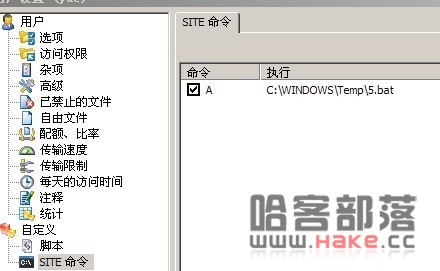
|  |
| --- |
| 今天朋友丢一个站  <http://www.xxxx.com.cn/xxxxx/Editor/Admin_Login.asp>  帐号和密码都是admin  进去一看 1.jpg  编辑器 帐号密码都有了进去看看拿webshell吧 他说上传都突不破我就去看了下  老步骤了 改上传模式 2.jpg  提交 3.jpg  提示成功 哇爽  太爽马上拉出大马（这个因为我小马不知道怎么的写不进我直接上大马）;  马上试试 4.jpg  不成功我靠  看来得到要突破了  在样式管理那里添加asa; （注意；）  5.jpg  再试试还是不行  抽支烟想想  如果把木马名后面也加一个；呢  想到做到  马上试试  6.jpg  可爱的后门拿下  找到地址看到了可爱的后门了  7.jpg  这样webshell算是告一断落了    提权开始  马上进去  8.jpg  没有wscript.shell组件现在都差不多没那个了看看网站有什么  权限还算可以能收集信息  1 扫端口  9.jpg  5900 哈哈 VNC 提权 但是他没有shell组件 要怎么弄到密码呢 又头痛了  又到webshell上看看有没有可以利用的  10.jpg  D盘发现  FLASHFXP 马上下载下来看看  11.jpg  这么多站点试试 不知什么原因一个也没连接上唉 又蛋痛了  再看看 12.jpg    G6 有点映相 下载来看看  马上明白原来是一个G6FTP 我找出WJS做的G6FTP提权 看了下    在webshell上找到密码连接  13.jpg  我靠人还真多看来这个服务器很好  照着教程提权  不知道成不成功  但还是没有拿到VNC密码 我又想到了JHACKJ高级黑客攻防视频教程 中对抗变态服务器的教程方法 我们能不能把那个注册表导出来呢  想到马上就去操作  写个批处理  regedit /e C:\WINDOWS\TEMP\port.reg "HKEY\_LOCAL\_MACHINE\SOFTWARE\RealVNC\WinVNC4\"  意思就是把HKEY\_LOCAL\_MACHINE\SOFTWARE\RealVNC\WinVNC4\里面的注册表倒出到C:\WINDOWS\TEMP\ port.reg  注意这个目录要有权限哦  上传webshell 17.jpg    保存成功后  我们在G6FTP上加上  OK  连接FTP 运行命令  Quote site A  回显成功后  去webshell看看有没有port.reg文件  15.jpg  哈哈  找到  下载回来破解拿到密码  现在连接服务器  16.jpg  出现在这我哭  从天堂打入地狱  搞了一天很累了  我在各论坛问了  没有解答  希望能解决的高手说下方法  3Q  PS：此服务器IP在<http://rootkit.net.cn/index.aspx>  查有272个站点  在webshell上有400多个域名用用户  RP大多》5  PS：这是本人很久前的提权手记了我一直放在我的博客上  今天拿来大家分享呵呵  再次感谢谢 哈客论坛给的学习机会 |

[14.jpg](http://wwww.hake.cc/forum.php?mod=attachment&aid=MjA0N3wzNDZlN2M5M3wxMzE5NzE0MjQzfDgxNTI%3D&nothumb=yes) (23.55 KB, 下载次数: 0)



[17.jpg](http://wwww.hake.cc/forum.php?mod=attachment&aid=MjA1MHwwMDk2MWQxN3wxMzE5NzE0MjQzfDgxNTI%3D&nothumb=yes) (14.56 KB, 下载次数: 0)

