本帖最后由 maya66 于 2011-5-12 09:22 编辑  
  
**BY: maya66  
  
=======================  
  
第一次**  
  
   
  
 

**Discuz! X1.5 程序，没有Discuz! X1.5 0day 就直接旁注了。。。**

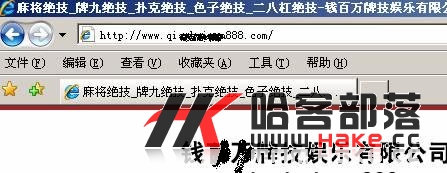
**IP:  
49.247.254.55  
韩国的一台服务器**

**旁注发现**

**Vip.yesmybi.com 也在这台服务器上**

**发现一个可利用的一站**[**www.qianbaiwan888.com**](http://www.qianbaiwan888.com/)**的站**

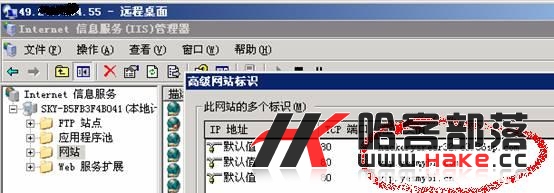
   
  
 

**中转注入很简单，直接获得后台用户与密码，上传一句话**

**直接菜刀连接,发现星外，找到可读可写目录，上传星外提权**

**（csript.exe+IISpwd.vbs 或 星外的 ee.exe ）**

   
  
   
  
**bbs.yesmybi.com**  
  
   
  
**vip.yesmybi.com**  
  
 

同时获得vip.yesmybi.com的管理账号与密码。。。。

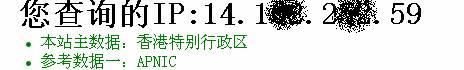
 

**没有过两天，发现华中论坛换了服务器。。。。。账号与密码，还没有获得呢。。。继续。。。。。**

**==================================**

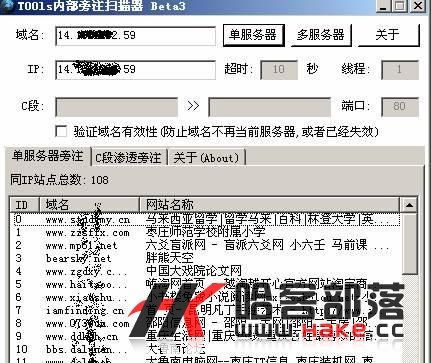
**第二次**

**这一次发现华中论坛挪到**



香港的一台服务器

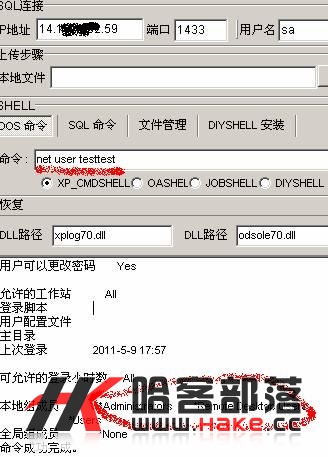
同样先旁。。。。。。



**108 个站，拿同站的shell问题，继续。。。。。**

**旁注之后还是星外提权，这里不再赘述,同时获得sa密码。。。**

**用sa 加个用户。。。。**

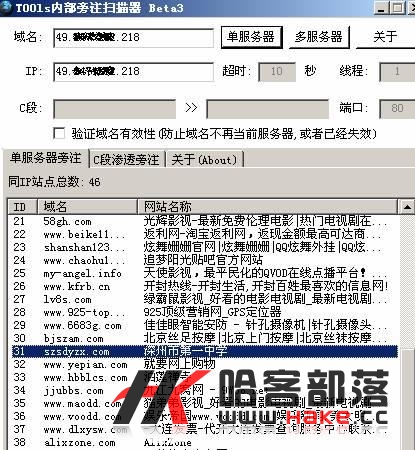
**添加用户成功。。。。**

**没有过两天，华中帝国又换了服务器。。。汗。。。**

**==================================**

**第三次**

14.jpeg



**找个站，先拿shell…..**



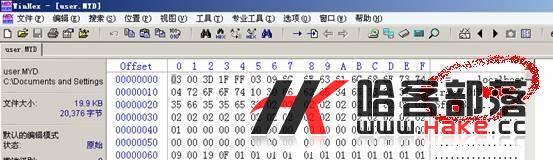
**然后看了一下，不支持aspx,支持php….**

**星外的服务器，没有0day提权，Pr提权不成功，读注册查不出mssql密码。。**

**用菜刀连一下。。。发现安装mysql安装路径。。。**



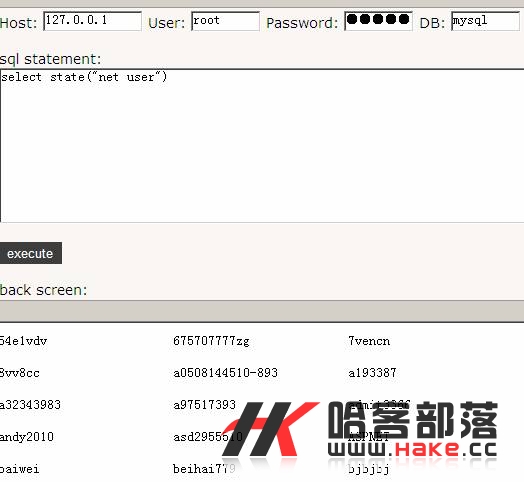
**直接下载user.myd  
user.myi文件,网上好多教程说搭建mysql环境，其实我觉得不用，直接winhex文件打开user.myd文件。。。**

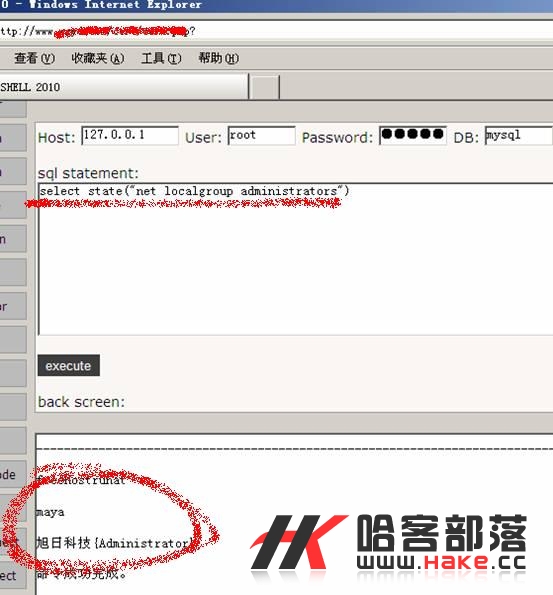




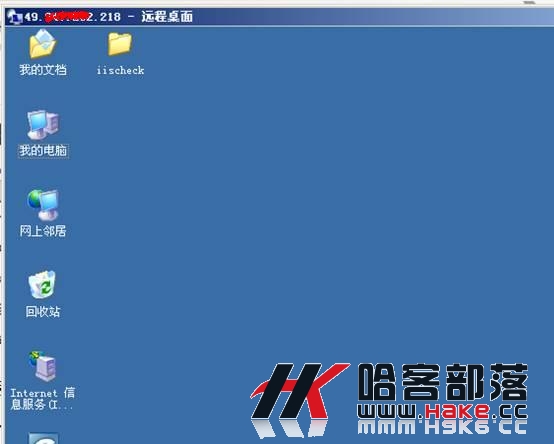
**直接破解。。。(是mysql加密方式)**

**提权就没有什么问题**



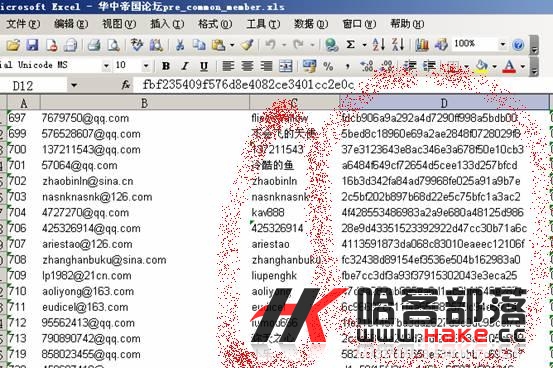


**提权成功。。。登陆。。。。**



**在想获得华中帝国的用户名与密码时候，费了很大功夫，一直也没有获得，在网上找到有dz x 1.5 (青龙的)记录密码，我也不会用,我太菜了。。。**

**Dz x 1.5 密码是一种 md5(md5(pass).$salt)格式  
就是拖了库，也没有好的办法破解。。。**



**后来想想用嗅探软件来获得用户与密码。。。**

**Cain 因为嗅探的丢包很大，所以也没有cain 挂个  
文本，装B走人。。**



**================================**

**昨天看了，华中又换了服务器**



**================================**

**人常说，事不过三，从此不再搞华中。。**