操作系统权限介绍

权限提升简称提权,顾名思义就是提升自己在目标系统中的权限。现在的操作系统都是多用户操作系统,用户之间都有权限控制,比如通过Web漏洞拿到的是web进程的权限,往往Web服务都是以一个权限很低的账号启动的,因此通过 Webshell进行一些操作会受到限制,这就需要将其提升为管理,提权一般分为这么几种情况

```
1、windows系统下的提权
2、linux系统下的提权
3、数据库系统下的提权
4、利用第三方软件提权
```

接下来介绍一下不同操作系统的权限

Windows权限介绍

windows提权一般是提权到administrator或者system权限

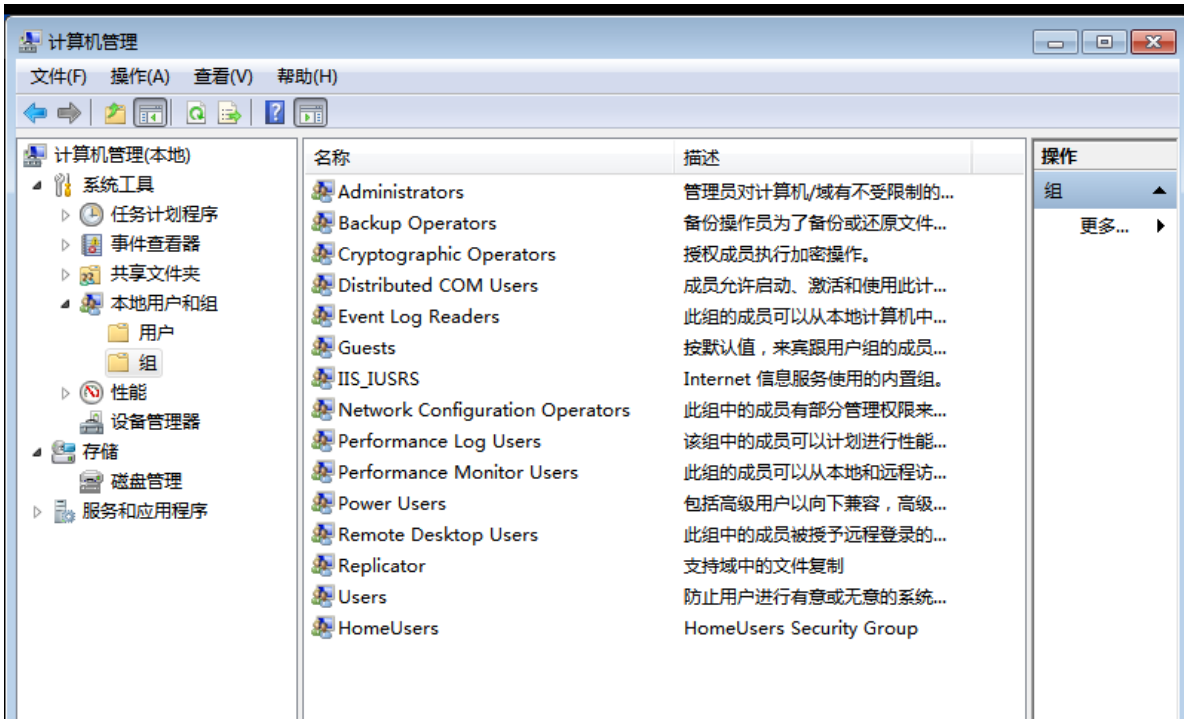
Windows用户帐户

windows中的用户账号一般分为以下几个

```
1、本地普通用户
2、本地一般管理员
3、本地最高管理员
4、域内普通用户
4、域内管理员
```

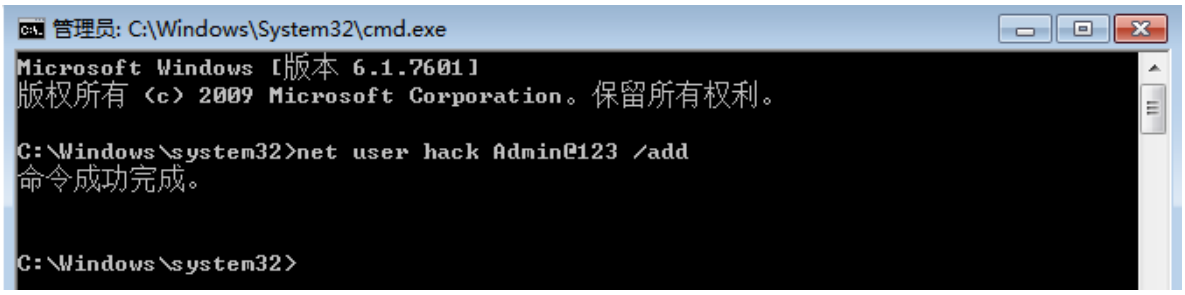
本地普通用户

本地普通用户，就是在windows电脑中本地新建的普通用户。没有管理员的权限，一般很多操作执行不了，需要管理员认证后才可以执行，以下是windows用户组，新建的用户一般默认是user组



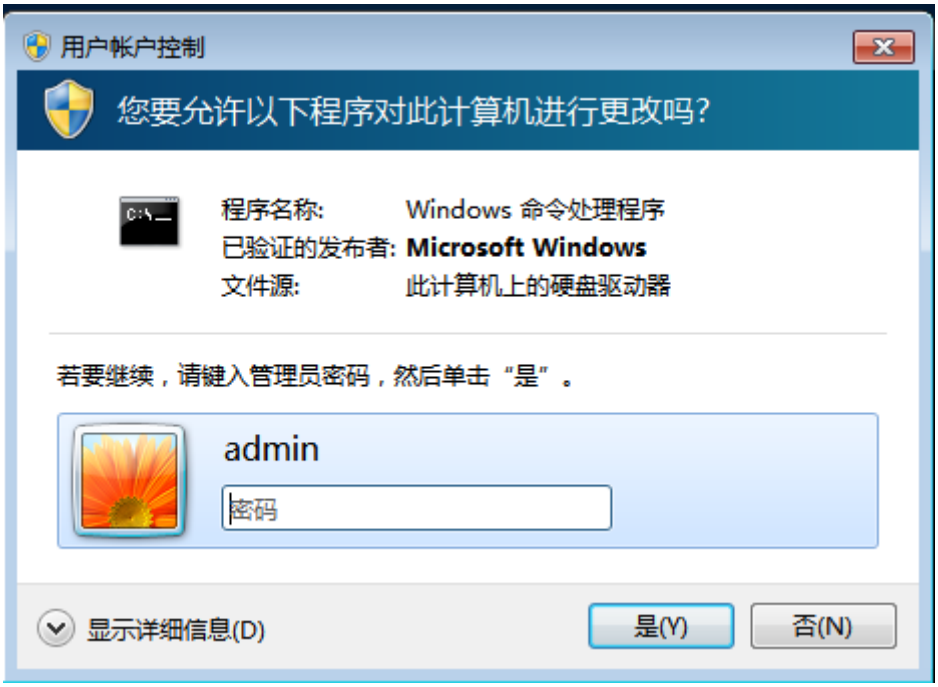
使用以下命令创建一个用户（必须是管理员打开的CMD）

```
net  user  hack Admin@123 /add
```



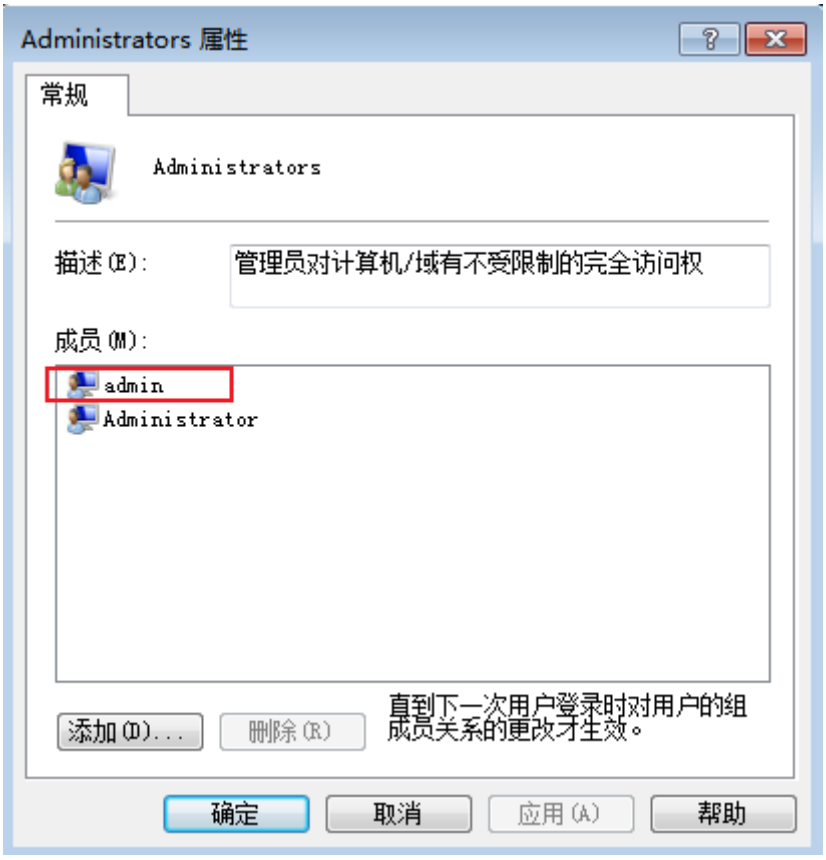
登录普通用户

当我们进行高权限的操作时候会出现以下的认证（需要输入管理员的账号和密码才可以）此时就需要提权

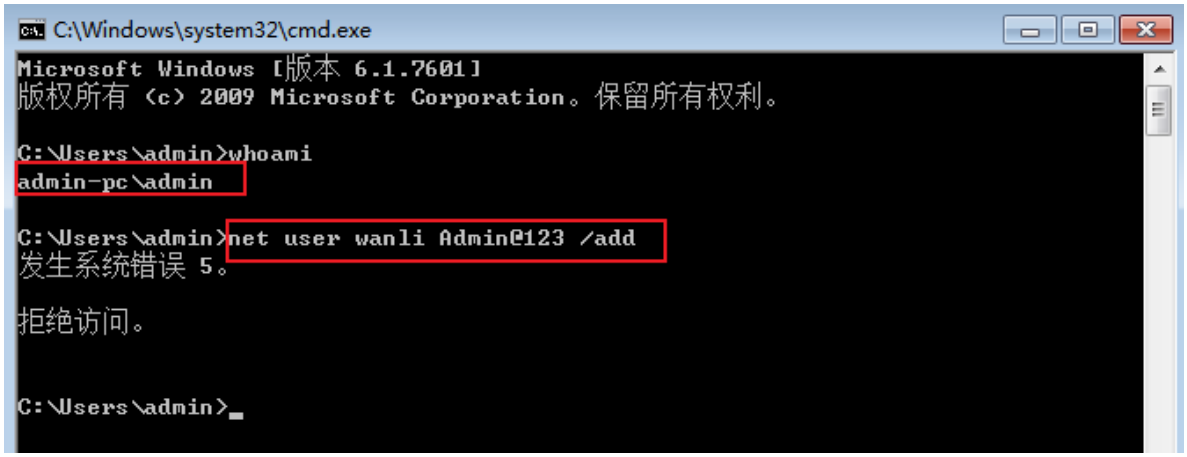


本地一般管理员

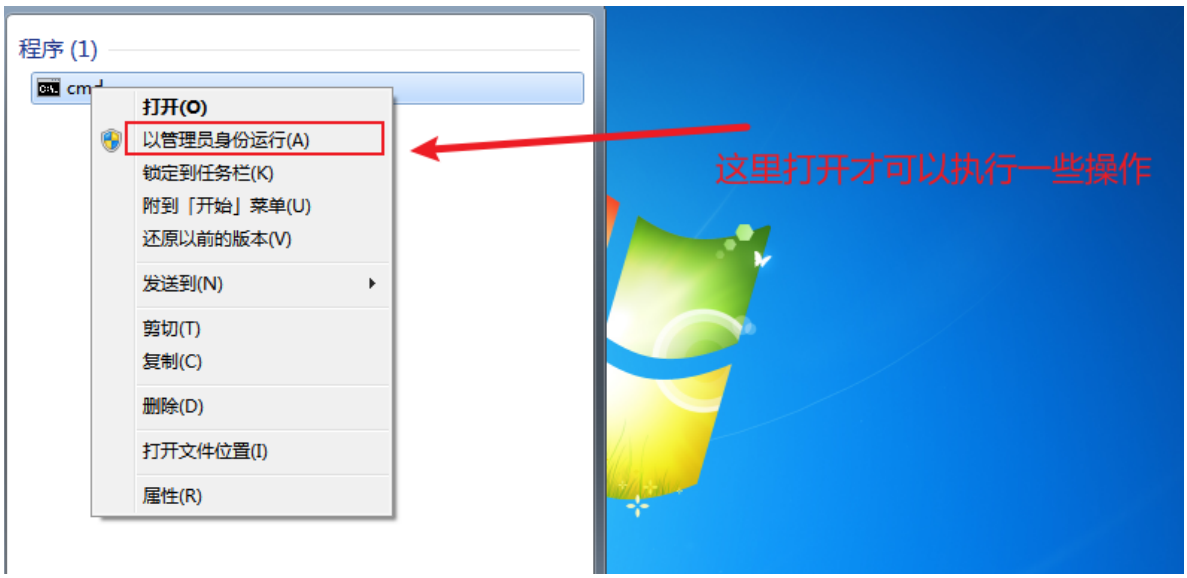
本地一般管理员就是加入了administratorts组的管理员但不是administrator用户



admin用户虽然也是管理员，但是有些操作也是执行不了的，因为有UAC，



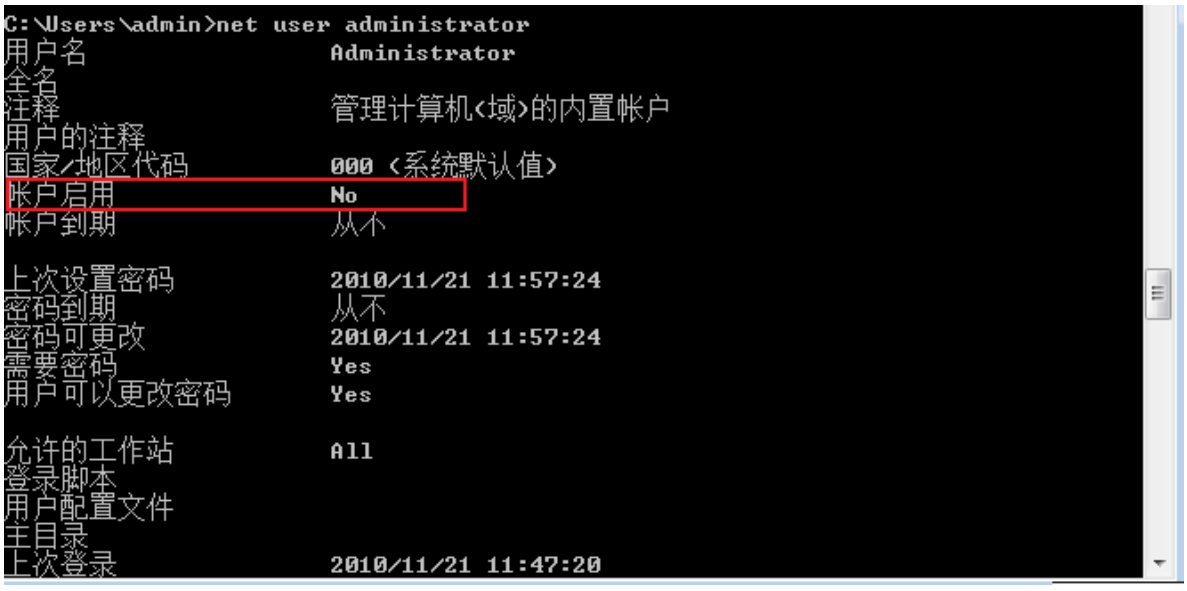
如果要执行高权限的操作必须右键使用管理员打开



本地最高管理员

本地用户最高管理员是administrator在windows电脑中administrator用户在一些版本电脑中是禁用的，如下

```
windows server  默认开启administrator
windows 家庭版，旗舰版  默认不开启administrator
windows 企业版，专业版  默认开启administrator
```



开启和关闭administrator

```
net user administrator /active:yes  开启
net user administrator /active:no   禁用
```

域内普通用户

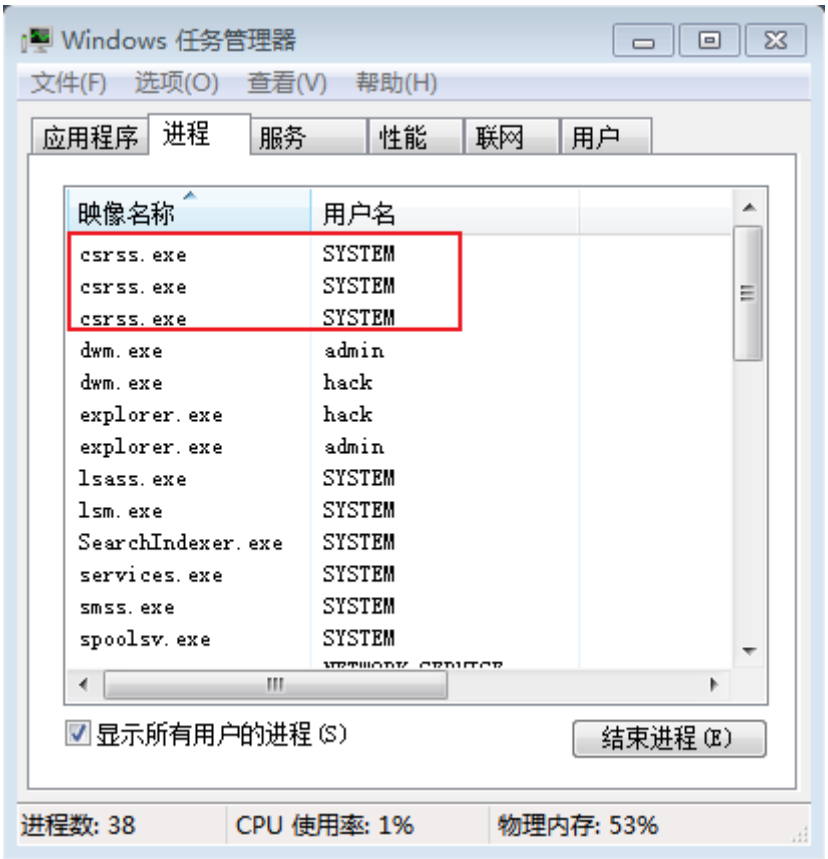
```
C:\Users\liwei>whoami
xyz\liwei
```

域内管理员

```
C:\Users\Administrator>whoami
hack\administrator
```

Windows服务账号

服务帐户用于在Windows中运行服务。服务帐户不能用于登录Windows系统。system是服务账号的最高权限，administrator是管理员用户，一般你平时运行的程序都是以这个权限身份运行的，你平时安装软件什么什么的、修改系统设置都是以这个权限操作的，system权限是系统自己的权限，任务管理器里面只要是以system这个用户名运行的程序都是系统本身的程序，比如任务管理器里面的winlogon.exe、svchost.exe、alg.exe这些进程等等，而不是你运行的程序



Linux权限介绍

linux提权就是将普通的用户提权到root用户

passwd文件

Linux 系统中的 /etc/passwd 文件，是系统用户配置文件，存储了系统中所有用户的基本信息，并且所有用户都可以对此文件执行读操作。

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
systemd-coredump:x:999:996:systemd Core Dumper:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
tss:x:59:59:Account used by the trousers package to sandbox the tcsd daemon:/
dev/null:/sbin/nologin
polkitd:x:998:995:User for polkitd:/:/sbin/nologin
unbound:x:997:994:Unbound DNS resolver:/etc/unbound:/sbin/nologin
chrony:x:996:993::/var/lib/chrony:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rngd:x:995:992:Random Number Generator Daemon:/var/lib/rngd:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
www:x:1000:1000::/home/www:/bin/bash
```

shadow文件

密码保存在 /etc/shadow的文件中，这个文件只有root用户能够读取，其他用户都无法读取该文件。

```
root:$6$GC215cnos$8UWojFMcndFVlbeHNUBZ1.ghLdTVmHjPM1bgQcJEw2YcZpmcnsdMpNWeQ3/Dwl0o4.TAyPPOKxeb0KMLrFUnb1:19220:0:9
9999:7:::
bin:*:18573:0:99999:7:::
daemon:*:18573:0:99999:7:::
adm:*:18573:0:99999:7:::
lp:*:18573:0:99999:7:::
sync:*:18573:0:99999:7:::
shutdown:*:18573:0:99999:7:::
halt:*:18573:0:99999:7:::
mail:*:18573:0:99999:7:::
operator:*:18573:0:99999:7:::
games:*:18573:0:99999:7:::
ftp:*:18573:0:99999:7:::
nobody:*:18573:0:99999:7:::
dbus:!!:19048::::::
systemd-coredump:!!:19048::::::
systemd-resolve:!!:19048::::::
tss:!!:19048::::::
polkitd:!!:19048::::::
unbound:!!:19048::::::
chrony:!!:19048::::::
sshd:!!:19048::::::
rngd:!!:19048::::::
nscd:!!:19048::::::
postfix:!!:19048::::::
tcpdump:!!:19048::::::
rpc:!!:19048:0:99999:7:::
rpcuser:!!:19048::::::
www:!!:19222:0:99999:7:::
```