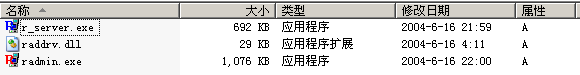
# radmin哈希提权

radmin是一款远控软件，免杀因为合法，可以上传到远程肉鸡进行控制，也可以借助他来提权，软件分为服务端和客户端，如下为2.2版的radmin



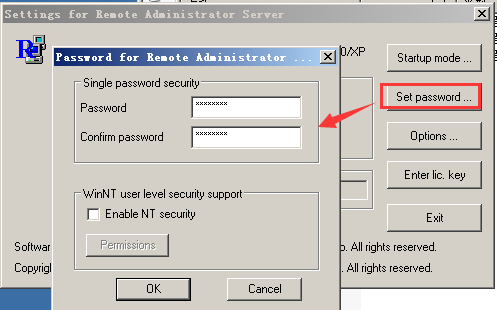
本次测试radmin的版本是2.2的，3.0的版本测试失败了，主要是注册表没有两个键

软件是收费的，当然也有破解版，不用注册也可以直接使用，如果作为后门木马，仅需要将

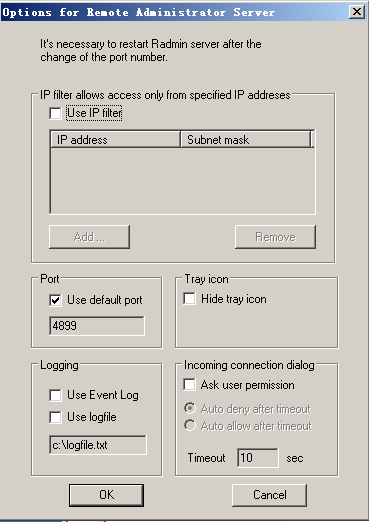
r\_server.exe和raddrv.dll上传到远端肉鸡就可以耍了，radmin.exe是客户端。

开始实验

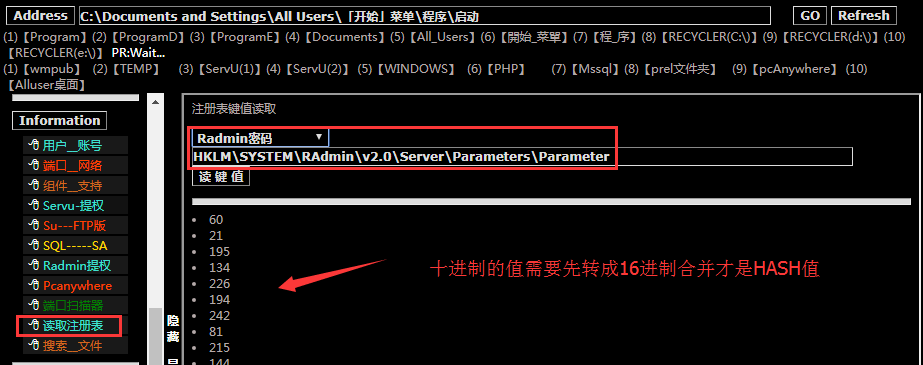
服务端开启radmin服务，默认监听端口为4899，如下图设置连接密码



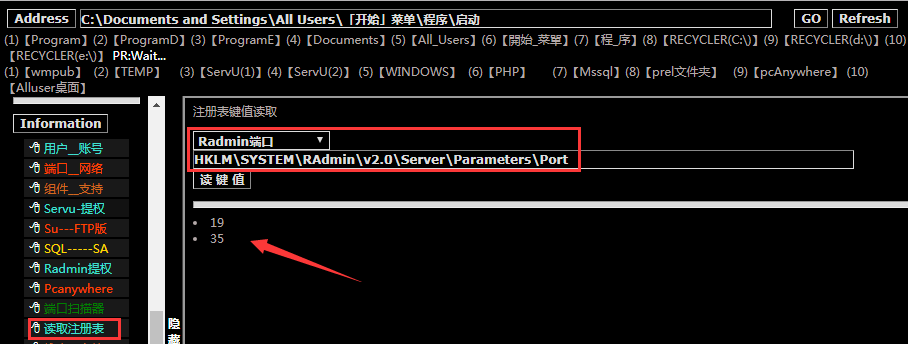
在option选项里可以设置端口号，黑白名单，和日志相关



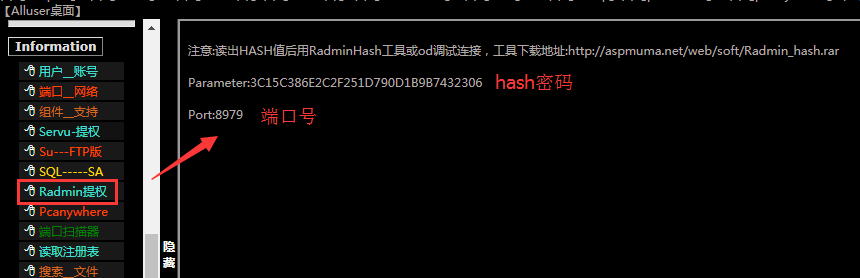
radmin的链接账号密码是用hash算法生成的，存放在注册表中，利用asp大马读取该值



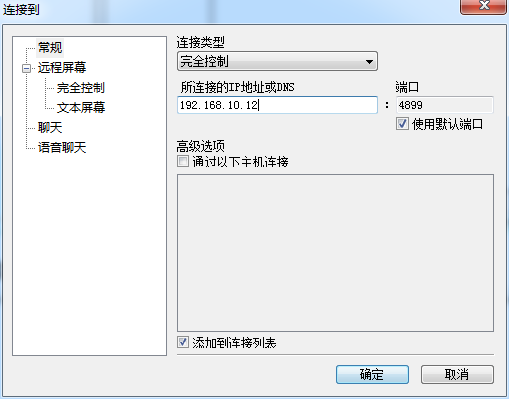
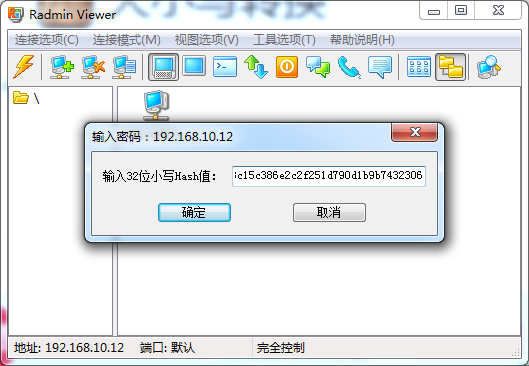
如果管理员更改了密码，也可以通过注册表读取端口号

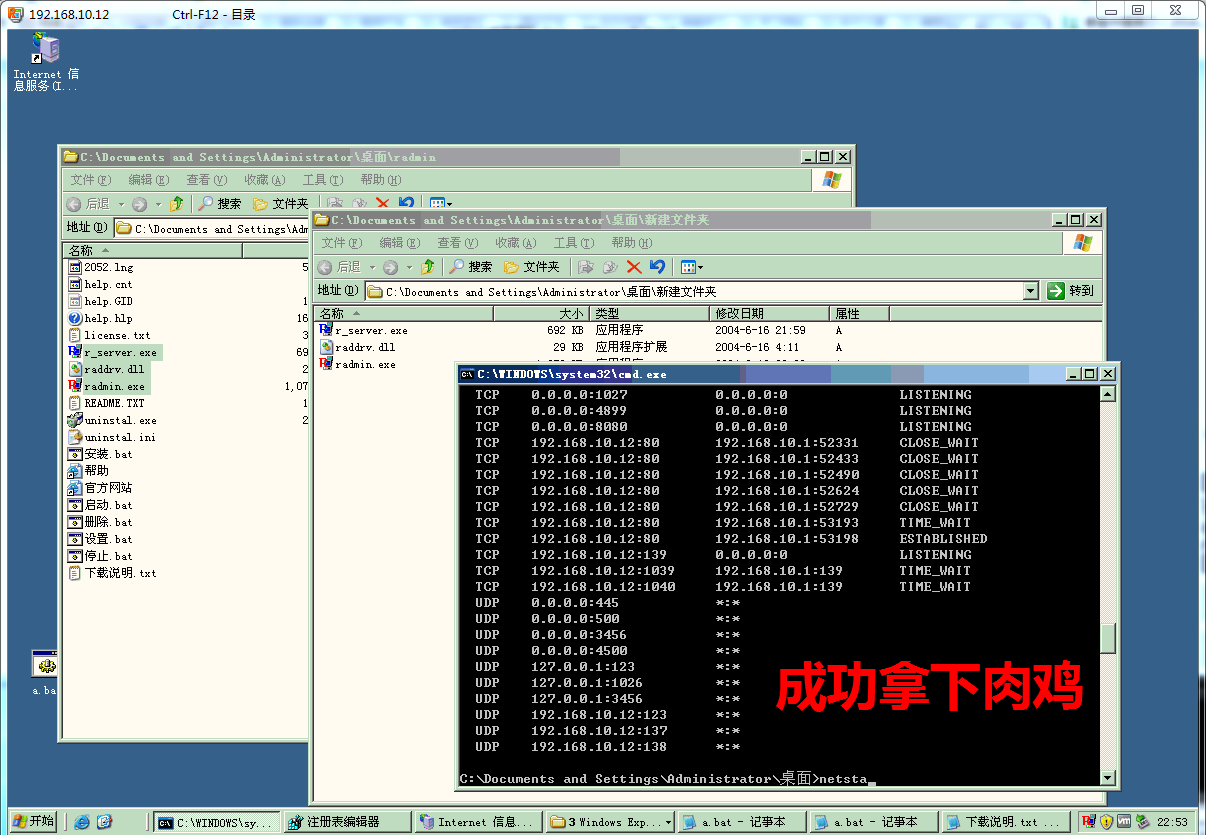


得到的这些值是十进制，需要转成16进制合并才是有效值，radmin提权模块自动完成显示

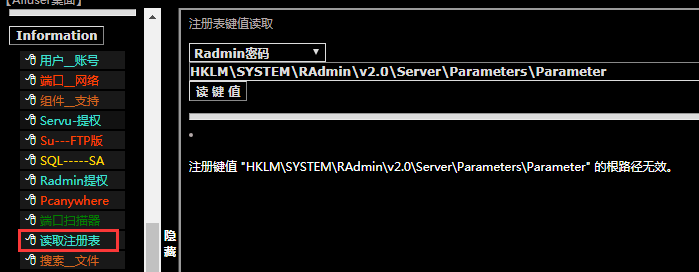


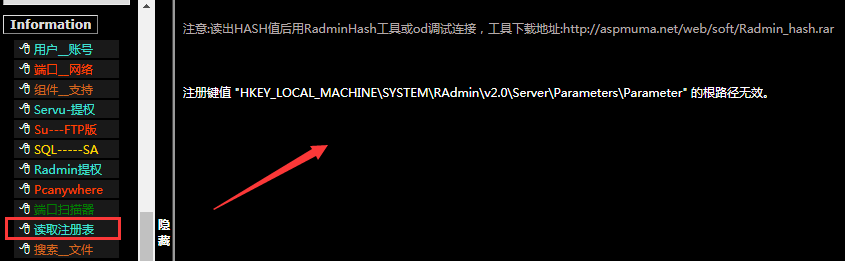
有了hash值可以利用一款著名的Radmin\_HASH 来连接远程，但作者偷懒所以hash值要转小写才行，在线大小写转换工具https://bigtosmall.51240.com/



当然大部分实验不一定如此顺利，下面是一些常见错误的分析，比如读取键值遇到下面情况



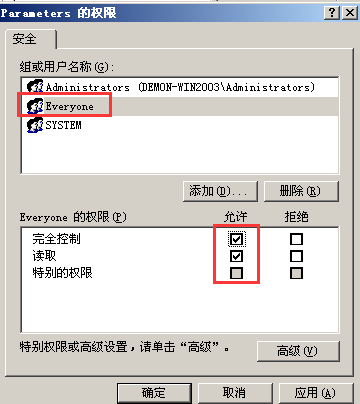
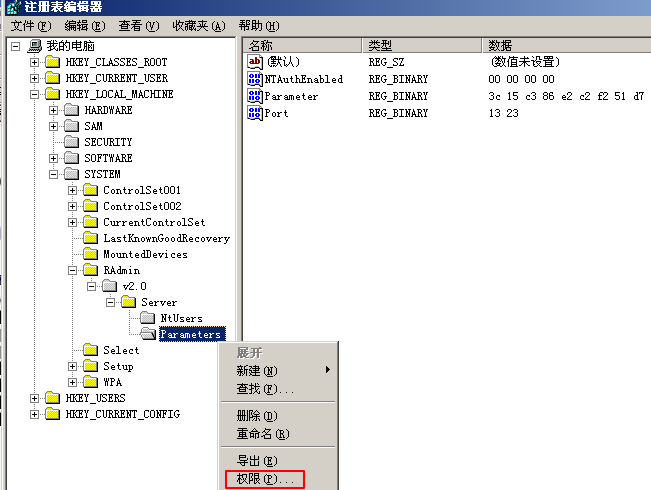


想到的两种可能，第一是下面两个读取端口和HASH的默认键值真的不存在，3.0版的就是

HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters\Port

HKLM\SYSTEM\RAdmin\v2.0\Server\Parameters\Parameter

第二种可能就是两个键值是存在的，但是没有相应的读取权限，如下注册表权限设置



有了everyone就可以读取了，但是一般情况很难在注册表上给到互联网来宾用户的权限

没有权限，基本上就读取不了了。

对于第一种可能的情况是因为版本号比如3.0的存放注册表位置不同，如果你知道存放的位置KEYS路径在哪，可以自己写一个Bat用asp大马文件上传，读取对应的KEYs值

bat代码如下：

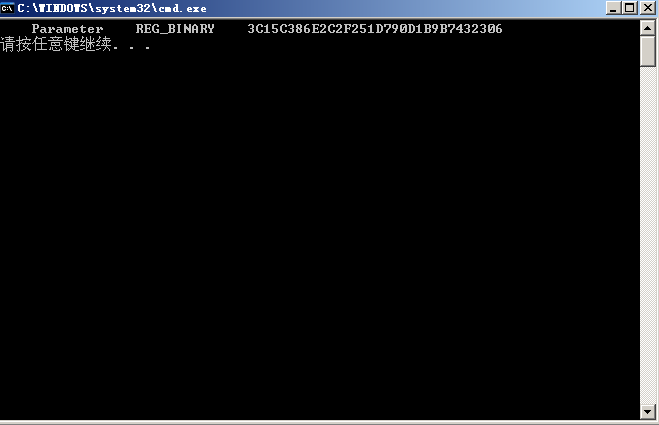
@echo off

For /f "delims=" %%i in

('Reg Query "HKEY\_LOCAL\_MACHINE\SYSTEM\RAdmin\v2.0\Server\Parameters" /v "Parameter" ') do Set a=%%i && echo %a%

echo %a% > 1.txt

pause



红色的文字就是Keys值得位置和名称，然后在大马上cmd.exe运行显示HASH值，当然前提还是得有权限。下面是关于本次实验的一些参考网址，有空可以看看。

http://www.361way.com/radmin-hash-loophole/2146.html

http://www.360doc.com/content/16/0309/10/30597078\_540693075.shtml

https://www.bugbank.cn/pwn/detail/57aaf57f720d432a348a05cb.html

最后再说几句：radmin-v3.0版本的软件挺好用的，有很多不错的功能，易用性也很高