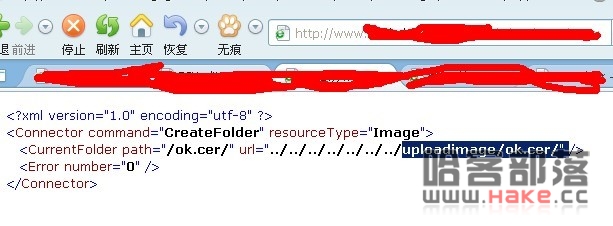
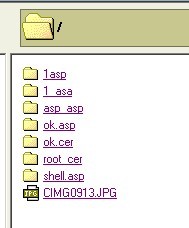
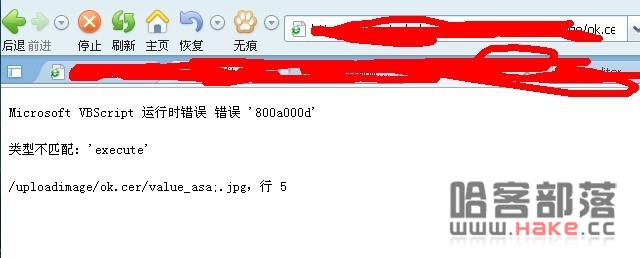
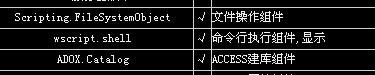
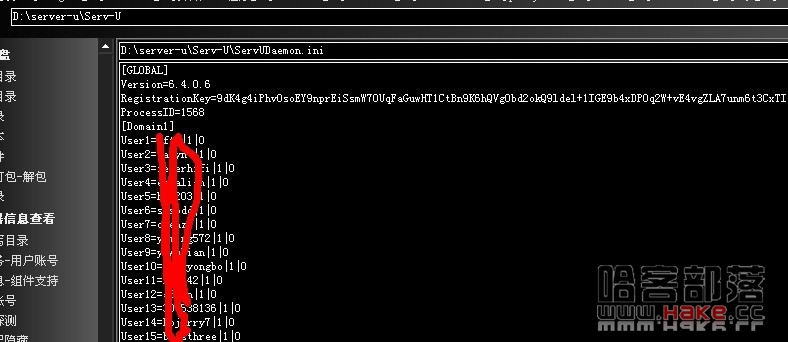
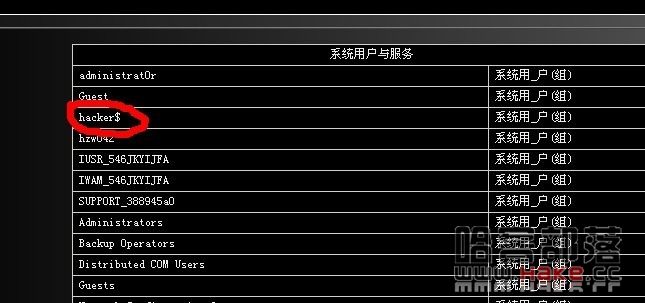
前沿：看帖不回帖，全家木有小JJ。http://wwww.hake.cc/static/image/smiley/coolmonkey/02.gif  
原创哈，首发:hake.cc   转载请注明，谢谢。大牛飞过，没啥太大的技术含量，仅仅是几个入侵的小技巧罢了。  
＞﹥親愛旳＞  
  
正愁蛋疼得无聊，群里一伙计发个fckeditor的，让帮忙，谁让咱最手贱呢，看看吧，，停下打飞机的手，开始敲键盘……  
   
  
这里可以看到，已经创建了/ok.asp/目录，并且上传了图片木马。利用解析漏洞，这里正常情况下，我们就可以直接利用解析漏洞访问我们的木马了。  
但是，当我们访问的时候，悲剧的发现  
   
500错误。这里为什么是500错误呢，我们分析一下原因。首先，我们回到上传地址，刷新下可以看到，木马确实还在（这里就可以完全不考虑是杀毒K掉木马导致的，当然了，如果你还不放心，可以直接传到更上级目录，不带ok.asp的目录，直接当图片去访问，如果可以访问，证明是OK的。）这里我们就不测试了，有经验的，一眼就可以看出原因。  
1：杀毒拦截  
2：解析漏洞补了（或者不是iis 6的）这里我们知道不可能，因为：  
 从这里可以看到是iis6.0没错  
3：又或者不支持asp，但是我知道这不可能，因为站点就是asp的。  
  
那么唯一的就是第一点，杀毒或者防火墙拦截。  
这里怎么去突破它呢？有人说可以试试FCK的二次上传呢？ 6.jpg   
没意义。  
那么回到之前的思路。  
我们创建个正常的目录1asp看看，  
   
可以看到，是正常访问的，这里我们就完全可以确定是防火墙拦截了ok.asp这个目录（具体规则：\*\*/\*.asp/\*）  
那么怎么突破它呢，这里我想起了智创web防火墙，日站比较多的牛绝对遇到过智创web防火墙这套系统，它的规则就是这样的。  
但是我仔细研究过它的规则，它是只拦截了几个常规的，.asp  .asa  .aspx   .php等这几个目录。  
像那种扩充的  \*.cer（仅仅只是思路，还有很多很多后缀自由发挥）是完全没有进行拦截的。  
OK，思路来了，这里回到目标，继续测试，我们就直接拿cer先开刀。  
   
之前有朋友说fck不会找路径，这里我简单的说明下吧。大家可以去网站的前台，看图片的路径  
fck的路径大多都有规律,一般都是userfile upload/file/  等等的，你们可以先在fck看看正常的图片  
   
这样就100%确定路径了。然后延伸下去。  
这是第一种，第二就是看我上面的，创建目录的截图。  
url="**../../../../../../../uploadimage/ok.cer/**" /  
一般的，图片的根目录都是从网站根目录延伸下去的。那么基本上可以确定是  
[www.xx.com/**uploadimage/ok.cer/xx.jpg**](http://www.xx.com/uploadimage/ok.cer/xx.jpg)**这样的路径**  
  
  
**好了，回到主题.这里毫无疑问，我已经利用.cer绕过了防火墙的拦截。**  
   
   
  
  
全过程就是这样，到这里，整个网站权限就已经完全沦陷。接下来就是属于提权部分了  
提权的思路就有千千万万了，每条延伸下去又有N条，完全是靠长时间经验的积累的。  
我这里就简单拿这个站的提权以一条思路来讲，大家看看就好，学不学得到东西那是你们的事咯  
  
提权，首先我们会先看看服务器是否支持aspx（当然了,jsp权限是最大的，一般直接是系统权限）。  
因为aspx权限比asp往往要大得多，不支持aspx,不支持ws.shell组建，往往无法执行cmd命令  
而如果支持aspx，那就完全不需要靠ws.shell组建，就可以执行cmd的，当然了，这里是需要你先去找个可写可执行权限的目录才OK  
回到目标站，不支持aspx,支持ws.shell组建（这里有丁点几率可以执行cmd）  
   
我们同样先找个可写可执行目录  
用asp自带的扫目录权限看看  
   
运气有点好，D盘溢出，可以说明，至少是D盘根目录我们有权限浏览，子目录暂时不确定  
好了，这里我就不墨迹了，直接在D盘找了个目录，上传cmd以及各种提权exp  
   
iis6漏洞就秒杀了。  
  
这里是借助的cmd权限提的，如果不支持ws组建呢？我们岂不是提不了？  
NO，这里说第二种提权，同样是这台服务器  
15.jpg   
首先FTP连下目标站，发现是serv-u 6.4  
思路回到webshell，D盘有权限浏览，OK，我们直接找su的目录，破管理密码，如果管理没设置密码，那更爽，直接serv-u给它溢出了。  
   
从配置文件可以看出，是没有password值的，也就是说，serv-u完全是空口令。  
   
直接用asp马自带的su提权给它溢出了。  
   
第一次提下就是SU提的，只是现在做教程想多给大家写点思路，才临时跑去看了cmd，然后多写了个第一种提权方式。  
  
OK，大牛飞过，教程就这样了，学多学少，看个人了哈···看帖不回帖，木有小J