WINDOWS COMMANDS FOR SOC ANALYSTS

By Danyal Saleem

BASIC WINDOWS COMMANDS FOR SOC ANALYSTS:

1. System Information and Configuration

- **systeminfo:** Displays detailed configuration information about the system, including OS version, memory, and uptime.
- **hostname:** Displays the name of the computer (hostname).
- **ver**: Displays the Windows version.
- **wmic:** Windows Management Instrumentation Command-line tool for system information and management.
- **wmic os get caption, version, buildnumber**: Shows OS version and build number.
- **wmic cpu get caption, deviceid, numberofcores**: Displays CPU information.
- **msinfo32**: Opens the System Information utility, providing a detailed overview of the system.

2. User and Account Management (Discovery and Administration)

- **net user**: Displays user account information or modifies accounts.
- **net user <username>:** Displays user information.
- **net user <username> <password>:** Changes the password for a user account.
- **net localgroup**: Displays or modifies local user groups.
- **net localgroup <groupname>:** Displays members of a specific group.
- **net localgroup <groupname> <username> /add**: Adds a user to a group.
- **whoami:** Displays the currently logged-in user’s username.
- **netstat -b:** Shows the executable involved in creating each connection or listening port.

3. Process and Service Management

- **tasklist**: Displays a list of currently running processes.
- **taskkill**: Terminates a running process by its process ID (PID) or image name.
- **taskkill /PID <PID>:** Kill a process by PID.
- **taskkill /IM <process-name>:** Kill a process by name (e.g., taskkill /IM notepad.exe).
- **services.msc:** Opens the Services management console.
- **sc:** Service control command used to start, stop, or configure Windows services.
- **sc start <service-name>:** Starts a service.
- **sc stop <service-name**>: Stops a service.
- **sc query <service-name>:** Displays the status of a service.
- **taskmgr**: Opens the Task Manager.

4. Security and Access Control

- **netstat -b**: Shows the executable involved in creating each connection or listening port.
- **net accounts**: Displays or modifies the password and logon requirements for the system.
- **gpresult**: Displays Group Policy settings for the user or computer.
- **gpresult /r**: Displays the Group Policy results for the computer and user.

- **secpol.msc**: Opens the Local Security Policy management console.
- **wevtutil:** Utility for managing event logs.
- **wevtutil qe Security /f**:text: Queries the security event log in text format.
- **auditpol**: Configures audit policies.
- **auditpol /get /category**:*: Shows the current audit policy settings.
- **tasklist /v**: Displays verbose information about running processes, including the user account.

5. Network and Connectivity

- **ipconfig:** Displays IP configuration information for all network adapters.
- **ipconfig /all**: Shows detailed IP configuration, including MAC address and DNS servers.
- **ipconfig /flushdns**: Clears the DNS resolver cache.
- **ping:** Tests connectivity to a remote host.
- **tracert**: Tracks the path packets take to a network host.
- **nslookup:** Queries DNS to obtain domain name or IP address mapping.
- **route:** Displays or modifies the IP routing table.
- **route print**: Displays the current routing table.
- **netsh:** A powerful tool for network configuration and troubleshooting.
- **netsh interface ipv4 show config**: Displays IP address configuration for all interfaces.
- **netsh advfirewall show allprofiles**: Displays firewall configuration for all profiles.

6. Disk and File Management

- **dir**: Lists the contents of a directory.
- **dir C:\:** Lists files and directories on the C: drive.
- **chkdsk:** Checks the file system for errors and attempts to fix them.
- **chkdsk C::** Checks the C: drive for errors.
- **diskpart:** Disk partition management tool.
- **diskpart:** Launches the DiskPart command line utility.
- **list disk:** Lists all disks.
- **select disk <n>:** Selects a disk by number for further operations.
- **fsutil:** File system utility for managing disk drives and file systems.
- **fsutil dirty query C**:: Checks if the file system of drive C: is marked as dirty.
- **robocopy**: Robust file copy utility with advanced features like resume, retries, and copying metadata.
- **robocopy C:\Source D:\Destination /E**: Copies all files and subdirectories from C: to D:.
- **xcopy**: Copies files and directories, including subdirectories.
- **xcopy C:\Source D:\Destination /E:** Copies all files and subdirectories.

7. System Maintenance and Cleanup

- **cleanmgr:** Opens the Disk Cleanup utility.
- **sfc /scannow:** System File Checker to scan and repair corrupted system files.
- **dism /online /cleanup-image /restorehealth**: Repairs Windows system image.

8. System Shutdown and Restart

- **shutdown**: Shuts down or restarts the computer.
- **shutdown /s /t 0**: Shuts down the system immediately.
- **shutdown /r /t 0**: Restarts the system immediately.

- **shutdown /s /t 0:** Immediate shutdown.
- **shutdown /r /f /t 0:** Immediate restart.

9. File and Folder Operations

- **copy**: Copies files from one location to another.
- **copy** C:\file.txt D:\file.txt
- **move:** Moves files from one location to another.
- **move C**:\file.txt D:\file.txt
- **del**: Deletes files.
- **del C:**\file.txt
- **rd or rmdir**: Removes directories.
- **rd /s /q C:\FolderName**: Removes a folder and its contents without confirmation.

10. Miscellaneous Commands

- **echo:** Displays a message or enables/disables command echoing.
- echo Hello, World!
- **cls:** Clears the command prompt screen.
- **cmd:** Opens a new Command Prompt window.
- **powershell:** Opens Windows PowerShell for advanced scripting and automation.

11. PowerShell Commands (Advanced)

- **Get-EventLog**: Retrieves event log entries.
- **Get-EventLog -LogName Security -Newest 10**: Retrieves the 10 most recent security event logs.
- **Get-Process:** Lists all running processes.
- **Get-Service:** Lists all services and their statuses.
- **Set-ExecutionPolicy:** Configures the execution policy for running PowerShell scripts.
- **Set-ExecutionPolicy RemoteSigned**: Allows locally created scripts to run while requiring signed scripts from remote sources.