Using WMI to query and monitor Windows devices

Introduction

NMIS uses WMIC to query Windows devices using remote WMI. You will fine the WMIC binary in /usr/local/nmis8/bin/wmic (or /usr/local/nmis9/bin/wmic).

Windows and WMIC are a little "picky" about the input fields they will accept and work with. Unless you have it "just right", you won't get the expected result.

The Opmantek team have done some testing around this, our findings are below.

General Use of WMIC

The standard command to use WMIC is below.

```
./wmic -U SHORTDOMAIN/USERNAME%PASSWORD //TARGET QUERY
```

Translating this into an actual example, we have

```
./wmic -U WINDEVDOMAIN/administrator%my_admin_password //192.168.1.2 "SELECT * FROM Win32_ComputerSystem"
```

Attributes

The attributes are describe in more detail below.

SHORTDOMAIN

This is the Windows short domain name. It is **not** the fully qualified domain. IE, mydomain, *not* mydomain.open-audit.com. It is often referred to as the NetBios Name.

The SHORTDOMAIN can be omitted and the query will validate the credentials against the local machine being queried.

The SHORTDOMAIN can be invalid and the query will validate the credentials against the local machine being queried.

If the SHORTDOMAIN is valid, the credentials will be validated against the Active Directory domain.

USERNAME

The user supplied to WMIC must have access to remote WMI queries.

If the target computer is not on a domain, in general it **must** be the Adminitrator account that is used.

The SHORTDOMAIN and USERNAME can be supplied as either SHORTDOMAIN/USERNAME or USERNAME@SHORTDOMAIN.

More info - https://docs.microsoft.com/en-us/windows/win32/wmisdk/user-account-control-and-wmi?redirectedfrom=MSDN

PASSWORD

WMI itself cannot cater to password that contain both single and double quotes. It is recommended to avoid these characters altogether in the password.

Using a pipe character in the password is also fraught with danger. Obviously the pipe character | directs the output of one command into another in the Linux shell. The can be avoided when using th eshell by enclosing the entire password in double quotes.

```
WINDEVDOMAIN/administrator%"my|admin|password"
```

TARGET

The target Windows computer should be specified as either the IP address or the hostname only (that must resolve in DNS).

Providing a FQDN to the target even if DNS resolves it, will not work as Windows relies on netbios for some aspects of authentication with Linux does not provide.

QUERY

Standard WMI queries are catered to. For more information, see the WMI reference at Microsoft - https://docs.microsoft.com/en-us/windows/win32/wmisdk/wmi-reference

Example

On the command line.

```
marku@test:/usr/local/nmis8/bin$ ./wmic -U WINDEVDOMAIN/administrator%my_admin_password //10.152.0.40 "Select *
from Win32_OperatingSystem"
CLASS: Win32_OperatingSystem
BootDevice|BuildNumber|BuildType|Caption|CodeSet|CountryCode|CreationClassName|CSCreationClassName|CSDVersion|CS
Name|CurrentTimeZone|DataExecutionPrevention_32BitApplications|DataExecutionPrevention_Available|DataExecutionPr
evention_Drivers|DataExecutionPrevention_SupportPolicy|Debug|Description|Distributed|EncryptionLevel|ForegroundA
pplicationBoost|FreePhysicalMemory|FreeSpaceInPagingFiles|FreeVirtualMemory|InstallDate|LargeSystemCache|LastBoo
tUpTime|LocalDateTime|Locale|Manufacturer|MaxNumberOfProcesses|MaxProcessMemorySize|MUILanguages|Name|NumberOfLi
censedUsers|NumberOfProcesses|NumberOfUsers|OperatingSystemSKU|Organization|OSArchitecture|OSLanguage|OSProductS
uite|OSType|OtherTypeDescription|PAEEnabled|PlusProductID|PlusVersionNumber|PortableOperatingSystem|Primary|Prod
uctType|RegisteredUser|SerialNumber|ServicePackMajorVersion|ServicePackMinorVersion|SizeStoredInPagingFiles|Stat
us|SuiteMask|SystemDevice|SystemDirectory|SystemDrive|TotalSwapSpaceSize|TotalVirtualMemorySize|TotalVisibleMemo
rySize|Version|WindowsDirectory
\Device\HarddiskVolume2|14393|Multiprocessor Free|Microsoft Windows Server 2016
Datacenter|1252|1|Win32_OperatingSystem|Win32_ComputerSystem|(null)
|WINNOW|0|True|True|True|3|False||False|256|2|2444088|943512|3478896|20201021053937.000000+000|0|20210531040349.
499770+000|20210604010119.214000+000|0409|Microsoft Corporation|4294967295|137438953344|(en-US)|Microsoft
Windows Server 2016 Datacenter|C:\Windows|\Device\Harddisk0\Partition3|0|57|8|8|(null)|64-bit|1033|400|18|(null)
|False|(null)|(null)|False|True|3|(null)|00376-40000-00000-AA947|0|0|1048576|OK|400|\Device\HarddiskVolume3|C:
\Windows\system32|C:|0|5241572|4192996|10.0.14393|C:\Windows
```

Using WMI with NMIS Attributes

The Windows user account being used ***must*** be a member of the Administrators group on the target device. By default, members of the active directory group "Domain Admins" are members of the clients Administrators group. Your specific Active Directory may have another Active Directory group you would prefer to use. As long as the user account is a member of the Administratos group on the target machine, it should work fine at least as far as access rights are concerned.

Use the IP address of the target in ***Host Name/IP Address*** field.

Use shortdomain/username in the ***WMI Username*** field.

Use your password in the ***WMI Password*** field.

Other useful links

Connecting to WMI remotely - https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-remotely-starting-with-vista?redirectedfrom=MSDN

Target Client Configuration (from the Open-AudIT wiki)

Connecting to WMI on a Remote Computer - https://docs.microsoft.com/en-us/windows/win32/wmisdk/connecting-to-wmi-on-a-remote-computer