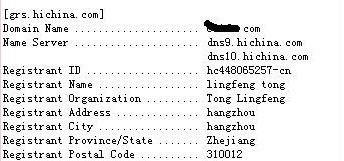
================================  
本篇文章源自《黑客防线》2007年10月刊  
================================  
某日在论坛上看到有人发贴寻求能写某程序的人，当时刚好没事干，看那人又是我们西安本地的，就联系他，说帮他开发那套程序，说白了就是偷代码。  
首 先看了一下他的网http://www.xxx.com（我以这个域名代替），是ASP+Access+雪孩BBS。一般我先从BBS入手，从网上找到 了此网站的源代码，发现内核就是用的DVBBS，很自然地找到默认数据库地址，地址栏输http://www.xxx.com/bbs/DataBase /Snowboy.mdb，顺利下载到数据库，破解出了MD5，我以为在一切顺利的情况下就可以搞到个WebShell了，然而当上传JPG木马准备备份 的时候发现出错，如图1所示。返回首页看了下，不支持FSO，备份没办法用。  
[](http://www.81sec.com/attachment.php?fid=104)  
论坛的“基本设置”里可以设置上传类型，加了个ASP后缀，返回前台，还真上传成功了ASP文件，但是在地址栏输入文件地址却显示“您试图从目录中执行 CGI、ISAPI或其他可执行程序，但该目录不允许执行程序。”，搞了半天也没想出什么好办法，放弃论坛！  
在 主站部分，我又找到了可以上传照片的地方，但NC提交不成功，其他工具也不可以，于是开始用上面获得的论坛的管理账号和密码（账号用ddst代替）登录 主站后台，试了多种组合依然不能成功。后来又想到，要是能在这台服务器上找到一个注入点，再加上DVBBS后台显示路径，基本上就可以备份马了。于是我就 一个站一个站的找，还真找到了注入点，不过仔细一看是Public权限，Public在默认情况下是没有备份权限的，在注入点上执行后确实没有备份权限。 又扫了下同段的服务器，运气还算好，成功找到一个Discuz5.0论坛，并暴密码成功，服务器环境是Apache+Windows 2003，默认情况下是System权限，模板写进去马之后可以执行，确认开放3389，但端口被改。打开CMD切换到S下，执行“s TCP 211.155.221.XX 1-65535 512”，成功扫到终端端口5151，mstsc连上服务器，“tracert arp –a”下发现在同一网关，装有WinPcap4.0，Cain后无法嗅探，大概做了防ARP设置，看来ARPsniffer也走不通了……另寻出路！  
在 Google上搜索他的ID：ddst，发现在好多站长站上都注册过，进了一个他注册过的DVBBS论坛，没有更改默认数据库，顺利下载数据库，破出了 ddst的密码是ddst1314521，然后用ddst/ddst1314521登http://www.xxx.com/admin /login.asp后台失败，用admin/ddst1315521登录成功，如图2所示。后台界面很简单，只有ewebeditor可以利用，但后台 地址被删。这时，有点绝望，费了那么多神，放弃的话……。在ww.net.cn上又查了下他的域名信息，如图3所示，记下他的邮箱 ddst@163.com，然后在Google和百度狂搜他的邮箱和ID，最后找到了他的QQ，知道了他经常上的网站是im286.com、 bbs.china.com。借用了女同学的QQ号加了他，跟他不时的聊上几句，因为他总是隐身，看不到什么时候在线，这样做是为了收集他每天上线的时间 和习惯，大概了解到了他是个人站长，没有固定工作，而且每天下午睡觉。随后我就一直试验他的邮箱密码，希望能找到更多有用的信息，一翻艰苦磨难后，最后用 ddst198211顺利登录。接下来就是查看一些邮件了，但查看邮件的话对方会知道，没有被查看过的标题是黑体字，最后想到了一个好办法，就是用163 邮箱的双克隆功能，把邮件克隆到我申请的邮箱里，在我的邮箱里进行查看。邮箱里好东西还真不少，发现他在万网注册过，而且还是代理。用万网密码找回功能， 直接修改密码进入了他的账户，如图4所示，在“个人资料”中找到了很多有用信息，手机号、身份证号、地址等，如图5所示。最重要的是，找到了一张服务器的 托管协议。上面虽然写的是公司，但其实经过一系列调查，发现其实就是一个个人站长租的服务器，那就先搞个WebShell上去看能提权。一般像这种情况， 比如是卖空间的我就装作大客户的样子，先让他们给开点空间测试一下，如果可以就买上几十个G；如果是个人服务器，也就买空间什么的，反正发挥聪明才智，让 他给开个空间，带数据库，如果发现路径有规律就直接用MSSQL备份过去或者列路径。这样，我就用QQ加了那个人，以买空间的名义让他给开空间，说试用两 天，没问题就打算买10个G，那人看有钱赚，很爽快地答应了；然后就问他都有哪些服务器，挑选了xxx.com所在的服务器，让他在上面给开空间，又说需 要MySQL数据库支持。一切很顺利，直接得到了FTP和MSSQL。连接数据库之后发现是Public权限，Public权限默认情况下是备份不了的， 试了之后果真如此。然后我装作什么都不懂，问他为什么程序不能正常运行，后来我说我们技术说是数据库权限问题，终于，他把MSSQL账号权限设成了 DB，OK，开工！  
[](http://www.81sec.com/attachment.php?fid=105)  
图2  
[](http://www.81sec.com/attachment.php?fid=106)  
图3  
[](http://www.81sec.com/attachment.php?fid=107)  
图4  
[](http://www.81sec.com/attachment.php?fid=108)  
图5  
由于禁止外部连接，那就自己构造一个注入点吧。在数据库里建了个admin表，写了个ID的字段，用conn.asp连接数据库，再建立一个x.asp文件，内容如下。

<!–#include file=”conn.asp”–>  
<%  
dim rs,strSQL,id  
set rs=server.createobject(“ADODB.recordset”)  
id = request(“id”)  
strSQL = “select \* from admin where id=” & id   ‘  
rs.open strSQL,conn,1,3  
rs.close  
%>

在 NBSI里输入http://my.xiaozei.cn/x.asp?id=1”可以注入，本以为结合之前BBS的路径备份一下就结束了，但最后才发 现原来之前的BBS目录是虚拟的，服务器关闭了错误提示，没办法列目录，猜了好几个目录也不行，传了个免FSO的马上去提权也没希望。看来只有另想其他办 法了……  
既然他的手机号、身份证、地址、邮箱、姓名之类的所有信息，那我就等于是他了吗？而且手里还有他的一份托管协议，于是想到了机房那边。 一般这种天天挂网上 的人都是以QQ联系的，什么都知道了，弄他QQ密码过来应该不难，而且邮箱里有他之前取回QQ密码的记录，说明这个邮箱就是绑密码保护的。身份证号现在有 了，就差保护答案了，查了下密码保护问题，问题是：您老婆的生日是几月几号？于是我用手机发短信给他。

引用

我：昨天我生日，你老婆送我礼物了，替我谢谢她。  
他：你是谁啊，我怎么不知道？  
我：啊，哈哈，我不告诉你，你当然不知道。明天见了再说吧。  
他：哦。  
我：对了，你老婆生日几号，到时候我也送他个娃娃。  
他：哦，她是4月20号的，都过了，你不知道？  
…………

得 到了生日，更改了几种组合后，顺利得到了他的QQ密码，上去发现有个网名叫世博科技的，签名上写着什么虚拟主机价格之类的，看来就是他了。前面用女QQ 和他聊天时发现他每天下午时间都不在，大概是睡觉时间，于是就在他正忽忽大睡的时候，我上了他的QQ和世博科技的人说话。

引用

我：你好，我服务器密码忘了，很急啊。  
世博科技：哦，请问您的IP是多少  
我：211.155.XXX.XX  
世博科技：这服务器确实是我们公司的，您打电话XXXX与我们技术部联系吧。  
……打电话联系……  
我：您好，我服务器密码忘了，客户一个站在测试，今天得给人家交工。  
技术：服务器密码如果您改过的话，我们没办法帮您找回或修改的，忘记密码只能ghost恢复系统了。  
我：那就恢复吧，现在真的很着急。  
技术：您寄张您的身份证复印件以及托管协议过来，我们这边确认后才能给您恢复。  
我：不是吧，寄过去得一两天呢，我那些程序今天必须得下下来，不然损失好几万，托管协议我用签协议时候的邮箱给你发过去，还有身份证号什么的，不都一样的嘛，不然我公司的损失你给负责啊。  
技术：那请您稍等下，我征求下上面的意见。  
（……半个多小时后电话回过来）  
技术：您好，上面同意您用邮件的形式发证明材料，您把信息发送到admin@11111.COM,确认后我们会给你进行ghost恢复，初始密码会变为11111.com@777，请您及时修改密码。

半 个小时后，我成功用11111.com@777登录服务器，打包，下载程序。一般我不习惯留后门在服务器上，只是放个gina，留好多一句话，记下 Root密码，然后把启动项目权限设置为可写，把任何一个系统软件，如su的目录设置为eveyone完全控制，记下一些数据库路径什么的，一般都很少 丢。  
回顾这次入侵过程，没有用到什么高深技术，不是所有的服务器都可以用纯技术方法去入侵的，所以一些容易被人忽视的人为漏洞就成为了我们突破的目标，