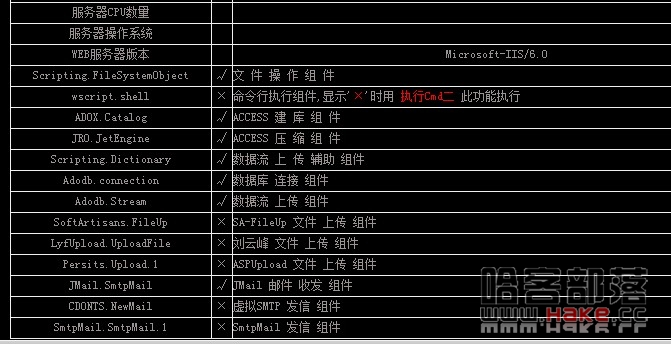
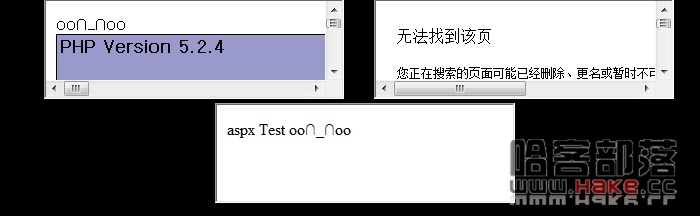
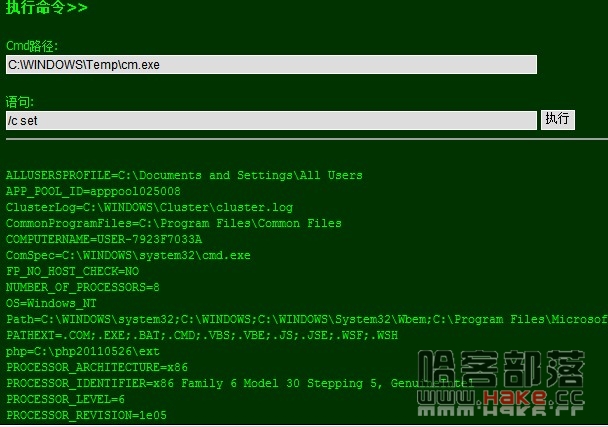
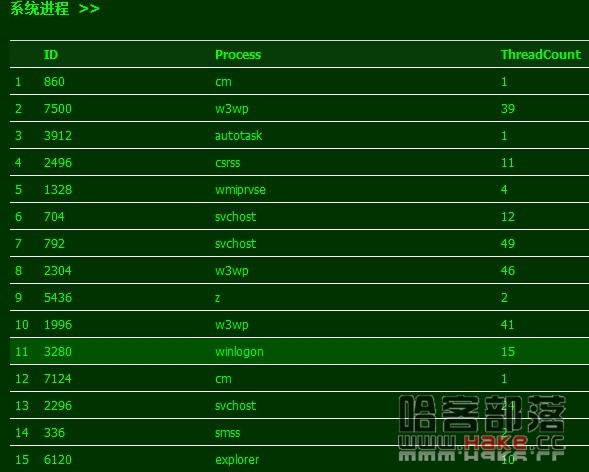
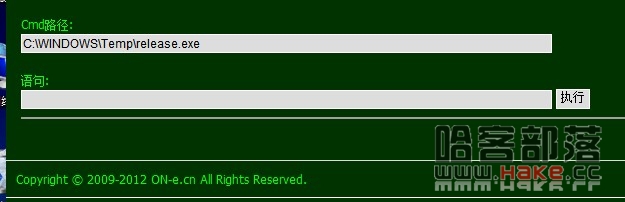
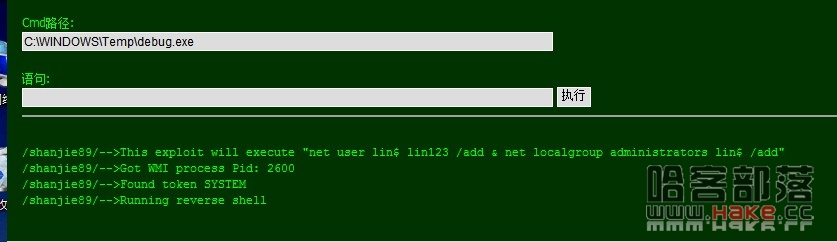
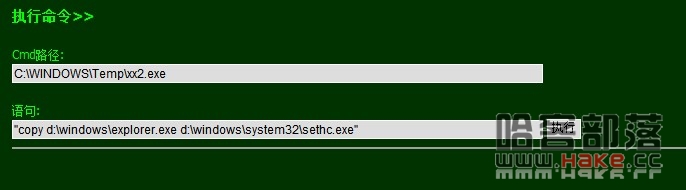
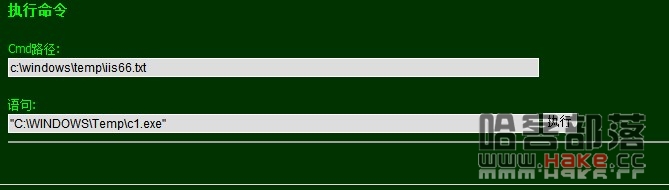
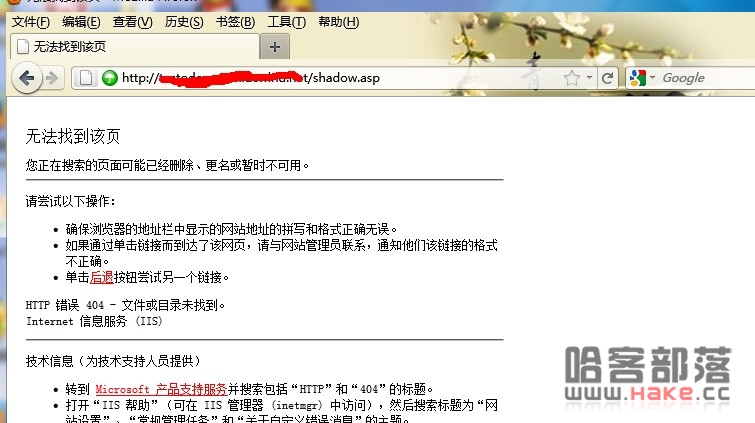
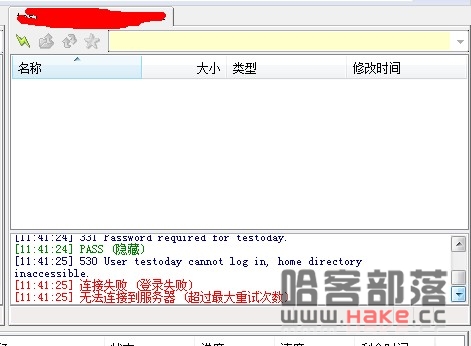
作者：叩桥不渡  
  
新开了个博客，需要写些原创的文章。另外，听朋友说，那些提供试用的空间商的服务器的安全设置都是很变态的。我也想去见识一下，于是就开始找了。找到了一个，填写了一大堆资料，终于申请到了。  
申请到，拿到了FTP的账号密码，还知道了服务器的IP。我不急着上马，我拿出工具，扫它开的端口，因为用马扫很慢。  
扫出来了，木有发现有什么可利用的第三方软件的端口，更发现了3389木有开，不过发现了一个可疑的端口，马上用连了上去，成功。  
   
好了，知道了远程桌面的端口，就上ASP马了。首先看一下组件情况  
  
   
  
该删的都删了，正常，要是没删才不正常了，呵呵。  
接着看脚本支持的情况  
   
支持PHP和ASPX  
我想，这服务器都提供免费试用，不太可能通过PHP能提权，不然早就被人干了。再说了，我随便点了一些目录，都是没有读的权限的，很难找到ROOT的密码。另外，在扫服务器的时候也木有发现开了第三方软件的端口，于是就放弃了通过PHP和第三方提权，果断上了ASPX的马。  
上了ASPX的马之后，马上找有执行权限的目录，进了一个常用的目录，发现如下信息   
         
访问被拒绝  
到这里，我想有些人肯定知道怎么用了。  
其实，它只是没有读的权限而已，还有写和执行的权限的，我上了个CMD，没有提示上传成功，还是提示拒绝访问，不过我可以通过上传的CMD执行命令。  
于是我就做了一个实验  
在ASP马上建了一个目录，成功了。  
再通过ASPX马访问这个目录，上传了一个TXT也成功了  
   
   
其实用ASP马上传，能提示上传成功，而不知道为什么ASPX马就木有提示呢?  
   
知道了temp目录下是有写权限的。  
通过上传的CMD执行命令成功。当时我还以为我会拿下这台服务器的，后来发现我错了。  
        
然后去看了系统的进程，没有发现有杀毒软件。  
       
于是就马上上了个面参数的PR，第一个运行没反应，上了另外一个版本的，我有两个免参数版的PR，有时一个不能，另一个就能用。  
运行另外一个，有回显，但是没执行命令成功。  
       
   
然后再上了一些提权神器，都木有用  
  
然后再试了传说中最淫荡的提权方法，替换粘贴键。  
不过失败了，执行木有反应，远程上去试了，也木有反应。  
   
看来管理员把一些危险的命令的system的权限去掉了  
不过，没有system权限执行那些命令，还可以通过上木马来运行的。  
由于我没有外网IP，就叫朋友配了一个发过来，我传了上去，运行，朋友说木有反应。  
   
这个就奇怪了，一般来说，遇到把一些命令的system权限取消掉，通过上木马都能成功的，看来管理员不知道弄了什么。  
      
然后再弄了很久，都木有弄下来，当时很晚了，差不多凌晨3点了，就睡觉了。今天起床，把那个马打开，结果被删了，ftp账号也被封了。。。  
       
   
不过就算没有删掉，我也是搞不下来的，因为没有思路了。  
发出来，只想给大家提供一下提权的思路，而且提权需要细心，善于发现可利用的信息，这样提权就事半功倍了。  
另外，如果有大牛有办法的，希望可以告诉下我，一起学习，一起进步，呵呵