为什么入侵 win2000 就非要用 IPC 通道或者终端服务器？今天我们来试试下面这既可图形监控, 又可文件传输, 还可 Telnet 的 “ 不三不四, 不伦不类，非马亦马 ” 的好东东，它就是 Remote Administrator v2.1 ，汉化版下载地址 http://www.hackervip.com/soft ，里面还有注册码。先在本机安装和注册 RemoteAdministrator ，（下面简称 Radmin）。

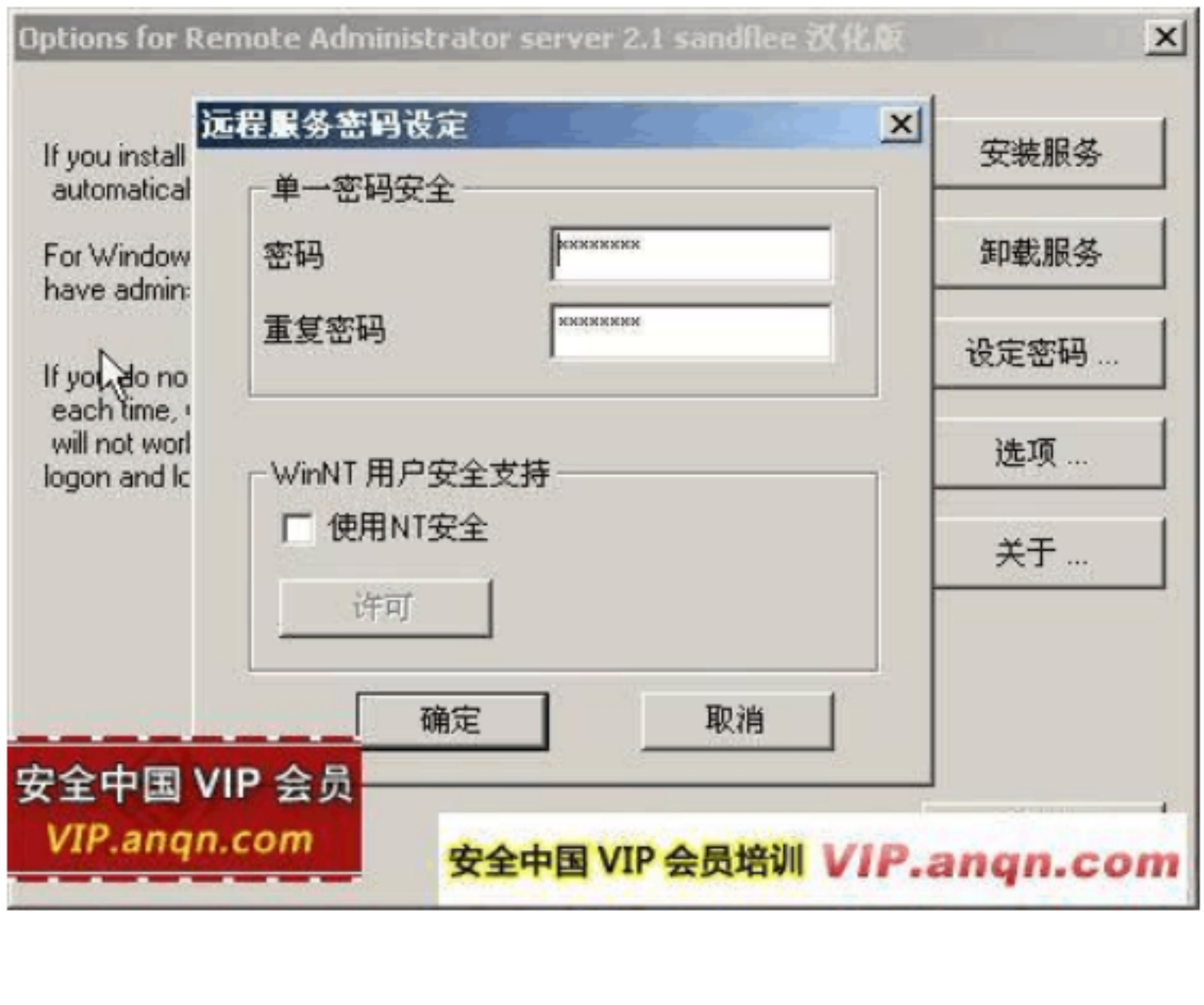
设置和启动 Radmin 服务端

一：先在本地设置 Radmin 的服务端 1 ：安装后在开始程序菜单打开 Settings for Remote Administrator server 来设置服务端

1：我们并不是真的在自己机器上安装这个服务，我们只是需要暂时用它来设置 Radmin 的服务端

www@bitscn@com

2：[设定密码] 。这里需要设置一个八位数的密码，以后你直接用这个密码就可直接操控肉鸡了

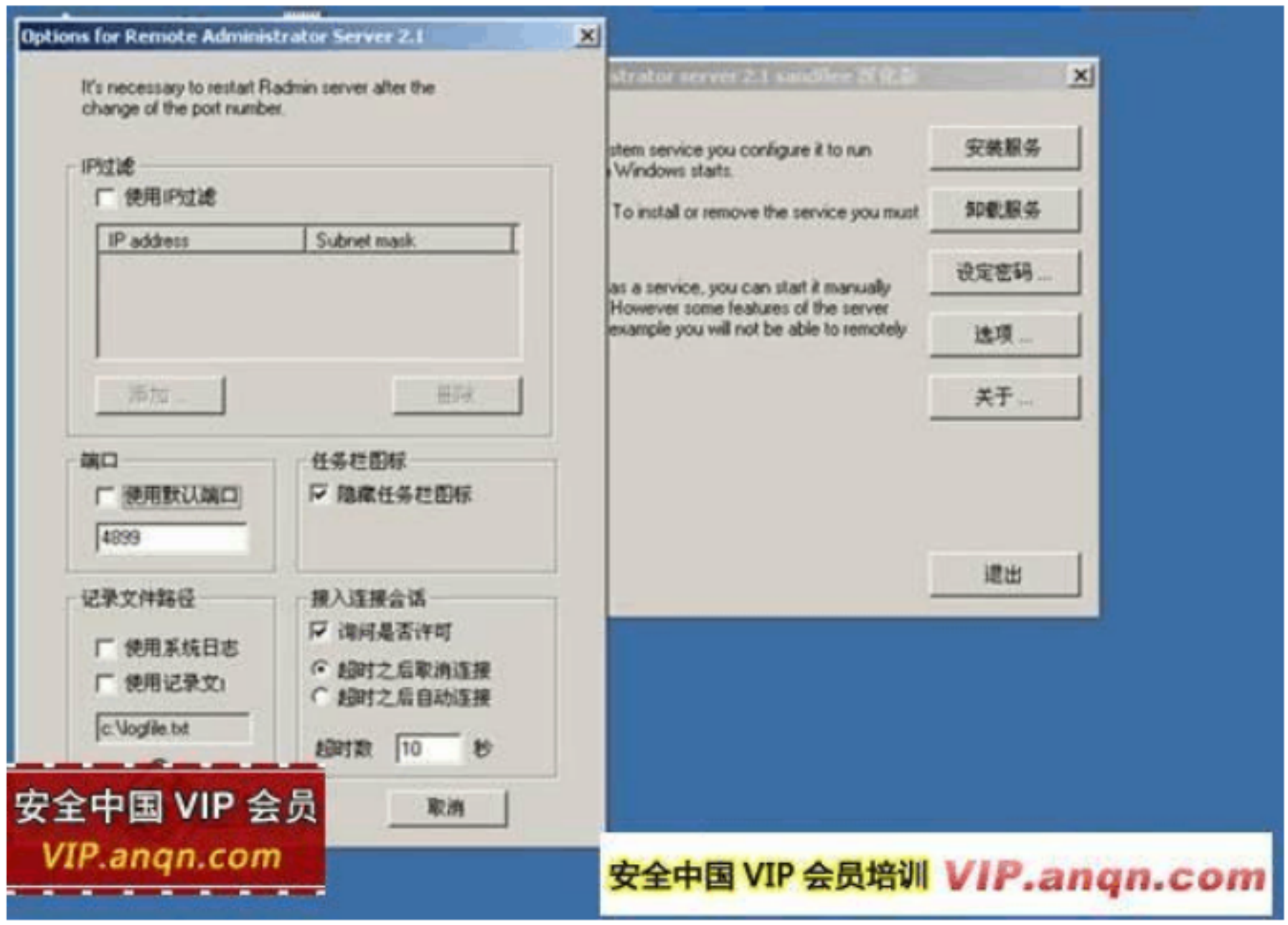


如果你想用 NT服务器的帐号登陆， 也可这里设置。 注意！ 这里可以设置肉鸡的任何组的帐号， 而且有全部的权限， 这样就跳过了 NT的帐号检查，

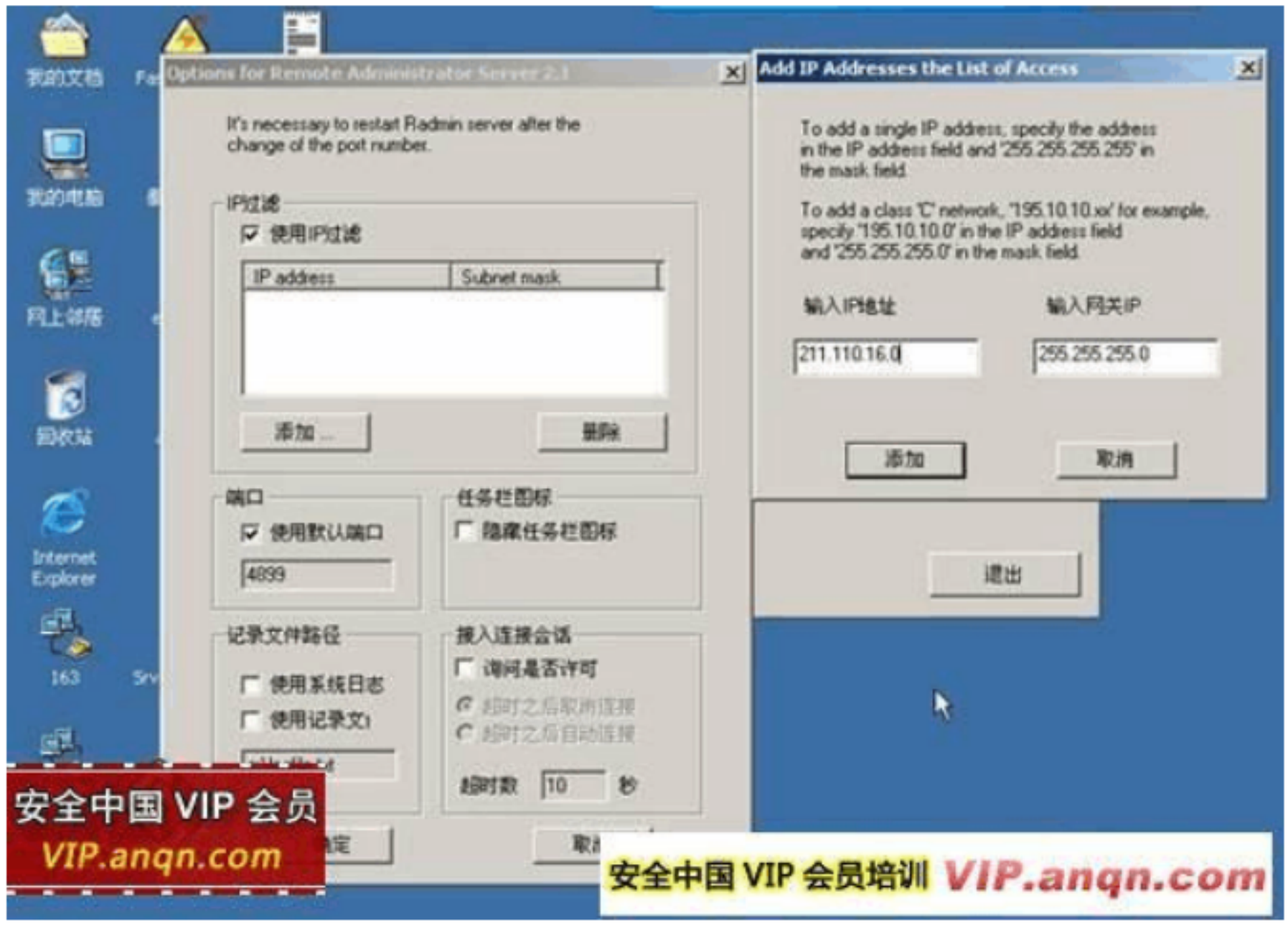
是不是像木马。

如果这样还需在 Access rights 里设置一下权限，一般我们选中 All access

All access　是代表全部允许　.



3 :[选项]‘ IP　过滤 ’可以设置允许连接的　　IP 地址（当然是自己的　IP 地址）, 可以是单个　IP 地址，如 211.110.16.241　, 网关设置成　255.255.255.254 就行了，当然也可以是　　C段 IP 地址，如 211.110.16.0　，网关设置成　255.255.255.0　就行了；‘ 端口 ’默认是　　4899，也可以自己设置为自己想要的端口，我设置的是　10258 ；



任务栏图标’一定要设置成隐藏！。还有，你可不要没事找事，把下面的日志和会话也选上！

4：为了得到设置好了的服务端文件，我们需要先在自己机器上安装一次服务端。

点击 [安装服务]

之后会在 c:\winnt\system32 目录里生成 r_server.exe 和 admindll.dll 文件，我们把这两个文件复制到一个目录，（不要现在就删掉，等会卸载可能要用到的！）

我们需要的正是这两个文件，r_server 和 admdll.dll 这两文件可以卸载服务端了。

卸载后就可以删掉那两个文件。

二：给肉鸡安装　Radmin 服务端

几个参数

/setup ---->　　图形界面安装服务

/pass:*** ---->　　设置密码

/port:1314 ---->　　服务端口　DL@bitsCN_com　网管软件下载

/install ---->　　命令行安装服务

/uninstall ---->　　删除服务

/save ---->　　保存服务设置

/silence ---->　　不要提示　--　这一个很有用哦！

/unregister ---->　　删除已经输入的注册码　　--　不知是什么意思？

注意：命令行下设置密码和端口优先于图形安装！

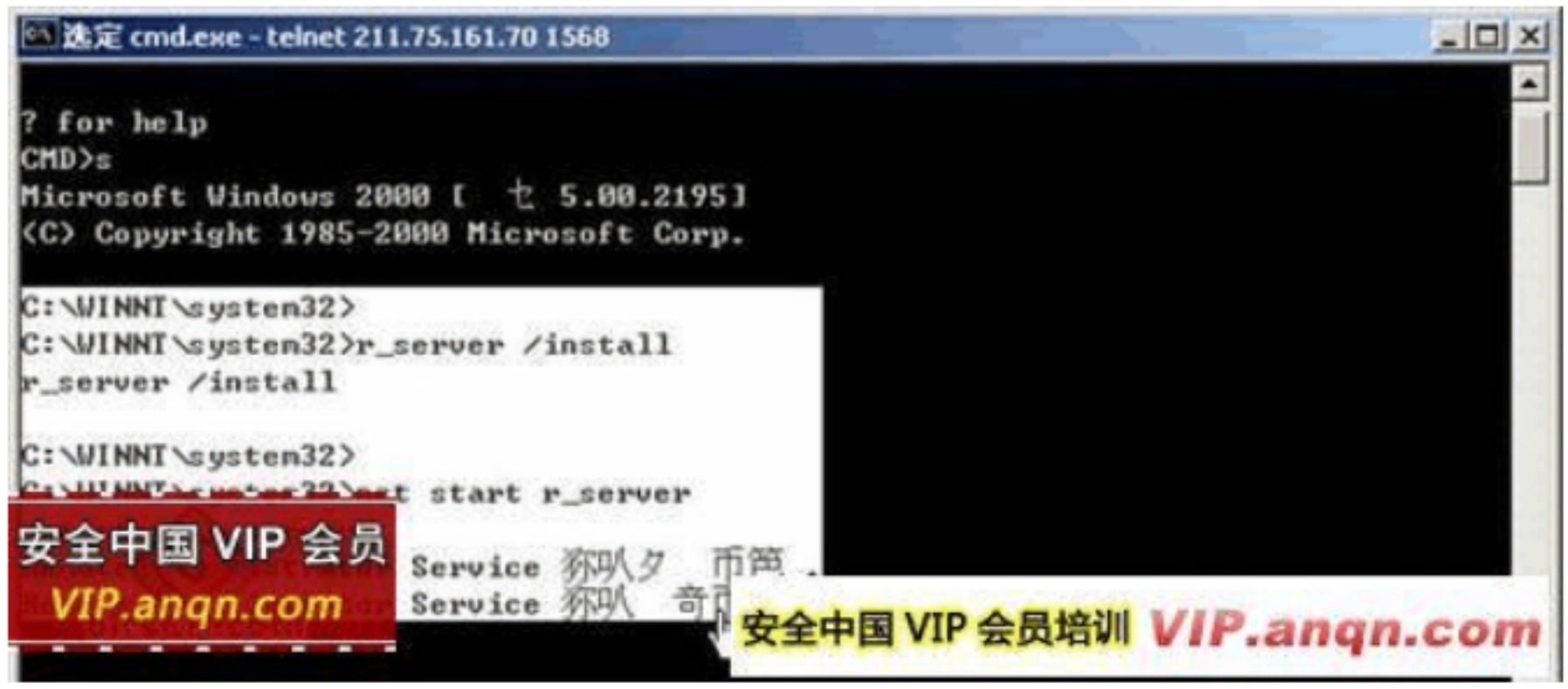
1：只要在自己机器上设置好了　　Radmin 服务端，上面的参数我们真正用到的只有　　/install　　。

随便找台你有　ADMIN权限肉鸡。呵呵，我试过　　Unicode　漏洞弄来的主机应该不行，至于怎么得到肉鸡不在这里多说。　　Telnet　进入它的命令行。

先用 tftp　或者别的方法把　r_server.exe　　和 admdll.dll　　上传到肉鸡　c:\admin$\system32　　目录下。

2： r_server /install　　安装　Radmin 服务。　3 ：net start r_server

启动　Radmin 服务



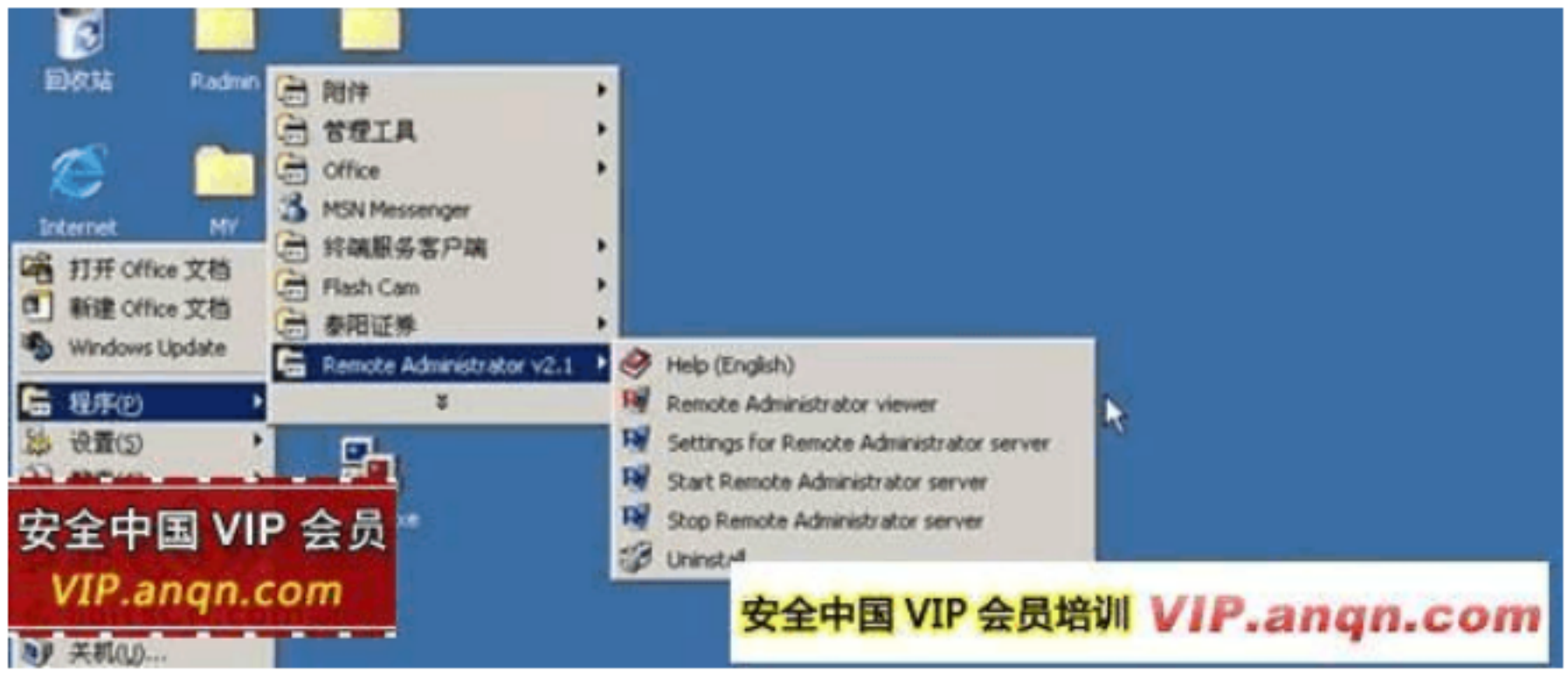
出现上面这个画面就是启动成功啦！如果出现有　　NET HELPMSG bitsCN.nET* 中国网管博客

2182 等等则表示没有成功哦。

GOOD Radmin 服务全部设置完毕。

远程控制肉鸡

打开 Remote Administrator viewer　　连接器来添加肉鸡



按工具栏第二个图标，把肉鸡　　IP 和服务端口填上点确定

然后在这个主机上点右键可以分别看

完全控制]-- 你动鼠标它也动的，管理员在的话可不要动。 www_bitscn_com 中国．网管联盟

[监视]-- 只看不动，最好用这个先观察一翻；

[Telnet]-- 调用了 M$ Win 的 Telnet 服务

[文件传输] —速度快稳定性能高

这些服务全都是用你设置的那一个端口。很像木马