|  |
| --- |
| 同学们，上课了，都做好了！！咳咳！！  这篇文章的由来还感谢“威慑”会做出贡献的腐败份子，俺们本地有个什么XX湖生态区，其实呢就一妓院！！  废话不多说现在开始上课、http://wwww.hake.cc/static/image/smiley/coolmonkey/01.gif  我就检测了下网站，目标站扫也没扫出什么东西，当然就想到旁注了！！！  过程我就不写了是社工的后台密码，网站安全做的还是很好的！工具也用了不少。进了后台直接修改上传格式，上传了asp马  1.jpg   成功拿下webshell     但是无WS  不支持php  不支持aspx    但是服务器确实是支持aspx的 但是在这webshell里面就不行，却步JJ说这是可以设置的！  这才明白，然后就想着找个支持aspx的shell，找到个叫“数字人的CMS”百度查了下没有0day  然后下载源码找到一个编辑器酷似FCKeditor但是不是，又一次失败  这时候陷入僵局了，然后群里找大牛提权，没人理我，就和他们聊天扯淡http://wwww.hake.cc/static/image/smiley/grapeman/04.gif  时间慢慢的过去了，然后继续。其实权限还是可以的，开了1433  3389 43958 21等没去查那么多  翻了翻目录也没找到sa密码  然后就放弃了，然后通过C:\Documents and Settings\All Users\「开始」菜单\程序\  找到Serv-U然后下载快捷方式找到SERv-U路径  2.jpg   居然有权限一看就知道不是6.0版本的了   最后查了下版本文件，7.0的  3.jpg  以前没接触过，再说我根本不会提权这可以说是第一次吧  对这东西又不熟悉，开始翻SERV-U目录  发现XXXX.Archive文件   好像和6.0版本里的ServUDaemon.ini文件差不多吧  很熟悉，然后破解了个密码看了下 果然是FTP用户  然后就想试着拷贝下文件简单修改成C盘权限，没想到成功了http://wwww.hake.cc/static/image/smiley/ccc/ali23.gif  然后直接弄个cmd替换掉sethc.exe文件     连接5下shift弹出我最爱的cmd窗口   。  然后敲打着熟悉的命令（你们懂的）！！  登陆服务器 4.jpg   第一次文章，大牛别见笑！！本人菜鸟一个！！  在此感谢一直帮助我的  isosky 小师父，还有群里的大牛！  同学们下课吧！！！http://wwww.hake.cc/static/image/smiley/coolmonkey/07.gif |

[3.jpg](http://wwww.hake.cc/forum.php?mod=attachment&aid=MjU1OHwxOGM1ODUyOXwxMzE5NjQyMDM0fDgxNTI%3D&nothumb=yes) (20.61 KB, 下载次数: 0)

