i春秋-在线挑战-真的很简单-过程记录

转载

weixin_33726943 于 2016-10-05 11:28:52 发布 1040 收藏 1
文章标签： shell
原文链接：http://blog.51cto.com/12125295/1858795

0x00 下载运行dedeCMS.exe意见爆帐号密码

下载并运行dedeCMS.exe获取帐号和密码。

0x01 获取hash值对应的密码

资料可知，dedeCMS的密码hash是32位的hash截取来的，因此对其前三位和最后一位进行裁剪后可得到16位的hash。破解可得密码only_system。

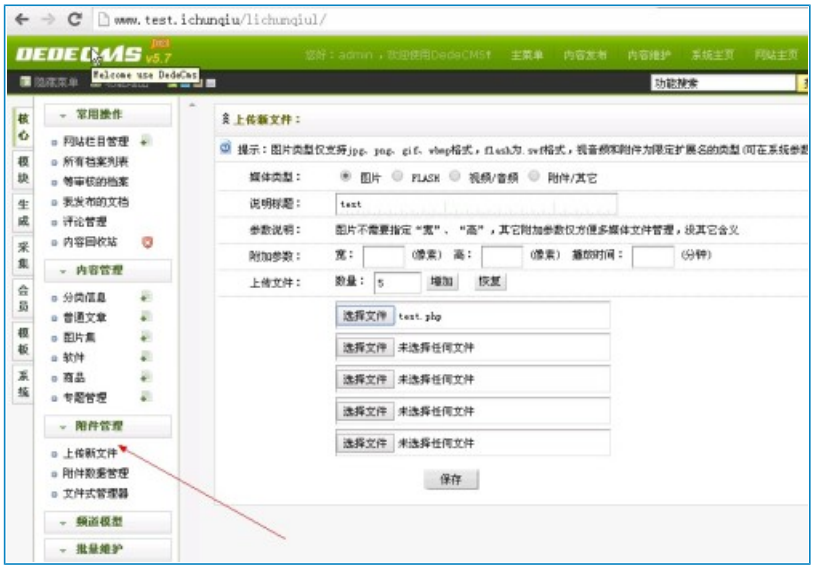
0x02 获取管理员后台目录

网上大量教程和经验总结获取后台的路径，但是绝大部分都是差之毫厘因此没有得到后台路径。

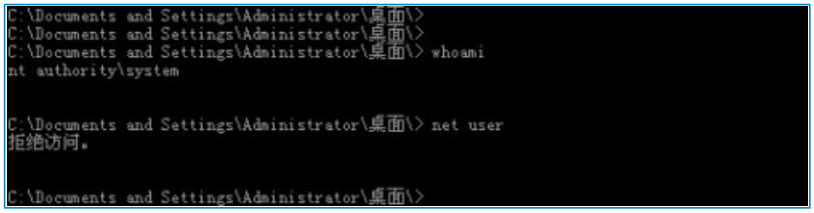
/data/mysql_error_trace.inc是各大经验教程总结的第一方法。但是在这个实验中不生效。最后获悉/data/mysqli_error_trace.inc才能爆破出路径。因为在这个实验环境中使用的mysqli函数集，因此也需要通过mysqli_error_trace.inc来爆破路径。

0x03 登录并获取shell

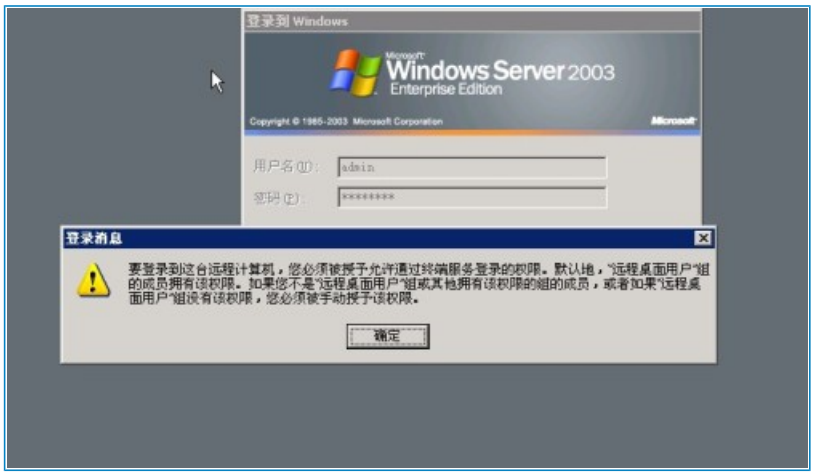
后台功能丰富，既有上传点也有修改上传附件限制的设置功能。对上传附件的限制进行修改，并进行上传获取shell。



0x04 连接shell初步探查主机

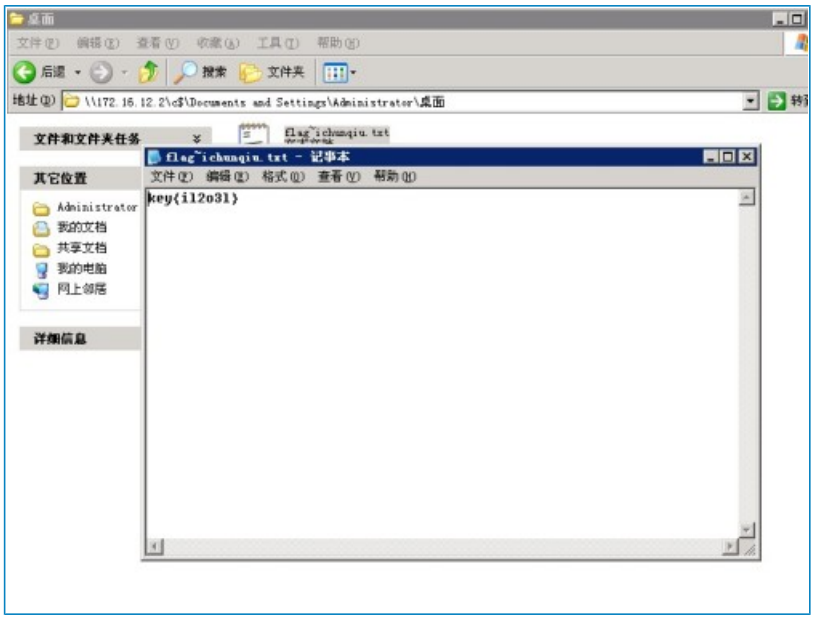


虽然是系统权限，但是做了一些限制。而且桌面上的flag文件也做了限制，无法通过type直接读取。自行上传net.exe实现net，直接修改ichunqiu的账户密码。



使用远程登录则发现所有账户都不在远程登录组里面。

0x05 通过共享获取flag文件



转载于:https://blog.51cto.com/12125295/1858795