Andrea Fortuna

Just some random thoughts about the Meaning of Life, The Universe, and Everything

About | Cybersecurity | Music

Windows Command Line cheatsheet (part 2): WMIC

August 9, 2017

This command-line tool is really useful for both penetration testing and forensics tasks

The previous article *has raised interest in readers regarding WMIC.*
So I decided to write an article dedicated to this tool.

If you've done any scripting for the Windows platform, you've probably bumped into the Windows Management Instrumentation (WMI) scripting API, which can be used to enumerate all kinds of information.

The WMIC command-line tool is basically another front-end to access the WMI framework, with the added bonus that numerous queries are pre-defined.
The pre-defined queries mean that you won't necessarily need to spend any time learning the WMI Query Language (WQL), which is syntactically similar to SQL.

WMIC is included in the default installation of Windows XP (excluding Home edition) and Windows Server 2003. Although WMIC is not included on Windows 2000, you can still usea Windows XP or Server 2003 client to remotely query Windows 2000 systems and receive similar results.

The first time you run WMIC you'll see a message that WMIC is beinginstalled, but no media is required for installation, nor will anything appear in the Add/Remove Programs

Basic WMIC Usage

Most WMIC commands are issued in the following format:

```
wmic [credentials] [area] [querystring]
```

For example, you can collect a list of groups on the local system using the following command:

```
wmic group list brief
```

which will return output similar to this:

```
Caption Domain Name SID

Lab7\Administrators Lab7 Administrators S-1-5-32-544

Lab7\Backup Operators Lab7 Backup Operators S-1-5-32-551

Lab7\Guests Lab7 Guests S-1-5-32-546

Lab7\Network Configuration Operators Lab7 Network Configuration Operators S

Lab7\Power Users Lab7 Power Users S-1-5-32-547

Lab7\Remote Desktop Users Lab7 Remote Desktop Users S-1-5-32-555

Lab7\Replicator Lab7 Replicator S-1-5-32-552
```

You can also perform the same data collection over the network without ever logging into the remote machine provided you know have some administrative credentials that the remote system will accept.

The same command issued against a remote system in another domain looks like this:

```
wmic /user:"FOREIGN_DOMAIN\Admin" /password:"Password" /node:192.168.33.25
```

and the output is

```
Caption Domain Name SID

REMOTE-DESK\Administrators REMOTE-DESK Administrators S-1-5-32-544

REMOTE-DESK\Backup Operators REMOTE-DESK Backup Operators S-1-5-32-551

REMOTE-DESK\Guests REMOTE-DESK Guests S-1-5-32-546

REMOTE-DESK\Network Configuration Operators REMOTE-DESK Network Configurati

REMOTE-DESK\Power Users REMOTE-DESK Power Users S-1-5-32-547

REMOTE-DESK\Remote Desktop Users REMOTE-DESK Remote Desktop Users S-1-5-32-

REMOTE-DESK\Replicator REMOTE-DESK Replicator S-1-5-32-552

REMOTE-DESK\Users REMOTE-DESK Users S-1-5-32-545

REMOTE-DESK\HelpServicesGroup REMOTE-DESK HelpServicesGroup S-1-5-21-789336

REMOTE-DESK\__vmware__ REMOTE-DESK __vmware__ S-1-5-21-789336058-1078081533
```

```
FOREIGN_DOMAIN\RAS and IAS Servers FOREIGN_DOMAIN RAS and IAS Servers S-1-5
2568877423-583830540-553
FOREIGN_DOMAIN\HelpServicesGroup FOREIGN_DOMAIN HelpServicesGroup S-1-5-21-
2568877423-583830540-1000
FOREIGN_DOMAIN\TelnetClients FOREIGN_DOMAIN TelnetClients S-1-5-21-19481207
FOREIGN_DOMAIN\DnsAdmins FOREIGN_DOMAIN DnsAdmins S-1-5-21-1948120765-25688
FOREIGN_DOMAIN\DnsUpdateProxy FOREIGN_DOMAIN DnsUpdateProxy S-1-5-21-194812
FOREIGN_DOMAIN\Domain Admins FOREIGN_DOMAIN Domain Admins S-1-5-21-19481207
FOREIGN_DOMAIN\Domain Computers FOREIGN_DOMAIN Domain Computers S-1-5-21-19
FOREIGN_DOMAIN\Domain Controllers FOREIGN_DOMAIN Domain Controllers S-1-5-2
FOREIGN_DOMAIN\Domain Guests FOREIGN_DOMAIN Domain Guests S-1-5-21-19481207
FOREIGN_DOMAIN\Domain Users FOREIGN_DOMAIN Domain Users S-1-5-21-1948120765
FOREIGN_DOMAIN\Enterprise Admins FOREIGN_DOMAIN Enterprise Admins S-1-5-21-
FOREIGN_DOMAIN\Group Policy Creator Owners FOREIGN_DOMAIN Group Policy Crea
FOREIGN_DOMAIN\Schema Admins FOREIGN_DOMAIN Schema Admins S-1-5-21-19481207
FOREIGN_DOMAIN\Shared FOREIGN_DOMAIN Shared S-1-5-21-1948120765-2568877423-
```

Note that you can issue ANY of the of the WMIC commands over the network in this fashion as a means of gathering information about the host. Now that we’ve seen the

WMIC in Vulnerability and Penetration Testing

In vulnerability and penetration testing, system footprinting is key. The more information that can be collected about a specific system or group of systems, the greater the likelihood that those systems can be compromised.

Granted, using WMIC requires administrative access on the remote host, but since most IT departments maintain standard images for each collection or group of workstations and servers, information you can obtain from one host is likely to be applicable to other similar systems.

Furthermore, for default configurations of the event log and auditing processes, WMIC requests won't be logged, so all of your enumerations can be undertaken in stealth mode.

The following are examples of useful information we can collect through WMIC.

Processes

WMIC can collect a list of the currently running processes similar to what you'd see in "Task Manager" using the following command:

```
wmic process list
```

Note that some of the WMIC built-ins can also be used in "brief" mode to display a less verbose output. The process built-in is one of these, so you could collect more refined output using the command:

```
wmic process list brief
wmic process call create "calc.exe"
```

- Terminate an Application

```
wmic process where name="calc.exe" call terminate
```

- Change Process Priority

```
wmic process where name="explorer.exe" call setpriority 64
```

- Get List of Process Identifiers

```
wmic process where (Name='svchost.exe') get name,processid
```

- Find a specific Process

```
wmic process list brief find "cmd.exe"
```

System Information and Settings

You can collect a listing of the environment variables (including the PATH) with this command:

```
wmic /output:c:os.html os get /format:hform
```

- Products/Programs Installed Report HTML Formatted

```
wmic /output:c:product.html product get /format:hform
```

- Turn on Remoted Desktop Remotely

```
Wmic /node:"servername" /user:"user@domain" /password: "password" RDToggle
```

- Get Server Drive Space Usage Remotely

```
WMIC /Node:%%A LogicalDisk Where DriveType="3" Get DeviceID,FileSystem,Free
```

- Get PC Serial Number

```
wmic /node:"HOST" bios get serialnumber
```

- Get PC Product Number

```
wmic /node:"HOST" baseboard get product
wmic STARTUP GET Caption, Command, User
```

- Reboot or Shutdown

```
wmic os where buildnumber="2600" call reboot
```

- Get Startup List

```
wmic startup list full
```

- Information About Harddrives

```
wmic logicaldisk where drivetype=3 get name, freespace, systemname, filesys
```

- Information about os

```
wmic os get bootdevice, buildnumber, caption, freespaceinpagingfiles, insta
```

- Information about files

```
wmic path cim_datafile where "Path='\windows\system32\wbem\' and FileSize>1
wmic useraccount list
```

```
wmic group list
```

```
wmic sysaccount list
```

For domain controllers, this should provide a listing of all user accounts and groups in the domain. The “sysaccount” version provides you with system accounts built-in and otherwise,which is useful for any extra accounts that may have been added by rootkits.

- Identify any local system accounts that are enabled (guest, etc.)

```
wmic USERACCOUNT WHERE "Disabled=0 AND LocalAccount=1" GET Name
```

- Number of Logons Per USERID

```
wmic netlogin where (name like "%skodo") get numberoflogons
```

- Get Domain Names And When Account PWD set to Expire

```
WMIC UserAccount GET name,PasswordExpires /Value
```

Patch Management

```
wmic qfe list
```

The QFE here stands for “Quick Fix Engineering”.
The results also include the dates of install should that be needed from an auditing standpoint.

Shares

Enumeration of all of the local shares can be collected using the command:

```
wmic share list
```

The result will also include hidden shares (named with a $ at the end).

- Find user-created shares (usually not hidden)

```
wmic SHARE WHERE "NOT Name LIKE '%$'" GET Name, Path
```

Networking

Use the following command to extract a list of network adapters and IP address information:

```
wmic nicconfig list
```

- Get Mac Address:

- Update static IP address:

```
wmic nicconfig where index=9 call enablestatic("192.168.16.4"), ("255.255.2
```

- Change network gateway:

```
wmic nicconfig where index=9 call setgateways("192.168.16.4", "192.168.16.5
```

- Enable DHCP:

```
wmic nicconfig where index=9 call enabledhcp
```

- Get List of IP Interfaces

```
wmic nicconfig where IPEnabled='true'
```

Services

WMIC can list all of the installed services and their configurations using this command:

```
wmic service list
```

The output will include the full command used for starting the service and its verbose description.

- Service Management

```
 wmic service where caption="DHCP Client" call changestartmode "Disabled"
```

- Look at services that are set to start automatically

```
wmic SERVICE WHERE StartMode="Auto" GET Name, State
```

- Services Report on a Remote Machine HTML Formatted:

```
wmic /output:c:services.htm /node:server1 service list full / format:htable
```

- Get Startmode of Services

```
Wmic service get caption, name, startmode, state
```

- Change Start Mode of Service:

```
wmic service where (name like "Fax" OR name like "Alerter") CALL ChangeStar
```

- Get Running Services Information

Of course, these are just samplings of the dozens of predefined aliases within WMIC. You can also go beyond the predefined aliases using WQL queries to collect and set any of themany thousands of parameters accessible through WMI.

WMIC in Forensics

In forensics, it’s often important to get as much information about the running system as possible before the system can be shut down.
You’d also like to collect that information while keeping close records that account for your own actions and leave the smallest footprint possible on the system.
Though WMIC wa sn’t really designed with this in mind, it certainly works.

Since WMIC is included by default on most Windows systems and can be executed remotely, that makes it all the more desirable.

Another interesting feature of WMIC is its ability to record the run-time command executed and runtime configuration all in one XML file. A recorded session might look something like this:

```
wmic /record:users_list.xml useraccount list
```

Of course, since WMIC wasn’t designed as a recording device, there are some caveats to using the XML. First, you can only use XML output, there are no other formats defined.

Event logs

- Obtain a Certain Kind of Event from Eventlog

```
wmic ntevent where (message like "%logon%") list brief
wmic nteventlog where (description like "%secevent%") call cleareventlog
```

Retrieve list of warning and error events not from system or security logs

```
WMIC NTEVENT WHERE “EventType < 3 AND LogFile != ‘System’ AND LogFile != ‘S
```

References

- **Understanding WMI Scripting: Exploiting Microsoft’s Windows Management Instrumentation in Mission…**
- **Windows Command Line cheatsheet (part 1): some useful tips**
- **WMIC – Take Command-line Control over WMI**

Related posts

1. How to detect Cobalt Strike Beacons using Volatility
2. How to process recent Windows 10 memory dumps in Volatility 2
3. OSX Forensics: a brief selection of useful tools
4. How to extract forensic artifacts from Linux swap
5. Linux Forensics: Memory Capture and Analysis