

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

No		Explanation	Sample Usage
1	<code>ipconfig</code>	Displays IP configuration information	<code>ipconfig /all</code> <code>ipconfig /?</code>
2	<code>systeminfo</code>	Displays system information	<code>systeminfo</code>
3	<code>netstat</code>	Displays network statistics	<code>netstat -ano</code>
4	<code>whoami</code>	Displays current user	<code>whoami</code>
5	<code>getmac</code>	Displays MAC address /v switch adds verbose output, providing more detailed information	<code>getmac /v</code>
6	<code>hostname</code>	Displays computer name	<code>hostname</code>
7	<code>ver</code>	Displays Windows version	<code>ver</code>
8	<code>winver</code>	Displays Windows version and build	<code>winver</code>
9	<code>ping</code>	Tests network connectivity Replace n [number] with the number of pings you want to send	<code>ping google.com</code> <code>ping -n 13 google.com</code>
10	<code>tracert</code>	Traces route to a destination	<code>tracert microsoft.com</code>
11	<code>nslookup</code>	Queries DNS servers	<code>nslookup google.com</code>
12	<code>tasklist</code>	Lists running processes	<code>tasklist</code>
13	<code>taskkill</code>	Terminates processes /IM stands for "Image Name" The /F flag forces termination of the process	<code>taskkill /IM notepad.exe /F</code> <code>taskkill /PID process_id /F</code> <code>taskkill /IM chrome* /F</code> <code>taskkill /PID PID1 /PID PID2 /F</code>
14	<code>sfc</code>	Scans and repairs system files	<code>sfc /scannow</code>

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

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

51	wmic	<p>Windows Management Instrumentation Command-line,</p> <p>It is a powerful Windows utility that can be used for both legitimate system administration tasks and potentially abused by attackers.</p>	<pre>wmic os get name,version,buidnumber</pre> <p>This retrieves basic OS information.</p> <p>Software inventory:</p> <pre>wmic product get name,version</pre> <p>This lists installed software.</p> <p>Remote code execution:</p> <pre>wmic /node:"victim_ip" process call create "powershell.exe -enc base64_encoded_payload"</pre> <p>This executes a malicious PowerShell script on a remote system.</p> <p>Malware persistence:</p> <pre>wmic startup create name="malware",command="C:\malw are.exe"</pre> <p>This adds malware to the startup folder.</p> <p>Evasion technique:</p> <pre>wmic process where name="antivirus.exe" delete</pre> <p>Attackers may try to terminate security software.</p>
52	assoc	Displays or modifies file extension associations	<pre>assoc .txt</pre>
53	ftype	Displays or modifies file types	<pre>ftype txtfile</pre>
54	driverquery	Displays installed device drivers	<pre>driverquery</pre>
55	msinfo32	Displays system information	<pre>msinfo32</pre>
56	mmc	Opens Microsoft Management Console	<pre>mmc</pre>
57	eventvwr	Opens Event Viewer	<pre>eventvwr</pre>
58	services.msc	Opens Services management console	<pre>services.msc</pre>

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

76	<code>pathping</code>	<p>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</p>	<pre>pathping -q 10 -n -p 100 example.com</pre> <p>This sets 10 queries per hop, disables hostname resolution, and sets 100ms between pings</p>
----	-----------------------	--	---

Resources:

Windows Commands Most Used by Attackers:

<https://www.cybrary.it/blog/windows-commands-used-attackers>

Top Windows Command Line Cheat Sheet (2024)

<https://www.stationx.net/windows-command-line-cheat-sheet/>