIS Lock Tool扫描服务器 095

四、防患于未然 097

- 1. 端口防范 097
- 2. 安装补丁 099

第12计

局域网中的猎犬 让嗅探入侵更彻底

- 一、嗅探原理概述 100
- 二、邮箱监听实战 102
- 三、多协议监听实战 103
- 四、影音嗅探 104
- 五、网管对嗅探的利用 104
- 六、怎样防御监听 106

第13计

动态中的秘密 网站挂马案例剖析

- 一、网站挂马概述 107
- 二、使用工具批量挂马 108
- 三、为网站模板添加一句话木马 109
- 四、检测是否被挂马 111
- 五、申请安全厂商来保护 112
- 六、防患于未然 112

第14计

入侵中的旁门左道 DLL攻击与防范详解

- 一、DLL文件概述 113

二、DLL木马制作实战 114

三、玩转DLL注入进程 116

四、查找和分析DLL木马文件 116

- 1. 通过文件对比找出DLL木马 117
- 2. 通过端口监控找出DLL木马 117
- 3. 快速判断是否为系统DLL文件 118
- 4. 查看调用DLL模块文件的进程列表 118

五、如何消灭DLL木马 118

第15计

捕风捉影
让日志成为安全管理好助手

一、日志概述 120

- 1. 修改系统日志存放路径 120
- 2. 修改安全日志存放路径 121

二、安全日志的启用 123

三、四项基本技能 124

- 1. 事件筛选 124
- 2. 查找记录 124
- 3. 排序事件 125
- 4. 新建查看 125

四、清除与保存日志 125

- 1. 本地清除 125
- 2. 保存日志 125
- 3. 远程清除 126
- 4. 清除IIS日志 126

五、远程管理日志 127

第16计

一起来入侵论坛
主流论坛攻防实战

一、Discuz 7.X入侵与防范 128

二、轻松暴库动网 130

三、终极注入PHPWind 131

四、BBSXP数据库挂马 132

第17计

剑走偏锋
巧用Cookies漏洞实现网站提权

一、Cookies概述 135

二、查看网站写入内容 136

三、Cookies欺骗实战 136

四、自己分析Cookies漏洞 137

第18计

快慢瞬间
与病毒厮杀的岁月

一、如何防止中毒? 140

- 1. 安装杀毒软件 140
- 2. 了解最新“毒报” 141
- 3. 主动防御和自我保护 141

二、感染病毒后该怎么做? 141

- 1. 基本设置 142
- 2. 提取病毒扫描日志 142

三、如何有效杀毒 143

- 1. 使用专业工具 143
- 2. 使用WinPE 144
- 3. 搜索解决方法 145

四、轻松制作U盘杀毒盘 145

五、“双动力”超强杀毒 可牛免费杀毒软件147

- 1. 又快又狠：“双引擎杀毒”绝不手软 147
- 2. “双杀软模式”：杀毒软件也能和平共处 147
- 3. 超强模式：邮件、网页监控全搞定 148

第19计

揭开无线入侵的面纱 无线网络安全攻防

一、无线概述	149
二、初识无线攻击	150
三、无线探测与第一次入侵	152
四、无线密码破解	152
五、安全配置	155
1. 更改默认设置	155
2. 关闭无线路由	155
3. MAC地址过滤	156
4. 设置强密码	156

第20计

直击核心 数据库攻防

一、数据库是什么	157
二、黑客是如何找到数据库的?	158
三、SQL溢出实战	158
四、SQL弱口令扫描	159
五、SQL 2005注入	160
六、数据库密码暴力猜解	160
七、数据库防范秘技	161
1. 本机中的数据库安全策略	161
2. 购买空间的安全策略	161
3. 奇妙的.ini	162

第21计

脚本漏洞的秘密 透过脚本玩入侵

一、脚本概述	163
--------	-----

二、入侵实战

1. 暴库	164
2. 注入	165
3. 旁注	166

三、安全防范篇

第22计

黑客焦点 手机入侵与防范

一、手机安全概述	169
二、手机骷髅木马	170
三、手机安全软件	171
1. 卡斯基手机安全软件8.0	172
2. 360手机卫士	172
3. 网秦手机安全卫士	173
4. 金山手机安全卫士	173
四、手机安全配置	173

第23计

开源系统攻防 Linux入侵与防范

一、Linux命令初识	175
二、入侵实战	178
三、安全配置	179

第24计

突破的魅力 软件破解绕开限制

一、破解概述	180
二、破解软件使用次数限制	180

三、破解软件使用时限	181
四、破解注册码	184
五、光盘隐藏文件功能的破解	185

第25计 致命一击 注册表入侵与防范

一、知己知彼，百战不殆	186
1. 为什么要保护注册表?	186
2. 注册表的结构	187
二、四项基本技能	189
1. 查找	189
2. 更改属性内容	189
3. 添加与删除	190
4. 重命名	190
三、本地篡改浅析	190
四、利用网页修改注册表	192
五、怎样开启和连接远程注册表服务	192
六、如何进行严密的安全防护	193
1. 关闭远程注册表管理功能	193
2. 禁用注册表编辑器	193
3. 如何彻底恢复注册表	193
4. 恢复注册表的初始化权限设置	194
七、备份注册表的三种方法	194
1. 导入和导出注册表	194
2. 备份或还原向导	195
3. 使用系统还原功能备份	195

第26计 桌面系统秒杀 Windows XP与Vista攻防

一、个人电脑和服务器有什么不同?	196
二、个人电脑“中招”解析	197

三、XP漏洞攻防	198
1. 创建开机脚本	198
2. 效果验证	198
四、Vista漏洞攻防	199
1. 本地提权实战	199
2. 安全防范	200
五、防御架构	200

第27计 千防万护总难全 服务器入侵与防范

一、服务器安全概述	201
二、服务器的漏洞侦测	202
三、MS08-067漏洞攻防	203
1. 攻击原理	203
2. 攻击实战	204
3. 安全防范	205
四、服务器的安全配置	206
1. 安装补丁	206
2. 权限设置	207
3. 删除LAN设置	208

第28计 浅探设备攻防 网络交换设备的安全配置

一、网络交换设备概述	210
1. 集线器	210
2. 交换机	211
3. 路由器	214
二、入侵路由实战	216
三、路由的安全配置	217
1. 登录密码的修改	217
2. 系统配置参数文件存储	217

- 3. 日志管理 218
- 4. 远程管理配置 218

第29计 神来之笔 批处理攻防实战

一、初识批处理 219

- 1. 创建批处理文件 219
- 2. 基本命令 220
- 3. 参数 222

二、批处理实例精华 223

- 1. 批量检测入机存活 223
- 2. 检查是否感染Wolf木马 223
- 3. 操作注册表 223
- 4. 终止进程 224
- 5. 遍历磁盘并删除gho文件 224
- 6. 禁止网络共享 224
- 7. 获取当前的IP和MAC地址 225
- 8. 磁盘映射 225
- 9. 删除默认共享 226

三、其他方面 227

- 1. 黑客帝国数字雨 227
- 2. 批量清除垃圾文件 227
- 3. 配置防火墙“例外”端口 228

第30计 流动的入侵 移动存储攻防

一、可移动存储 229

二、Autorun病毒实战 229

- 1. 原理与分析 230
- 2. 病毒的查找 232
- 3. 病毒的清除 233
- 4. 故障的修复 233

三、病毒的防范 234

四、禁止使用USB设备 235

- 1. 禁止安装USB设备的驱动程序 235
- 2. 禁用USB存储设备 236

五、设置可移动存储设备的权限 236

第31计 来无影去无踪 代理服务器的使用

一、IP、MAC和域名 239

二、获得和追踪IP地址 240

三、隐藏IP地址 241

- 1. 使用代理服务器 241
- 2. 使用代理网站 242

四、使用VPN代理 243

- 1. 内置拨号 243
- 2. 自动搜索VPN代理 244

第32计 不可不学的基础 常用黑客命令

一、命令实例 245

- 1. Arp 245
- 2. AT 246
- 3. Del和RD 246
- 4. Gettype和Systeminfo 247
- 5. Ipconfig 247
- 6. Netstat 248
- 7. Ping 248

二、命令集大成者Net 250

- 1. Net share 250
- 2. Net Start/Stop 251
- 3. Net time 251
- 4. Net use 251

5. Net view	252
6. Net User	252

第33计 密码风云 加密与解密

一、 电脑中的秘密	255
二、 文件的加密与解密	255
1. 内置功能加密	255
2. 使用WinRAR加密	256
三、 破解网络密码	257
1. 破解缓存密码	257
2. 破解共享密码	257
四、 破解Word文档密码	258
1. 创建加密文件	258
2. 使用WordKey解密	258
五、 EFS加密	259

第34计 网络暴力 拒绝服务攻击

一、 攻击原理	260
二、 实战DDoS攻击	261
1. 攻击实例	261
2. 识别DDoS攻击	261
三、 实战CC攻击	262
1. 攻击原理	262
2. 攻击实例	263
3. 识别CC攻击	264
四、 防范与反击	264

1. DDoS攻击防范	264
2. CC攻击防范	265
3. 通用防范要点	267

第35计 城门失火 殃及池鱼 常用工具也防黑

一、 常用工具与漏洞	268
二、 Word黑客攻防	269
1. 漏洞简介	269
2. 攻击实战	269
3. 安全防范	270
三、 EXCEL漏洞攻防	270
1. 漏洞简介	270
2. 入侵实战	271
3. 防范策略	271
四、 Adobe Flash漏洞攻防	271
1. 入侵实战	271
2. 漏洞分析与防范	272
五、 Serv-U入侵攻防	272
1. 准备工作	272
2. 入侵实战	273

第36计 快乐身后的杀手 游戏攻击与防范

一、 游戏安全概述	274
二、 游戏外挂	275
三、 游戏木马查杀	275
四、 游戏密码保护	276



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，在重新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.ysl68.com>”或“<http://e.ysl68.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这个问题：

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？

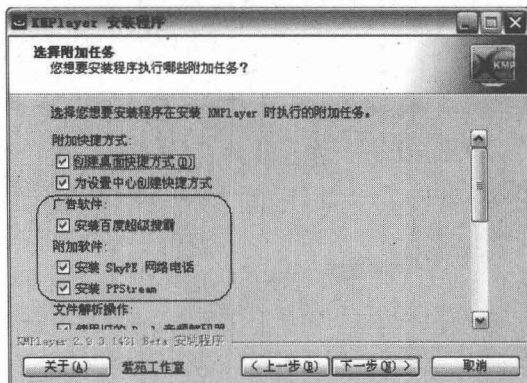
除非已经明确判断目标用户在安全技术掌握程度上是“菜鸟”级别，否则黑客通常不会使用上述的“入门”级启动项目添加方法，因为太容易被有经验的电脑用户发现和清除了，他们通常会使用如下两种比较隐蔽的方法：

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。

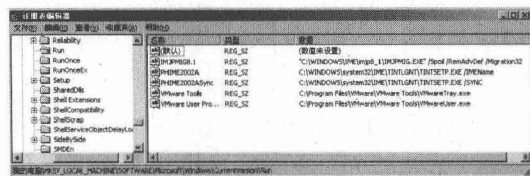


内置恶意插件

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。

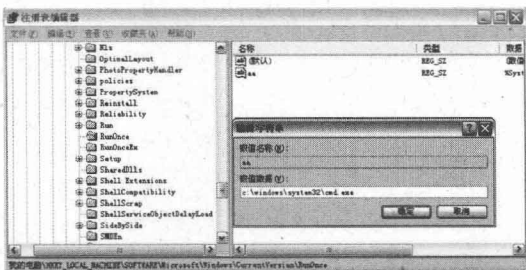
* 在[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]和[HKEY_LOCAL_MACHINE\Software\

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。

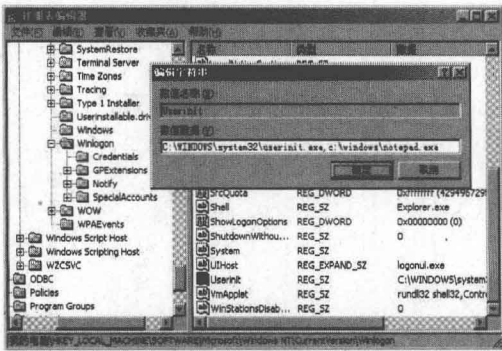
* [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]和[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]中的程序会在用户登录之前及其他注册表的启动项加载前“潜在”、自动执行一次。

* [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\CURRENTVERSION\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

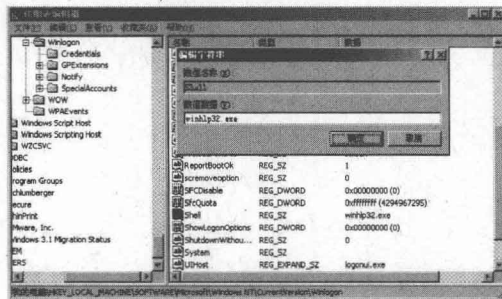
启动而每次自动执行。



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\SharedTask Scheduler] 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