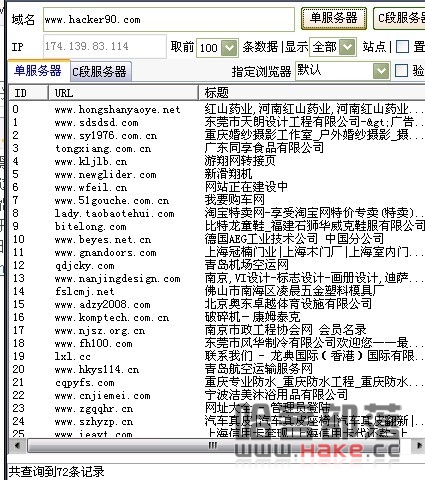
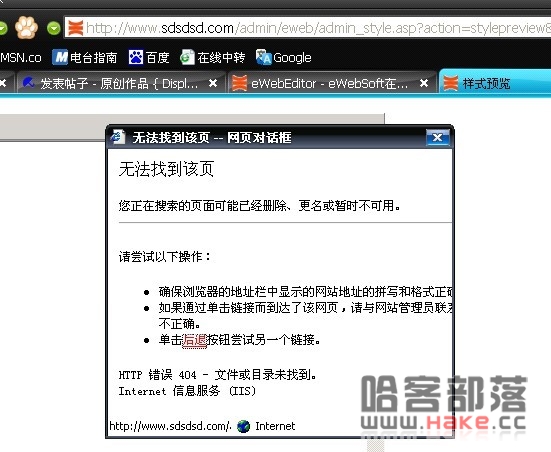
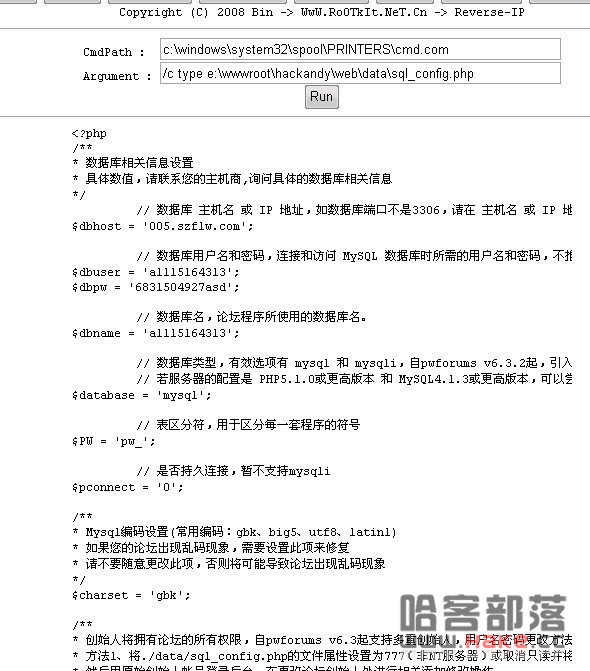
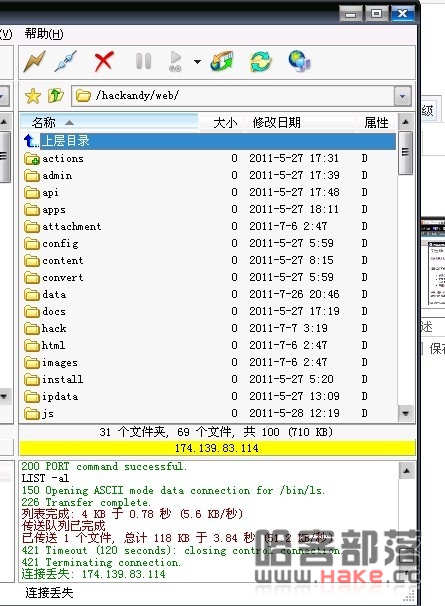
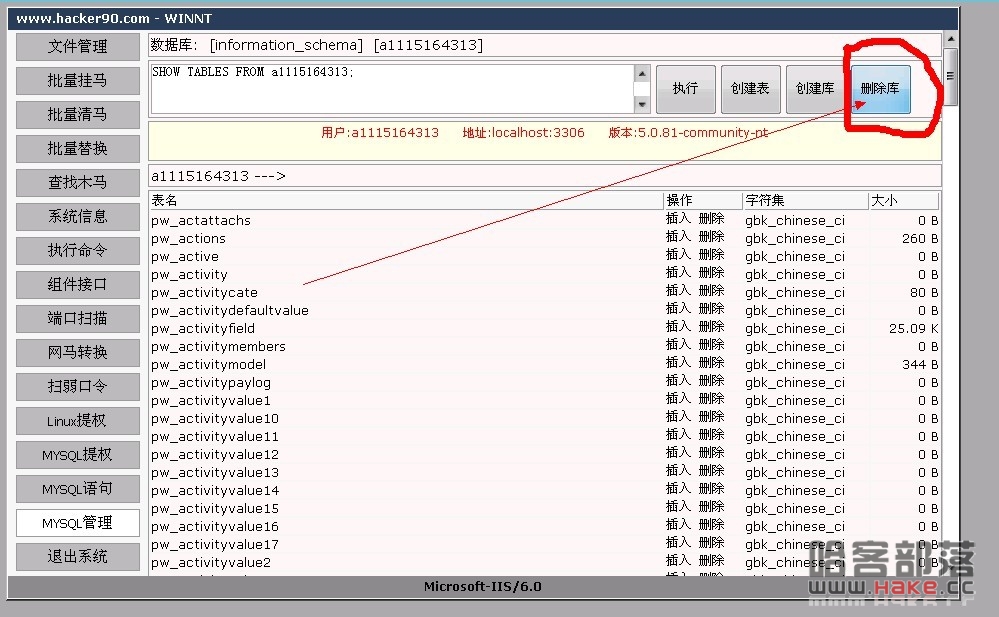
今天逛逛论坛，发现一个帖子，标题是90黑客脑残什么的，不记得鸟。。。里头直接给出的标语是人家日了XX的博客，然后写出鸟那90黑客的域名，咱表示确实没听说过这什么鸡巴狗屁90黑阔站。。。而且那帖子有点问题，，不知道是不是想骗点流量还是啥的，藐视下午就看不到那个帖子了，可能是某管理给她XXOO了···悲剧的娃，哥为你感到悲哀，，，如果你是想在这里打广告，那哥哥帮你打个响点的哈····不过sorry，哥哥表示要格了你的站，删了你的数据库，脱了你的库，公布你的库。。额。。。在万分纠结的心情下，2分钟日下旁站，10分钟日下主站，蛋疼额。。。  
不废话了，，目标站：[www.hacker90.com](http://www.hacker90.com/)  
   
运气有点好，随便点一个，就那第二个，就日下了，直接命中  
   
很简单根据图片找到了eweb的上传，进了后台，发现上传页面被删了，但是我看到了里头又黑阔留下的，加的asa,肯定有人日过，  
这怎么办呢，直接利用edit 2.8漏洞遍历下Admin\_UploadFile.asp?id=&dir=../..  
   
额，很简单就日下了一个旁站shell。  
根据观察，应该是星外改的，有星外注册表及程序名字，但是sa破了进不去，换思路  
找可写可执行目录...  
c:\windows\system32\spool\PRINTERS\cmd.com  
找到了个可写可执行目录，但是权限相当小，不知道怎么回事，执行带参数的一律没回显，有可能是权限低导致的，执行不带参数的倒是可以执行。可是很奇怪，执行cmd命令带参数又没问题。  
好吧，绞尽脑汁的我不浪费时间去提权了，服务器咱多的不能再多了，懒得要了都。日了这个狗日的就好了。  
   
有人问为什么我知道路径，同样，利用强大的For日出来的，不过因为站点很多  
我执行for等了30分钟才扫出来，这里我就不截for找目录的图了，直接甩命令  
在要跨的站里找个标志性强的文件，例如一个图片20030201.jpg  
for /r e:\ %i in (\*20030201.jpg) do @echo %i >>C:\windows\temp\1.txt  
先看看目标站，找个突出点的页面或者图片，然后扫呀扫。  
这里我又蛋疼了，知道了路径等等，可是我依然没有办法写进去，没权限（或者还有啥我没想到的方式）  
怎么办呢，，，没关系，，静下心继续想各种命令，，，，  
沉思1分钟，果断的type  
   
数据库信息，不过是dz的，我不会破密码和后台拿shell  
这里我就不蛋疼了，直接社FTP。  
根据路径，我知道FTP账号是hackandy  
密码呢？草她娘的黑阔也是人，数据库密码和FTP密码一样。  
   
表示压力大大滴。。。哟西。。。。  
 <http://www.sdsdsd.com/a.php>脱裤咯，干你娘的  
接下来邪恶的一幕到来了，，，咱该做点啥呢，，，  
   
   
额，今天咱就这么玩玩算鸟，以后她奶奶的别到处打广告，你站点要是没人，爹去顶顶你。不然的话，爹一时手贱，就会忍不住要草一草的。。。孩子，祈祷你有备份过。。  
  
  
