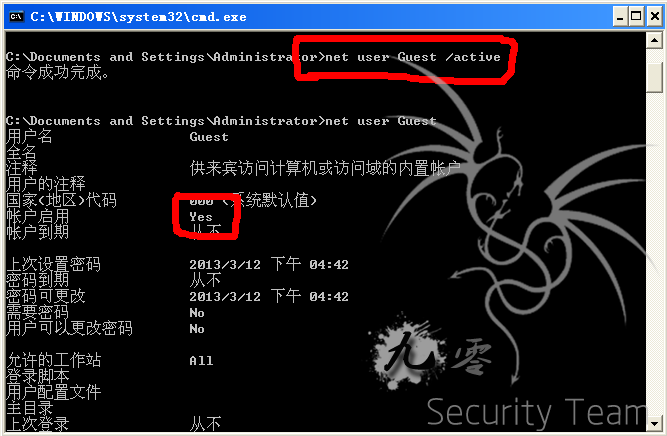
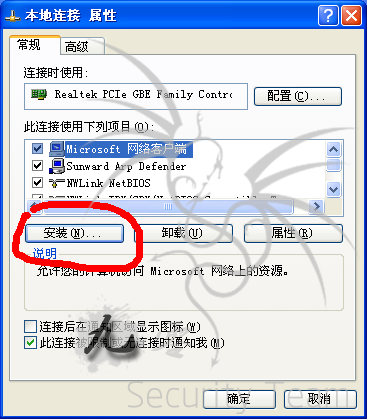
[**虚拟主机调用远程路径去执行CMD提权(转)**](http://www.cnblogs.com/demonspider/archive/2013/03/12/2956624.html)

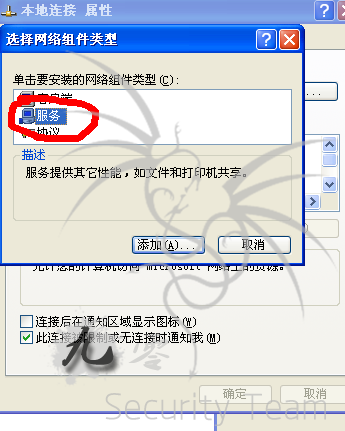
看见最近大家讨论远程调用cmd比较热，所以就想写一下自己使用远程调用CMD的一些小结

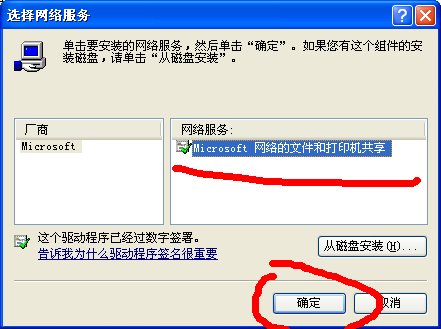
主要细节请参考 <http://lcx.cc/?i=3221>  
我以windows 2003系统做演示.  
1.激活本地Guest账号 

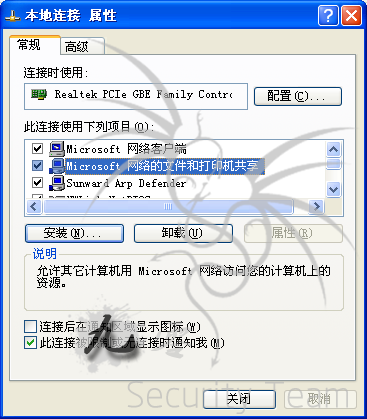
2.在组策略中将 网络访问: 本地帐户的共享和安全模型 改为经典 (2003系统默认为经典模式，不用修改) (gpedit.msc)

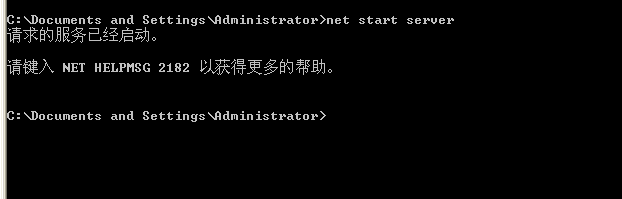
3.开启server服务,server服务就是网络共享需要的服务 看我的，本地没有server服务(这个要特别注意)  


我们去网络添加打印机协议即可. 

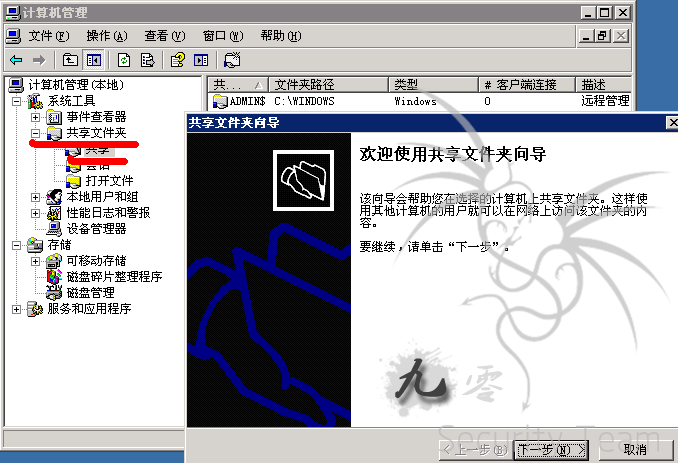


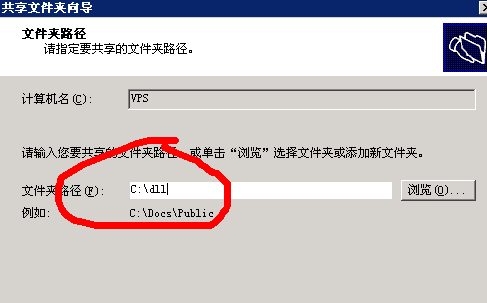


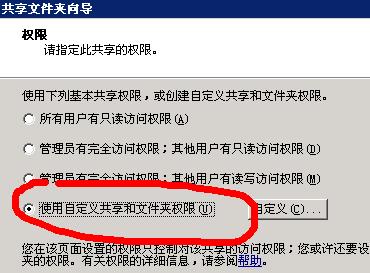
现在就安装成功了.  


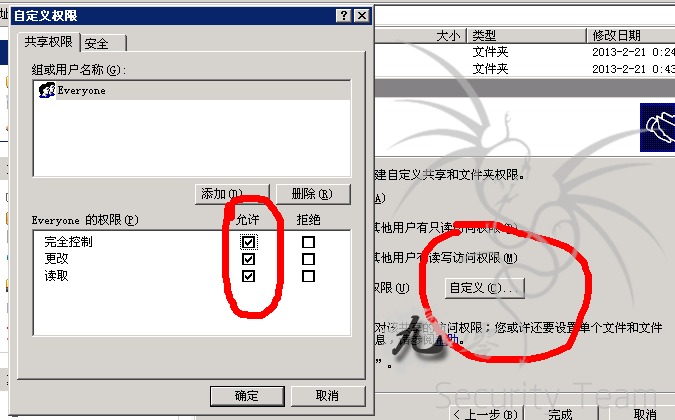
安装成功后默认自动启动server服务  


4.建立一个共享文件夹 

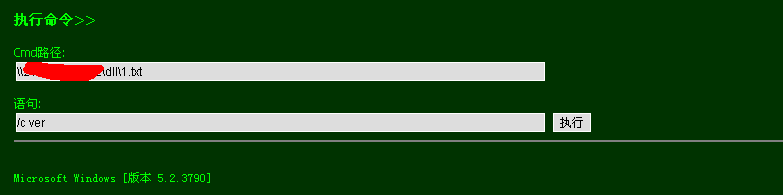










到此一切准备工作做完了.放进去个cmd。 我们来测试一下 

总结：（必看） 1.为什么我做完了上面的，我在我的shell上执行还是提示找不到网络路径？ 解释：托ms08-067的福，国内基本上445端口都被屏蔽了。一般情况445端口只允许城域网内相互访问。 2.我应该怎么利用？ 解释：拿下目标C段的一台服务器做肉鸡，其实不一定要C段的，服务器城域网内的都可以，比如一个机房的机子都可以。 3.要是我连C段的机子都日不下怎么办？ 解释：找抓鸡大牛去，他们知道哪些IP段的445端口没有被屏蔽。 对了不要忘记关闭肉鸡上的杀软什么的，这些都碍事。