Windows_wmic

WMIC (Windows Management Instrumentation Command-line) ### Wmic.exe The WMIC utility is a Microsoft tool that provides a WMI command-line interface that is used for a variety of administrative functions for local and remote machines and also for wmic queries, such as system settings, stop processes and run scripts locally or remotely. Therefore, it can invoke the XSL script (eXtensible Stylesheet Language).

wmic is enable in windows 7,8,10,11

this used for the wmic(help_command)
wmic /?
used for the bios info
wmic bios list /format

wmic CPU list/format
wmic CPU /?
wmic CPU get Architecture,Name
wmic Desktop list/format
wmic DESKTOPMONITOR list/format
wmic NETLOGIN list/format
wmic NIC list/format:xml
wmic NIC list/format:hform
wmic NIC list/format:hform > NIC.html
wmic server
wmic startup
wmic qfe

Get System Roles, User Name, and Manufacturer

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

Get the SIDs

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

Create a process

wmic process call create "taskmgr.exe"

Terminate a process

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

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

Locate System Files

Extract paths of all the important system files like temp folder, win directory and much more.
wmic environment get Description, VariableValue

Get a list of Installed Applications

wmic product get name

Get a list of Running Services

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

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

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:list

Get OS Details

wmic os get CurrentTimeZone, FreePhysicalMemory, FreeVirtualMemory, LastBootUpdate, NumberofProcesses, NumberofUsers, Organization, Registereduser, Status /format:list

Rename a user account

We can rename a local user by using **useraccount alias**
wmic useraccount where name='demo' rename hacker

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, productState, pathToSignedProductExe

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

https://www.hackingarticles.in/post-exploitation-using-wmic-system-command/