WMIC

COMMAND LIST

Spot Odd Executables	– wmic PROCESS WHERE “NOT ExecutablePath LIKE ‘%Windows%'” GET ExecutablePath
Look at services that are set to start automatically	– wmic SERVICE WHERE StartMode=”Auto” GET Name, State
Find user-created shares (usually not hidden)	– wmic SHARE WHERE “NOT Name LIKE ‘%$'” GET Name, Path
Find stuff that starts on boot	– wmic STARTUP GET Caption, Command, User
Identify any local system accounts that are enabled (guest, etc.)	– wmic USERACCOUNT WHERE “Disabled=0 AND LocalAccount=1” GET Name”
Change Start Mode of Service	– wmic service where (name like “Fax” OR name like “Alerter”) CALL ChangeStartMode Disabled
Number of Logons Per USERID	– wmic netlogin where (name like “%skodo”) get numberoflogons
Obtain a Certain Kind of Event from Eventlog	– wmic ntevent where (message like “%logon%”) list brief
Clear the Eventlog (Security example)	– wmic nteventlog where (description like “%secevent%”) call cleareventlog
Get Mac Address	– wmic nic get macaddress
Reboot or Shutdown	– wmic os where buildnumber=”2600” call reboot
Update static IP address	– wmic nicconfig where index=9 call enablestatic(“192.168.16.4”), (“255.255.255.0”)
Change network gateway	– wmic nicconfig where index=9 call setgateways(“192.168.16.4”, “192.168.16.5”),(1,2)
Enable DHCP	– wmic nicconfig where index=9 call enabledhcp
Service Management	– wmic service where caption=”DHCP Client” call changestartmode “Disabled”
Start an Application	– 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
Information About Harddrives	– wmic logicaldisk where drivetype=3 get name, freespace, systemname, filesystem, size, volumeserialnumber
Information about os	– wmic os get bootdevice, buildnumber, caption, freespaceinpagingfiles, installdate, name, systemdrive, windowsdirectory /format:htable > c:\osinfo.htm
Information about files	– wmic path cim_datafile where “Path=’\\windows\\system32\\wbem\\’ and FileSize>1784088” > c:\wbemfiles.txt

Process list	– wmic process get /format:htable > c:\process.htm
Retrieve list of warning and error events not from system or security logs	– WMIC NTEVENT WHERE “EventType<3 AND LogFile != ‘System’ AND LogFile != ‘Security’” GET LogFile, SourceName, EventType, Message, TimeGenerated /FORMAT:”htable.xsl”:” datatype = number”:” sortby = EventType” > c:\appevent.htm
Total Hard Drive Space Check	– wmic LOGICALDISK LIST BRIEF
Get Running Services Information	– Wmic service where (state=”running”) get caption, name, startmode, state
Get Startmode of Services	– Wmic service get caption, name, startmode, state
Get Domain Names And When Account PWD set to Expire	– WMIC UserAccount GET name,PasswordExpires /Value
Get Hotfix and Security Patch Information	– WMIC QFE GET /format:CSV >QFE.CSV
Get Startup List	– wmic startup list full
Find a specific Process	– wmic process list brief find “cmd.exe”
Get List of IP Interfaces	– wmic nicconfig where IPEnabled=’true’
Change IP Address	– wmic nicconfig where Index=1 call EnableStatic (“10.10.10.10”), (“255.255.255.0”)
OS/System Report HTML Formatted	– wmic /output:c:\os.html os get /format:hform
Products/Programs Installed Report HTML Formatted	– wmic /output:c:\product.html product get /format:hform
Services Report on a Remote Machine HTML Formatted	- wmic /output:c:\services.htm /node:server1 service list full / format:htable
Turn on Remoted Desktop Remotely!	– Wmic /node:”servername” /user:”user@domain” /password: “password” RDToggle where ServerName=”server name” call SetAllowTSConnections 1
Get Server Drive Space Usage Remotely	– WMIC /Node:%%A LogicalDisk Where DriveType=”3” Get DeviceID,FileSystem,FreeSpace,Size /Format:csv MORE /E +2 >> SRVSPACE.CSV
Get PC Serial Number	– wmic /node:”HOST” bios get serialnumber
Get PC Product Number	– wmic /node:”HOST” baseboard get product
Get Services for Remote Machine in HTML Format	– wmic /output:c:\services.htm /node:server1 service list full / format:htable