

黑客手抄本

黑客VS网管 大作战

黑客与红客的终极较量！
肖遥 编著

1对1

的情景模式，入侵与反入侵、陷阱攻防战、控制权限的争夺、看似绝不可能完成的VPN漏洞检测……

- ▶ 黑客IP隐藏术与破解
- ▶ 如何探察目标的可用漏洞与防御
- ▶ 入侵之无孔不入与陷阱反击战
- ▶ 如何强制木马植入、运行被黑电脑中的程序
- ▶ 入侵和破坏留下的各种日志如何清理、网管又如何回击

更多触目惊心的颠峰对决

More...

电脑迷 荣誉出品

黑客手抄本

黑客VS网管 大作战

基本书库丛书

2000年三月十九日

肖遥 编著

名 称：黑客VS网管大作战

策 划：彭 葵

编 著：肖 遥

责任编辑：欧阳鹏 孙玮贤

执行编辑：彭 葵

组版编辑：汤 立 邹萍 唐荣曦

封面设计：黄 丹

出版单位：云南出版集团公司 云南科技出版社

技术支持：（023）63658888-13101

邮购热线：（023）63658888-13126

版权所有 盗版必究

未经许可 不得以任何形式和手段复制或抄袭

发 行：重庆中科普传媒发展股份有限公司发行部

电 话：（023）63658888—13138

传 真：（023）63659779

经 销：各地新华书店、报刊亭

光盘生产：四川釜山数码科技文化发展有限公司

文本印刷：重庆升光电力印务有限公司

开本规格：787×1092毫米 正度16开 15印张

版本号：ISBN 978-7-900747-07-5

版 次：2008年7月第1版

定 价：32元（1CD+1手册）

目录



CONTENTS

注：本目录中凡标有  的章节均在光盘中有全程配音的教学视频

第一篇 “洞”网之争，论坛谁作主

攻击回放——遗忘引发的攻击 1

一、勘察踩点 2

二、评论带来的机会 2

加油站：搜索使用动网论坛的站点 3

三、高效的手工注入 4

1. 嗅探数据 4

2. 转换密码 6

3. 修改嗅探数据 7

4. 提交数据 8

加油站：图形化数据提交工具“Httpost” 8

5. 修改后台管理员密码 9

四、工具注入攻击 10

加油站：如何使用工具快速入侵Dvbbs7.1动网论坛 12

防守回放——巧妙的伪装补漏 13

一、关闭论坛 13

二、安装论坛补丁 14

三、升级论坛程序 14

攻击回放——悄然潜入 15

一、阴差阳错的攻击 16

二、论坛点券的漏洞 16

加油站: Dvbbs8.1注入漏洞简述	17
1. 生成交易记录	17
2. 漏洞测试	18
3. 注入攻击	19
加油站: 单引号提交法	19
4. 破解管理员密码	21
加油站: MD5密文破解	23

攻击回放——意外的惊喜 24

一、修改文件上传许可	24
二、数据库备份上传	26
三、Dvbbs 8.1后台拿后门新方法	27
加油站: 用数据库备份拿Webshell的前提	28
1. 制作MDB文件	28
2. 数据库备份获得Webshell	33
3. 访问Webshell	35
4. 下载数据库	36
5. 留后门	37

防守回放 揪马与设权 38

一、SQL注入补漏	39
二、查出服务器中的木马后门	39

第二篇 黑客追踪与反追踪——入侵的教训

攻击回放——FCKeditor上传控制网站 43

一、定位FCKeditor编辑器	44
加油站: FCKeditor简介	45
二、检测FCKeditor漏洞	45
加油站: 漏洞的第二种检测方式	46
三、上传网页后门	47
加油站: 漏洞的第二种利用方式	47
四、隐藏的后门	48
五、提权与控制	50

加油站：入侵与提升权限	51
加油站：Kaspersky的klif.sys文件权限提升漏洞	52
六、小小木马，嗅遍机密	54
加油站：上兴远程控制木马	55
1. 配置上传上兴木马	55
2. 远程控制网站服务器	56
3. 密码大窃取	58
加油站：汉字密码的截取	60
七、内存搜索，截取隐藏信息	60
防守回放——发现入侵者脚印	61
一、网站漏洞的弥补	61
二、根据事件日志追踪黑客	62
三、木马暴露黑客踪迹	63
攻击回放——黑客的挑战	67
一、攻击前的准备	67
二、扫描网站漏洞	69
三、远程溢出重获控制	70
加油站：如何确认Imail Server	70
四、教训——擦掉入侵脚印	73
加油站：为什么要关闭“审核策略”	73
第三篇 黑客的堕落—破解与文档陷阱	
防守回放——加密的邮件	79
攻击回放——黑客的灵感	82
一、失败的破解	82
二、溯雪破解邮箱	83
加油站：非弹出式窗口	86

三、代理破邮箱	86
1. GoldenEye设置	86
2. 破解邮箱	88
加油站：非弹出式入口	89
3. 验证密码	90
四、失密邮件导致的破解	90

防守回放——机密数据乎？陷阱乎？ 93

一、伪装的机密数据	93
加油站：MS06-027漏洞	93
1. 简单的DOC捆绑	93
2. office系列挂马	94
二、双重加密伪装	100
1. 设置Word文档密码	101
2. PDF文档加密	102
3. WinPAP为压缩包设置密码	103

攻击回放——最后的破解 104

一、WinRAR压缩包中的秘密	104
1. PAP Password Cracker破解	104
2. APPP破解压缩包密码	105
加油站：Zip压缩包密码破解	107
二、瞬间破解Word密码	107
三、破解PDF密码	109

第四篇 不可能的任务——入侵没上网的电脑

攻击回放——木马侵入内部网络 111

一、突破一切障碍的Byshell	112
加油站：SSDT	112
二、文档中的秘密	115
加油站：MS08-014漏洞简介	115
三、奇怪的上线肉鸡	118
1. 奇怪的肉鸡IP	118
2. 命令行下的扫描	121

加油站：内网中扫描公网IP地址	122
-----------------------	-----

防守回放——无懈可击的VPN 125

加油站：什么是VPN	125
一、构建VPN网络	125
二、VPN加密保护办公安全	127
1. 通过VPN共享资源	127
2. 通过VPN实现远程打印	130

攻击回放——在VPN上打洞 131

一、无线路由的WEP破解	132
1. 收集SSID信息	132
加油站：什么是SSID	132
2. 无线驱动更新	135
3. SSID破解	136
4. 破解无线网络密钥	137
二、跳板渗透	138
1. 寻找弱口令Serv-U FTP Server	139
加油站：Serv-U FTP远程溢出漏洞	139
2. Serv-U FTP Server 5.0.0.4远程溢出	141
三、获取目标文件	142

第五篇 网管与“伪”黑客的QQ争夺战

攻击回放——追查攻击者来源 145

一、隐身，准备攻击	146
二、初试图片木马——受挫	147
加油站：QQ安全中心	147
三、甜蜜欺骗——再受挫	148

防守回放——防范QQ木马 152

一、安全中心设置	152
加油站：常见的QQ盗号木马伪装格式	153

二、病毒监视防范盗号木马	153
三、其它安全措施	154

攻击回放——隐蔽的QQ木马 156

一、追捕隐身的QQ用户	156
1. 揪出伪黑客的IP地址	156
加油站: QQiPPro	157
2. 剥去隐身伪装	158
3. 盯住伪黑客	159
二、完美的欺骗	159
1. 隐藏保护IP地址	159
加油站: 通过代理的QQ掉线后的操作	161
2. 巧伪装, 迷惑伪黑客	161
加油站: 手工发送伪装IP的几条指令	163
三、欺骗运行XLS木马	163
四、WinRAR挂木马的新招	165
1. WinPAP挂马的原理及优点	165
加油站: WinPAP压缩包挂马	165
2. 挂马的简单测试	166
3. 自解压挂网页木马	168
4. 让WinPAP自解压木马更完美	169
加油站: 自解压文件安全性检查	169

防守回放——密码找回 172

攻击回放——社会工程学破解密保 174

一、社会工程学——采集信息	174
二、社会工程学——欺骗	177
三、扩大战果	179

第六篇 渗透与蜜罐——校园网的人侵

攻击回放——控制图书馆 181

一、踩点	181
二、埋下后门	184
三、巧用xls木马提权	186
1. 确定网站漏洞	186
2. 上传xls木马	187
3. 运行xls提权	188
四、MDB溢出提权	188
五、隐藏ASP木马无踪迹	191
1. 插入一句话木马代码	191
加油站：后门木马的容错	192
2. 修改网页文件时间	192
3. 合二为一，图片留后门	193
六、让ASP木马躲过杀毒软件查杀	195
1. 加密ASP木马	195
2. 修改ASP木马特征码	195

防守回放——查出隐藏的ASP木马后门 196

一、检查常规ASP木马后门	196
二、检查渗透式木马	197
三、揪出最隐蔽的图片木马	198

攻击回放——刺入网站的黑手刃，图书馆网站挂马 199

一、准备内网渗透的木马	199
加油站：炽天使远程控制木马	201
二、生成网页木马	201
三、加密免杀的网马代码	202
四、挂马	203

防守回放——网页木马解密 203

一、另存解密网页	204
二、Alert弹出窗口解密代码	206

加油站：JS加密方式	206
三、<xmp>标签再解密	210
四、逆序代码的解密	212
加油站：分析有毒的网页	213
五、shellcode的解密	214

攻击回放——渗透教研室 215

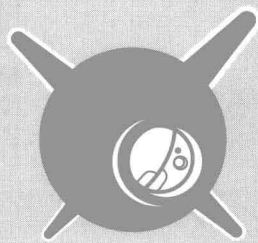
一、hijack渗透嗅探	215
1. 查获远程网络信息	217
2. 嗅探子网主机密码	217
加油站：其他密码的嗅探	218
二、端口转发	219
三、代理连接	221

防守回放——蜜罐诱人 224

加油站：“蜜罐”技术	224
一、下套诱捕	224
二、监控攻击者	226
加油站：时刻监控“蜜罐”	227

第 1 篇

“洞”网之争 论坛谁作主



日出与日落总在重复，在这个很普通的日子，某个普通的论坛，正上演着一场黑客与网管的论坛争夺战。

黑客攻击论坛的理由，只不过是一时的好奇；而管理员保护论坛的目的，则不言而喻……



攻击回放——遗忘引发的攻击

“……左手写着你的名字，右手刻着忘记，让我试着去学会……”

遗忘总比忘记好，这样的记忆即使上面覆盖了尘土，擦完后还是完整的，所以要试着遗忘……”

“遗忘和忘记有多少区别？”枫看着论坛上的帖子，觉得发帖者真是无聊。不过无意间看见了发帖人的用户名——

“雪？呵，好像是一个MM？”枫立刻提起了兴趣，“嗯，看起来应该是个多愁善感的MM，不知道是不是一个美女？”

枫点击了雪的用户名，试图查看雪在论坛中注册的身份资料，不过论坛禁止了枫的过客身份，权限不足无法查看资料。枫随便注册了一个会员身份登录上论坛，发现论坛设置得很BT，会员身份居然也无法查看到用户的注册资料。

“那就到管理页面去看看她的资料吧！”精于黑客攻击技术的枫，打算直接进到论坛的管理页面中瞧瞧。

——于是，一个普通的论坛，因为一个无意的网络闲逛者想要查看某MM的资料，遭受了一场意外的入侵。

一 勘察踩点

枫先仔细地查看分析了一下论坛的结构。看来论坛的管理者没有太在意隐藏论坛使用的系统，在论坛首页上看到了“Powered By Dvbbs Version 8.0.0”的字符（图1），很明显这是一个最新版本的动网论坛系统。



图1 查看论坛版本

动网论坛系统有一个默认管理员密码，如果管理员疏忽的话，很可能没有对它进行修改，可以先用这个密码来尝试登录论坛的后台管理页面。这个方法虽然简单却很有效，很多动网论坛都有这样的漏洞，枫曾用它进入过的大大小的动网论坛也不在少数了。

枫在论坛首页地址后面加上了管理员登录页面链接“admin_index.asp”，浏览器打开了链接：

http://www.yl**.com/bbs/admin_index.asp

在该页面中输入用户名“admin”，密码“admin888”（图2），回车登录。很可惜，提示密码出错，看来此路不通，枫得另辟途径。

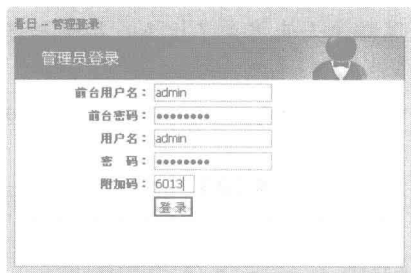


图2 默认用户名密码登录

二 评论带来的机会

在退出后台登录页面时，枫留意到了上面有“动网先锋论坛SQL 版8.0.0”这几个标志，很显然，这是一个使用SQL数据库的动网Dvbbs8论坛。枫想起了前段时间发现的Dvbbs8论



坛注入漏洞，正好籍此机会利用这个漏洞来攻击！

Dvbbs8动网论坛的这个SQL注入漏洞，主要是由于论坛发帖回复评论时，对用户提交的帖子数据未进行严格的过滤。因此，可以在提交数据中加入SQL语句，从而修改论坛管理员的账号密码，进而控制整个论坛。

枫以前进行攻击测试时，由于目前的许多动网论坛网站还未堵上此漏洞，因此攻击成功率非常高。



【加油站】搜索使用动网论坛的站点

可以利用Google或百度等，搜索出存在此漏洞的Dvbbs8动网论坛。搜索的方法比较简单，直接在百度或Google中搜索关键词“powered by Dvbbs Version 8.0.0”，即可查找到大量使用动网论坛Dvbbs8的站点（图3）。



图3 大量可能存在漏洞的站点

查找到Dvbbs8动网论坛后，并不是所有Dvbbs8动网论坛都能成功攻击的，一般只有SQL数据库的Dvbbs8动网论坛，才可在提交数据中加入和执行SQL语句；而使用Access数据库的论坛很难构造攻击语句。

由于在漏洞利用过程中，修改提交数据中是使用SQL语句进行攻击的，因此只有SQL版的Dvbbs8动网论坛才能利用此漏洞攻击成功。

一般来说，SQL版的Dvbbs8论坛，其后台登录页面上通常有“动网先锋论坛SQL版8.0.0”的字符串标识（图4）。只要查看后台登录页面，通过此字符串，就可以确定论坛的数据库版本。

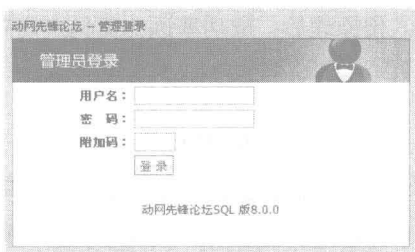


图4 通过后台页面判断数据库版本

不过许多论坛为了避免攻击，通常都会将自己论坛首页及后台上的数据库版本或相关的标识字符串进行修改或删除，因此不显示相应的数据库版本信息，或者显示的是错误的数据库版本。

枫碰到的这个论坛就没有任何数据库信息提示。怎么确定论坛是否采用SQL版数据库呢？枫使用了一个小技巧来判断论坛的数据库版本：

在SQL数据库版本的Dvbbs8动网论坛源码文件目录中，有一个名为“data”的文件夹，其下有一个名为“DvSQLLOG.mdb”的文件，该文件是用来记录SQL语句执行记录的。要检测某个Dvbbs8动网论坛究竟是SQL版还是Access版，可在论坛网址后加上“data/DvSQLLOG.mdb”进行检测。

例如论坛网址为“http://www.xx.com/index.asp”，那么可提交链接为：
http://www.xx.com/data/DvSQLLOG.mdb

回车后，如果能够下载该数据库文件，那么说明该论坛为SQL版本（图5）。如果该论坛未打最新的补丁的话，那么就可以成功入侵此论坛了。

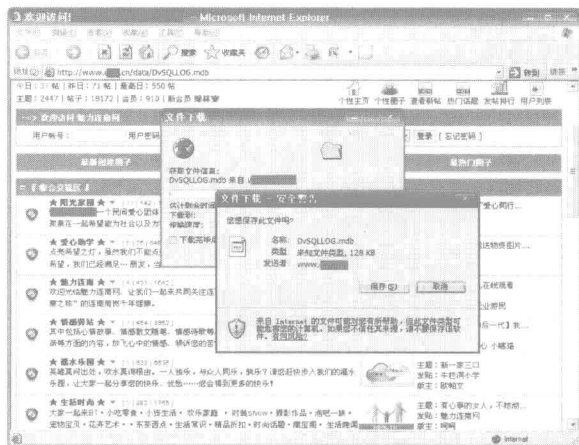


图5 下载SQL记录数据库

高效的手工注入

枫决定手工利用SQL版Dvbbs8动网论坛ODay进行入侵，虽然手工注入SQL语句的方法比较麻烦，但只要了解了漏洞入侵原理后，成功率远比工具入侵高得多。

1. 嗅探数据

枫在IE中打开此论坛网页，用刚才注册的账号登录论坛，随便打开某个帖子。点击帖子右下角处的“点击发表评论”链接（图6），输入任意内容，点击“发表评论”按钮，即可提交评论。

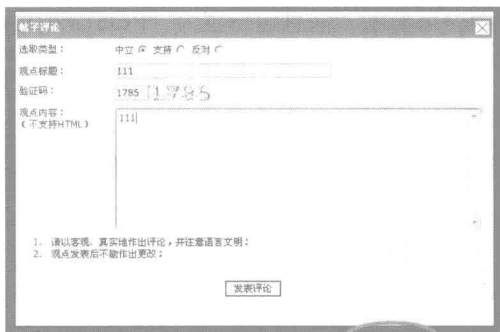


图6 发表评论

枫没有立即发表评论，因为在发表评论前，需要先运行抓包工具，以便抓取发表评论时提交的数据，然后才能开始入侵攻击。

枫常用的抓包工具是WSockExpert，依然使用此工具进行入侵。关闭其它无关的IE浏览器窗口，运行WSockExpert，点击工具栏上的“打开”按钮，弹出进程选择对话框。在对话框中找到“IEXPLORE.EXE”（图7），点击“打开”按钮，返回程序主界面窗口中，即可自动监听抓取IE浏览器提交的数据了。



图7 指定嗅探IP

切换回IE浏览器，在网页中点击“发表评论”按钮，发表评论成功后，再返回WSockExpert窗口中，就可以看到嗅探到的数据包了（图8）。

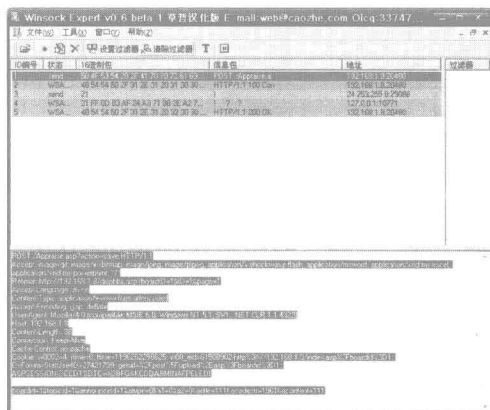


图8 嗅探到数据



在WSockExpert窗口中，可看到“信息包”栏为“POST /Appraise.asp”数据记录（一般为开始第一行数据信息）。打开“记事本”程序，复制此条数据记录下方的详细窗口内所有字符串，粘贴到记事本窗口中（图9）。

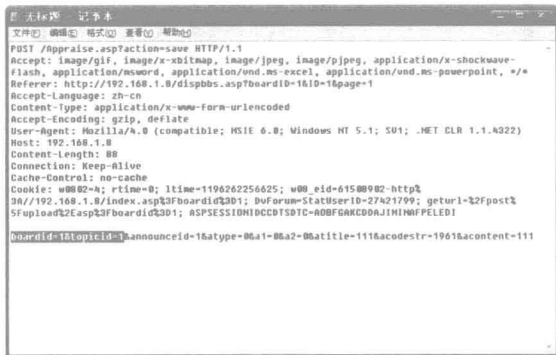


图9 复制嗅探到的数据

2. 转换密码

枫上网随便找了一个MD5加密解密站点 (<http://md5.mmkey.com/>)，在页面中的“输入待转换值：”处输入了“123456”（图10）。然后点击“转换”按钮，在下方的“中间16位结果”中，可以看到16位的MD5散列加密字符串为“49ba59abbe56e057”（图11）。



图10 转换MD5加密

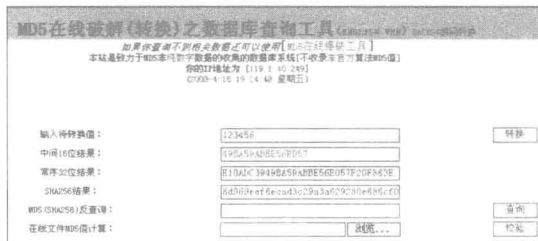


图11 加密字符串

运行“小葵多功能转换工具”，将“49ba59abbe56e057”粘贴到“要转的”输入框中，然后点击“给我转”按钮，即可以看到各种编码转换结果了。复制其中的“SQL_En”字符，内容如下：

0x3400390062006100350039006100620062006500350036006500300035003700D00A00