电脑迷 荣誉出品

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…

云南出版集团公司 •云南科技出版社

电脑迷 荣誉出品

黑客手抄本

黑客VS网管大作战

肖遥 编著

云南出版集团公司 • 云南科技出版社

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　唐荣橼
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

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：四川蓥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

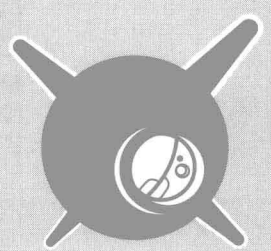
CONTENTS

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

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里，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。

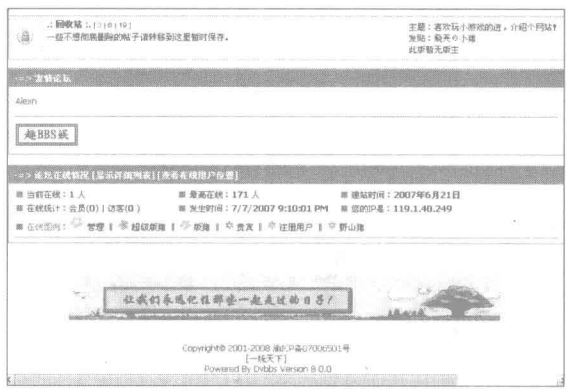


图1 查看论坛版本

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。

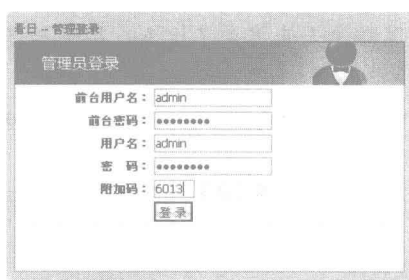


图2 默认用户名密码登录

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。

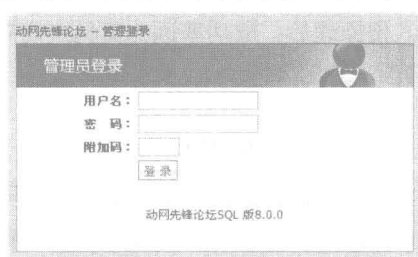


图4 通过后台页面判断数据库版本

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。

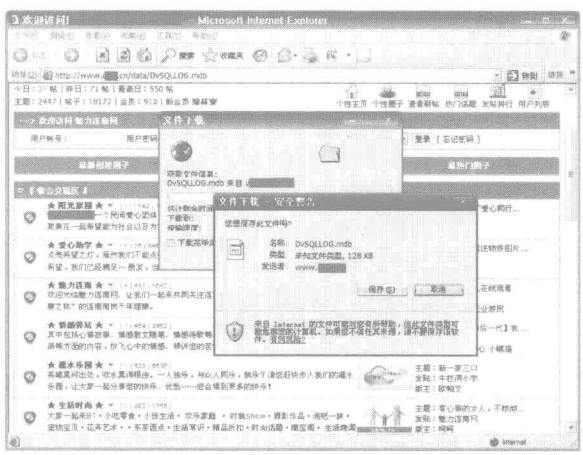


图5 下载SQL记录数据库

三 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。

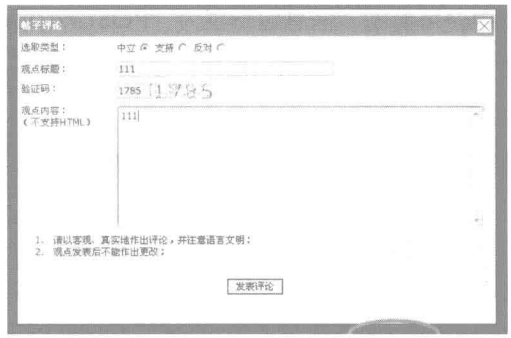


图6 发表评论

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IE

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）。

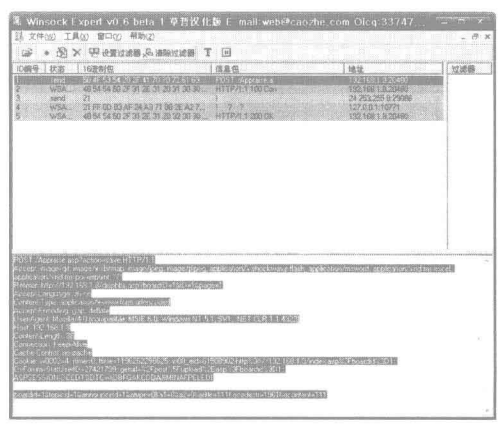


图8 嗅探到数据

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）。

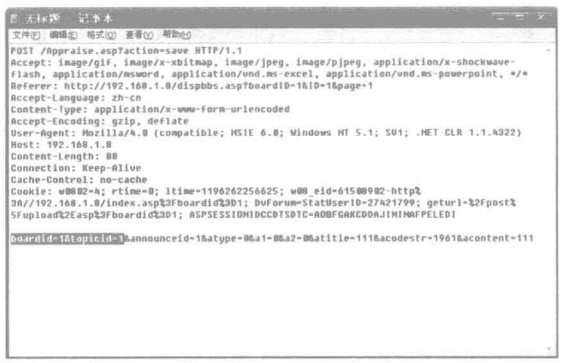


图9 复制嗅探到的数据

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

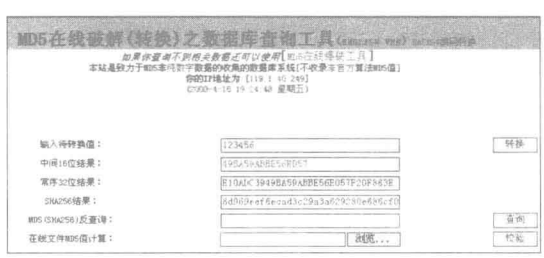


图11 加密字符串

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