Windows

75+ Vital Windows Commands
Every Cybersecurity Analyst Should Master

Open the Command Prompt by pressing Win + R, typing "cmd", and pressing Enter.

No		Explanation	Sample Usage
1	`ipconfig`	Displays IP configuration information	`ipconfig /all` `ipconfig /?`
2	`systeminfo`	Displays system information	`systeminfo`
3	`netstat`	Displays network statistics	`netstat -ano`
4	`whoami`	Displays current user	`whoami`
5	`getmac`	Displays MAC address /v switch adds verbose output, providing more detailed information	`getmac /v`
6	`hostname`	Displays computer name	`hostname`
7	`ver`	Displays Windows version	`ver`
8	`winver`	Displays Windows version and build	`winver`
9	`ping`	Tests network connectivity Replace n [number] with the number of pings you want to send	`ping google.com` `ping -n 13 google.com`
10	`tracert`	Traces route to a destination	`tracert microsoft.com`
11	`nslookup`	Queries DNS servers	`nslookup google.com`
12	`tasklist`	Lists running processes	`tasklist`

13	`taskkill`	Terminates processes
		/IM stands for "Image Name"
		The /F flag forces termination of the process
			`taskkill /IM notepad.exe /F`
			`taskkill /PID process_id /F`
			`taskkill /IM chrome* /F`
			`taskkill /PID PID1 /PID PID2 /F`

14	`sfc`	Scans and repairs system files	`sfc /scannow`

15	`chkdsk`	Checks disk for errors	`chkdsk C: /f`
16	`diskpart`	Manages disks and partitions	`diskpart then list disk`
17	`format`	Formats a disk	`format C: /fs:ntfs`
18	`xcopy`	Copies files and directories	`xcopy C:\source D:\dest /E`
19	`robocopy`	Advanced file copy utility	`robocopy C:\source D:\dest /E`
20	`dir`	Lists files and directories	`dir C:\`
21	`cd`	Changes directory	`cd C:\Users`
22	`md`	Creates a new directory	`md NewFolder`
23	`rd`	Removes a directory	`rd OldFolder`
24	`del`	Deletes files	`del C:\file.txt`
25	`copy`	Copies files	`copy C:\file.txt D:\`
26	`move`	Moves files	`move C:\file.txt D:\`
27	`ren`	Renames files or directories	`ren oldname.txt newname.txt`
28	`type`	Displays contents of a text file	`type C:\file.txt`
29	`find`	Searches for a text string in files	`find "error" C:\log.txt`
30	`findstr`	Searches for strings in files	`ipconfig /all | findstr DNS`
31	`sort`	Sort the contents of a file named "names.txt" alphabetically.	`sort < names.txt`
32	`comp`	Compares contents of two files	`comp file1.txt file2.txt`
33	`fc`	Compares files and displays differences	`fc file1.txt file2.txt`
34	`tree`	Displays directory structure graphically	`tree C:\`

35	`attrib`	Changes file attributes	`attrib +r C:\file.txt`
36	`cipher`	Displays or alters file encryption	`cipher /e C:\SecretFolder`
37	`compact`	Displays or alters file compression	`compact /c C:\folder`
38	`powercfg`	Manages power settings	`powercfg /energy`
39	`shutdown`	Shuts down or restarts computer	`shutdown /r /t 0`
40	`gpupdate`	Updates Group Policy settings	`gpupdate /force`
41	`gpresult`	Displays Group Policy results	`gpresult /r`
42	`net user`	Manages user accounts	`net user JohnDoe newpassword`
43	`net localgroup`	Manages local groups	`net localgroup Administrators`
44	`net start`	Starts a network service	`net start "Print Spooler"`
45	`net stop`	Stops a network service	`net stop "Print Spooler"`
46	`netsh`	Network configuration tool	`netsh wlan show profiles`
47	`sc`	Manages Windows services	`sc query`
48	`reg`	Manages registry	`reg query HKLM\Software`
49	`runas`	Runs a program as a different user	`runas /user:Admin cmd`
50	`schtasks`	Schedules commands and programs	`schtasks /create /tn "MyTask" /tr notepad.exe /sc daily`

51	`wmic`	Windows Management Instrumentation Command-line,
		
		It is a powerful Windows utility that can be used for both legitimate system administration tasks and potentially abused by attackers.
			`wmic os get name,version,buildnumber`
			This retrieves basic OS information.
			
			Software inventory:
			`wmic product get name,version`
			This lists installed software.
			
			Remote code execution:
			`wmic /node:"victim_ip" process call create "powershell.exe -enc base64_encoded_payload"`
			This executes a malicious PowerShell script on a remote system.
			
			Malware persistence:
			`wmic startup create name="malware",command="C:\malware.exe"`
			This adds malware to the startup folder.
			
			Evasion technique:
			`wmic process where name="antivirus.exe" delete`
			Attackers may try to terminate security software.

52	`assoc`	Displays or modifies file extension associations	`assoc .txt`
53	`ftype`	Displays or modifies file types	`ftype txtfile`
54	`driverquery`	Displays installed device drivers	`driverquery`
55	`msinfo32`	Displays system information	`msinfo32`
56	`mmc`	Opens Microsoft Management Console	`mmc`
57	`eventvwr`	Opens Event Viewer	`eventvwr`
58	`services.msc`	Opens Services management console	`services.msc`

59	`devmgmt.msc`	Opens Device Manager	`devmgmt.msc`
60	`diskmgmt.msc`	Opens Disk Management	`diskmgmt.msc`
61	`taskmgr`	Opens Task Manager	`taskmgr`
62	`perfmon`	Opens Performance Monitor	`perfmon`
63	`resmon`	Opens Resource Monitor	`resmon`
64	`msconfig`	Opens System Configuration	`msconfig`
65	`control`	Opens Control Panel	`control`
66	`mstsc`	Opens Remote Desktop Connection	`mstsc`
67	`cleanmgr`	Opens Disk Cleanup	`cleanmgr`
68	`defrag C:`	Defragments a drive	`defrag C:`
69	`fsutil fsinfo drives`	File system utility	`fsutil fsinfo drives`
70	`path`	Displays or sets PATH environment variable	`path`
71	`set`	Displays, sets, or removes environment variables	`set`
72	`echo`	Displays messages or turns command echoing on/off	`echo Hello World`
73	`cls`	Clears the screen	`cls`
74	`query`	Displays information about processes that are running on a Remote Desktop Session Host (RD Session Host) server.	`query process *` To show all processes

75	`winget`	Winget is Microsoft's official package manager for Windows 10 and Windows 11. It allows users to easily discover, install, upgrade, remove and configure applications from the command line.	`List installed applications:`
			`winget list`
			`Search for an application:`
			`winget search <app name>`
			`Install an application:`
			`winget install <app id>`
			`Upgrade an application:`
			`winget upgrade <app id>`

76	`pathping`	Pathping is a command-line utility that combines functionality of the **ping and tracert** commands. It traces the route between a source and destination while providing detailed information about network latency and packet loss at each hop along the path	`pathping -q 10 -n -p 100 example.com`
			
			`This sets 10 queries per hop, disables hostname resolution, and sets 100ms between pings`