Windows Commands for Security Analysts

1. System Informations Configuration

systeminfo

Displays detailed OS configuration, hardware, patches (hotfixes).

systeminfo

systeminfo | findstr /B /C:"OS Name" /C:"OS Version" /C:"System Type" (Quick OS details)#

systeminfo /s <remote_hostname> (Query remote system - requires permissions)

whoami

Displays current user context.

whoami (Current user)

whoami /groups (Group memberships)

whoami /priv (User privileges - essential for capability assessment) **(Admin Required often needed to see all)**

whoami /fqdn (Fully qualified domain name) whoami /all

(Combines user, groups, privileges)

hostname

Displays the computer's hostname.

```
hostname
```

ver / winver

Displays Windows version.

```
ver (Command-line version)
winver (GUI window with build number)
```

getmac

Displays MAC address(es).

```
getmac /v (Verbose, shows adapter name)
```

bcdedit

Manages Boot Configuration Data. **(Admin Required)**

```
bcdedit /enum all (Check for unusual boot entries)
```

driverquery

Displays installed device drivers.

driverquery (Basic list)

driverquery /v (Verbose, includes signature info) driverquery /si (Signed drivers)

msinfo32

Opens System Information GUI (comprehensive hardware/software info).

msinfo32 (Opens GUI)

msimsinfo32 /report C:\temp\sysinfo.txt (Saves report to file)nfo32 (Opens GUI)

path

Displays or sets the command search path.

path

wmic

(Windows Management Instrumentation Command-line *- Note: Being deprecated, PowerShell's Get-CimInstance is preferred, but wmic is still widely used/encountered)*

wmic os get Caption,Version,BuildNumber,OSArchitecture

wmic product get name,version (Installed software - can be slow)

wmic qfe list brief (Quick Fix Engineering - installed patches) wmic process list brief (Running processes)

wmic logicaldisk get caption,description,filesystem,size,freespace

wmic useraccount list brief

wmic netlogin get name,lastlogon (Requires permissions)

Attacker Usage Examples (Detection & Understanding): wmic

/node:"<target>" process call create "cmd.exe /c <command>" (Remote exec)

wmic startup create Name="evil", Command="C:\path\payload.exe" (Persistence)

wmic process where name="calc.exe" delete (Terminate process)

powercfg

Manages power settings.

powercfg /a (Shows available sleep states)

powercfg /energy (Generates energy efficiency report, can reveal issues)

powercfg /lastwake (Shows what woke the system)

fsutil

File system utility.

fsutil fsinfo drives (List drives)

fsutil fsinfo volumeinfo C: (Detailed volume info)

fsutil dirty query C: (Check if volume is marked 'dirty') **(Admin Required)**

fsutil usn readjournal C: (Read USN change journal - advanced forensics) **(Admin Required)**

set

Displays, sets, or removes environment variables.

set (Show all variables)
set PROCESSOR_ARCHITECTURE (Show specific variable)

msconfig

Opens System Configuration utility (boot options, services, startup).

msconfig (Opens GUI)

2. Network Analysis Configuration

ipconfig

Displays IP configuration.

ipconfig (Basic IP/Subnet/Gateway)
ipconfig /all (Detailed info including MAC, DNS, DHCP)
ipconfig /displaydns (Show DNS resolver cache contents)
ipconfig /flushdns (Clear DNS resolver cache) **(Admin Required)**
ipconfig /registerdns (Register DNS name and IP) **(Admin Required)**
ipconfig /release & ipconfig /renew (DHCP operations)

ping

Tests network connectivity using ICMP Echo requests.

ping 8.8.8.8
ping -n 20 <hostname_or_ip> (Send 20 pings)
ping -t <hostname_or_ip> (Ping continuously until stopped)

netstat

Displays network connections, listening ports, statistics.

netstat -ano (Show TCP/UDP, listening ports, IPs/ports, PIDs) netstat -anob (Like -ano but includes executable name - can be slow) **(Admin Required)**

netstat -p tcp -ano (Filter by protocol)

netstat -r (Show routing table, similar to route print) netstat -e (Ethernet statistics)

netstat -s (Per-protocol statistics)

tracert

Traces the route (hops) to a destination.

tracert 8.8.8.8

tracert -d <hostname_or_ip> (Do not resolve addresses to hostnames - faster)

pathping

Combines ping and tracert, showing latency and packet loss at each hop over time. More informative than tracert but slower.

pathping 8.8.8.8

pathping -n -q 15 google.com (No hostname resolution, 15 queries per hop)

nslookup

Queries DNS servers.

nslookup google.com (Basic A record lookup)

nslookup -type=mx google.com (Query for MX records)

nslookup google.com 8.8.8.8 (Query using a specific DNS server) nslookup (Interactive mode)

arp

Displays and modifies the Address Resolution Protocol (ARP) cache (IP-to-MAC mapping).

arp -a (Show current ARP entries)

arp -d * (Delete ARP cache entries) (Admin Required)

netsh

(Network Shell): Powerful network configuration tool. **(Admin Required for most modifications)**

netsh interface ip show config (Alternative to ipconfig)

netsh advfirewall firewall show rule name=all (Show all firewall rules)

netsh advfirewall set currentprofile state off (Disable firewall for current profile - **use caution!**)

netsh wlan show profiles (List saved Wi-Fi profiles)

netsh wlan show profile name="ProfileName" key=clear (Show saved Wi-Fi password) **(Admin Required)**

netsh interface show interface (List network interfaces)

route

Displays and modifies the local IP routing table.

route print (Show routing table)

route print -4 (Show IPv4 routes only)

route add <destination> MASK <subnet_mask> <gateway> METRIC <metric_cost> IF <interface_index> **(Admin Required)**

route delete <destination> **(Admin Required)**

3. Process s Service Management

tasklist

Lists running processes.

tasklist (Basic list)

tasklist /svc (Show services hosted in each process) **(Admin Required for some info)**

tasklist /m <dllname.dll> (Show processes using a specific DLL) tasklist /v (Verbose output, includes user context, window title) tasklist /fi "IMAGENAME eq chrome.exe" (Filter by image name)

tasklist /s <remote_hostname> (Remote query - requires permissions)

query process / query user / query session

Shows Remote Desktop Session Host information.

query process * (Show processes for all users) query user or quser (Show logged-on users)

query session or qwinsta (Show session information)

taskkill

Terminates processes. **(Admin Required often needed, especially for /F)**

taskkill /IM notepad.exe (Terminate by image name)

taskkill /PID <process_id> (Terminate by Process ID)

taskkill /IM <imagename.exe> /F (Force termination)

taskkill /PID <PID1> /PID <PID2> /F (Terminate multiple PIDs)

taskkill /T /IM <parent_process.exe> /F (Terminate process and its children)

schtasks

Schedules commands and programs (Task Scheduler).

(Admin Required for creating/modifying system tasks)

schtasks /query /fo LIST /v (Detailed list of all tasks) schtasks

/query /tn "MyTask" (Query a specific task)

schtasks /create /tn "MyTask" /tr "C:\path\script.bat" /sc ONLOGON (Example creation)

schtasks /delete /tn "TaskName" /f (Delete task) schtasks

/run /tn "TaskName" (Run task now)

schtasks /end /tn "TaskName" (Stop running task)

sc (Service Control)

Manages Windows services.

(Admin Required for most actions)

sc query (List running services)

sc query state= all (List all services)

sc qc <ServiceName> (Query Configuration: binary path, dependencies, start type - **CRITICAL** for analysis)

sc queryex <ServiceName> (Query Extended: PID, flags)

sc getdisplayname <ServiceNameKey> (Get friendly display name)

sc getkeyname "Display Name" (Get the service key name) sc

start <ServiceName>

sc stop <ServiceName>

sc config <ServiceName> start= disabled (Change start type) sc

delete <ServiceName> **(Use extreme caution)**

net start / net stop

Starts or stops services (simpler than sc for basic operations).

net start (List running services) net
start "Print Spooler"
net stop "Print Spooler" **(Admin Required)**

taskmgr

Opens Task Manager GUI.

```
taskmgr
```

4. File Systems Data Management

dir

Lists files and directories.

```
dir C:\Windows
dir /a (Show hidden and system files) dir /s
(Recursive)
dir /b (Bare format, names only) dir
/o:d (Sort by date)
dir /tc (Show creation time)
```

cd or chdir

Changes directory.

```
cd C:\Users
cd .. (Move up one level)
```

md or mkdir

Creates a new directory.

```
md C:\Temp\NewFolder
```

rd or rmdir

Removes a directory.

rd C:\Temp\OldFolder (Only if empty)

rd /s /q C:\Temp\OldFolder (Remove directory and contents, quiet mode - **use caution**)

del or erase

Deletes files. **[WARNING: Destructive]**

del C:\Temp\file.txtdel C:\Temp\file.txt

del /f /q C:\Temp\*.tmp (Force delete read-only, quiet mode)

copy

Copies files.

copy C:\file.txt D:\backup\

xcopy

Copies files and directories (more options than copy).

xcopy C:\source D:\dest /E /H /I /Y (/E=subdirs, /H=hidden/system, /I=assume dest is dir, /Y=suppress prompt)

robocopy

Robust file copy utility (preferred over xcopy).

robocopy C:\source D:\dest /E /COPYALL /R:3 /W:10 (/E=subdirs, /COPYALL=all file info, /R=retries, /W=wait time)

robocopy C:\source D:\dest /MIR (Mirrors directory - **WARNING: deletes files in dest not in source**)

move

Moves files or renames directories.

move C:\file.txt D:\ (Move file)

move C:\OldFolderName C:\NewFolderName (Rename folder)

ren or rename

Renames files or directories.

ren oldname.txt newname.txt

type

Displays contents of a text file.

type C:\Windows\System32\drivers\etc\hosts

find

Searches for a text string in files (basic).

```
find "error" C:\logs\app.log
```

findstr

Searches for strings in files (more powerful, supports regex).

```
findstr /i /s /c:"password" C:\Users\*.txt (Case-insensitive, search subdirs, literal string)
ipconfig /all | findstr /i "DNS Servers" (Pipe output to findstr)
```

sort

Sorts input (e.g., file contents) alphabetically.

```
type names.txt | sort
sort < names.txt > sorted_names.txt
```

comp / fc

Compares contents of files.

```
comp file1.bin file2.bin (Binary comparison)
fc file1.txt file2.txt (Text comparison, shows differences)
```

tree

Displays directory structure graphically.

tree C:\Windows /F (Include files)

attrib

Displays or changes file attributes.

attrib C:\Windows\System32\ntdll.dll (Show attributes)

attrib +h C:\secret.txt (Hide file) **(Admin Required often needed)**

attrib -r C:\config.ini (Remove read-only)

cipher

Displays or alters file encryption (EFS).

cipher /c <filename> (Show encryption status)

cipher /e C:\SecretFolder (Encrypt folder - new files will be encrypted) **(Admin Required)**

cipher /w:C: (Wipe free space - can take a long time) **(Admin Required)**

compact

Displays or alters file compression (NTFS compression).

compact /c /s:C:\Logs (Compress directory and contents) **(Admin Required)**

compact /u /s:C:\Logs (Uncompress) **(Admin Required)**

diskpart

Manages disks, partitions, and volumes. (Admin Required) [WARNING: Destructive]

Run diskpart, then use commands like:

list disk

select disk <n>

list partition list

volume detail

disk

clean **(DANGEROUS: wipes disk)**

create partition primary

format fs=ntfs quick assign

letter=E

format

Formats a disk. **[WARNING: Destructive - erases all data on the target volume!]**

format D: /fs:ntfs /q (Quick format drive D: as NTFS - **EXTREME CAUTION)**

chkdsk

Checks disk for errors and attempts repairs.

chkdsk C: (Read-only check)

chkdsk C: /f (Fixes errors on the disk - requires reboot if system drive) **(Admin Required)**

chkdsk C: /r (Locates bad sectors and recovers readable info - includes /f) **(Admin Required)**

takeown

Allows administrator to take ownership of a file/folder.
(Admin Required)

takeown /f <filepath_or_folderpath>

takeown /f <folderpath> /r /d y (Take ownership recursively, default 'yes' to prompts)

icacls

Displays or modifies Access Control Lists (Permissions).
(Admin Required)

icacls <filepath_or_folderpath> (Display permissions)

icacls <filepath> /grant Administrators:F (Grant Administrators Full Control)

icacls <folderpath> /inheritance:d (Disable inheritance)

icacls <folderpath> /reset /t (Reset permissions to defaults, recursive)

openfiles

Queries or displays open files/folders, often accessed via network shares.
(Admin Required)

openfiles /local on (Enable local file tracking - requires reboot) openfiles /query /v (Verbose query after enabling)

5. User, Group, s Policy Management

net user

Manages user accounts (local database or domain).

net user (List local users)

net user <username> (Show user details)

net user <username> <newpassword> (Change password) **(Admin Required)**

net user <username> /active:no (Disable account) **(Admin Required)**

net user <username> /add <password> (Add user) **(Admin Required)**

net user <username> /delete (Delete user) **(Admin Required)**

net localgroup

Manages local groups. (Admin Required)

net localgroup (List local groups)

net localgroup Administrators (List members of Administrators group)

net localgroup Administrators <username> /add (Add user to group)

net localgroup Administrators <username> /delete (Remove user from group)

net localgroup NewGroup /add (Create group)

gpupdate

pdates Group Policy settings.

gpupdate (Update applied policies)

gpupdate /force (Re-apply all policies) **(Admin Required sometimes)**

gpresult

Displays Group Policy results (Resultant Set of Policy - RSoP).

gpresult /r (Summary data for current user/computer)

gpresult /Scope Computer /v (Verbose computer policy results)
(Admin Required)

gpresult /Scope User /v (Verbose user policy results) gpresult /h

C:\temp\gp_report.html (Generate HTML report)
(Admin Required)

runas

Runs a program as a different user.

runas /user:DOMAIN\Administrator cmd.exe (Prompts for password)

runas /user:LocalAdmin /savecred "notepad.exe C:\windows\system32\drivers\etc\hosts" (Save credentials - use with caution)

assoc

Displays or modifies file extension associations.

assoc .txt (Show what opens .txt files)

ftype

Displays or modifies file types used in extension associations.

ftype txtfile (Show command used for 'txtfile' type)

control

Opens Control Panel. Can open specific applets.

control
control printers
control userpasswords2 (Opens advanced user accounts panel)

6. Event Log Management

wevtutil

(Windows Event Utility): Manages event logs. **(Admin Required for Security/System logs)**

wevtutil el (List event logs)

wevtutil qe Security /c:10 /rd:true /f:text (Query 10 newest Security events, text format)

wevtutil qe System /q:"*[System[Level=2]]" /c:5 /f:text (Query 5 newest Error level events from System log)

wevtutil epl Security C:\Backup\SecurityLog.evtx (Export Security log)

wevtutil cl Security (Clear Security log - **use caution, erases evidence!**)

eventvwr

Opens Event Viewer GUI.

eventvwr

eventvwr <logname> (e.g., eventvwr Security)

7. Security Auditing Utilities

sfc

(System File Checker): Scans and repairs protected system files.
(Admin Required)

sfc /scannow (Scan entire system, repair if possible) sfc
/verifyonly (Scan only, no repair)

auditpol

Manages audit policies. **(Admin Required)**

auditpol /get /category:* (Show current audit policy settings) auditpol
/set /subcategory:"Process Creation" /success:enable
/failure:enable (Enable detailed process auditing)

bitsadmin

Manages BITS (Background Intelligent Transfer Service) jobs.
Often abused by malware. **(Admin Required)**

bitsadmin /list /allusers (List BITS jobs for all users)
bitsadmin /info <JobID> /verbose (Get details of a job)
bitsadmin /reset (Cancel all jobs)

certutil

Manages certificates. Also abused by attackers for various purposes (Living-off-the-Land).

certutil -hashfile <filename> SHA256 (Calculate file hash - **VERY useful**)

certutil -hashfile <filename> MD5

Attacker Usage Examples (Detection & Understanding):

certutil -urlcache -split -f <URL> <outputfile> (Download file)

certutil -encode <infile> <outfile.b64> (Base64 encode) certutil -decode <infile.b64> <outfile> (Base64 decode)

fltmc

Manages audit policies. **(Admin Required)**

fltmc instances (Show active filter driver instances)

fltmc filters (List installed filters)

8. PowerShell (The Modern Standard)

PowerShell is a powerful task automation and configuration management framework, featuring a command-line shell and scripting language. It's essential for modern Windows administration and security analysis. Run powershell.exe or pwsh.exe (for PowerShell Core) to start. **(Admin Required often needed)**

Key Cmdlets (Examples)

Process: Get-Process (like tasklist), Stop-Process -Id <PID> -Force (like taskkill)

Service: Get-Service, Start-Service <Name>, Stop-Service <Name>, Get- Service <Name> | Select-Object * (Details like sc qc)

AttaNetwork: Get-NetIPConfiguration (like ipconfig /all), Test- NetConnection <hostname> -Port <port> (Connectivity test), Get- NetTCPConnection (like netstat -ano), Resolve-DnsName <hostname> (like nslookup)cker Usage Examples (Detection & Understanding):

Event Log: Get-WinEvent -LogName Security -MaxEvents 10, Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4625} -MaxEvents 50 (Query specific events)

Files/Registry: Get-ChildItem or ls or dir (like dir), Get-Content or cat or type (like type), Get-FileHash <filepath> -Algorithm SHA256, Select-String -Path <filepath> -Pattern "error", Get-ItemProperty -Path HKLM:\Software\Microsoft\Windows\CurrentVersion

System Info: Get-ComputerInfo, Get-HotFix (Patches)

WMI/CIM: Get-CimInstance -ClassName Win32_OperatingSystem (Modern way, replaces many wmic uses)

Users/Groups: Get-LocalUser, Get-LocalGroup, Get-LocalGroupMember Administrators

Security: Get-MpComputerStatus (Windows Defender status)

Remote: Invoke-Command -ComputerName <remote_host> -ScriptBlock { Get-Process } (Run commands remotely)

9. Essential Helper Commands s GUI Shortcuts

cls

Clears the command prompt screen.

```
cls
```

echo

Displays messages or toggles command echoing.

```
echo  Investigation  Started:  %DATE%  %TIME%
```

clip

Redirects command output to the Windows clipboard.

```
ipconfig /all | clip (Copies output to clipboard)
```

shutdown

Shuts down or restarts the computer. **(Admin Required)**

```
shutdown /r /t 0 (Restart immediately) shutdown /s /t 0
(Shutdown immediately) shutdown  /a  (Abort  a
scheduled  shutdown)
```

winget

Windows Package Manager command-line tool (install, manage apps).

```
winget list

winget install <AppId>
winget search <appname>
```

mmc

Opens Microsoft Management Console (load snap-ins).

services.msc

Opens Services management console GUI.

devmgmt.msc

Opens Device Manager GUI.

diskmgmt.msc

Opens Disk Management GUI.

perfmon

Opens Performance Monitor GUI.

resmon

Opens Resource Monitor GUI.

mstsc

Opens Remote Desktop Connection client.

cleanmgr

Opens Disk Cleanup utility.

defrag

Defragments a drive (less critical on SSDs). **(Admin Required)**

10. Sys-internals Suite (Highly Recommended External Tools)

These are **not built-in** but are considered essential for deep analysis. Download from Microsoft.

Autoruns/Autorunsc: View and manage startup locations (Registry, Services, Scheduled Tasks, etc.). autorunsc.exe -a * - ct -h is invaluable.

Process Explorer (procexp.exe): Advanced Task Manager replacement (shows DLLs, handles, process tree, verifies signatures).

Process Monitor (procmon.exe): Real-time monitoring of file system, Registry, process, and network activity. Powerful for behavior analysis.

PsExec (psexec.exe): Execute processes remotely. **(Admin Required)**

Sigcheck (sigcheck.exe): Check file signatures, hashes, VirusTotal integration. sigcheck.exe -i -vt <filepath>

TCPView (tcpview.exe): GUI view of network endpoints and the processes using them (like netstat but real-time GUI).