	Command	Explanation
1	ver	displays the version information of the Windows OS installed on your computer
2	path	the "path" is an environment variable that specifies a set of directories where the OS looks for executable files when you enter a command
3	assoc	displays or modifies file type associations. It allows you to associate a specific file extension with a particular file type or program.
4	Wmic process get ExecutablePath,processid,parentprocessid,commandline /format:textvaluelist	The output will include the executable path, process ID, parent process ID, and command line for each process
5	date /t	displays the current system date in a short format, without prompting for any input
6	wmic /node:localhost product list full /format:textvaluelist	it will display a list of installed products or software on your local machine, along with detailed information for each product. The output will include various properties of each product, such as installation location, version, publisher, install date, and more.
7	wmic product get name,version /format:textvaluelist	it will display a list of installed products or software on your local machine, along with their respective names and versions. The output will include the name and version information for each installed product.
8	tree C:\ /F	it will generate a visual representation of the folder and file structure within the specified directory. Each level of the hierarchy is indicated by indentation, and files are listed underneath their respective folders
9	tasklist -v	it will display a list of running processes on your system, along with various details for each process. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more
10	wmic process list full /format:textvaluelist	it will display a list of running processes on your local machine, along with their detailed information. The output will include a wide range of properties for each process, such as process ID (PID), command line, creation date, executable path, parent process ID, priority, and much more
11	whoami /all	it will display a list of information about the currently logged-in user. The output will include details such as the user name, security identifiers (SID), user and group privileges, logon session ID, logon type, and more
12	ipconfig /all	it will display a list of information about each network interface on your machine. The output will include details such as the IP address, subnet mask, default gateway, DNS servers, MAC (Media Access Control) address, and more
13	arp -a	it will display a list of entries in the ARP cache. Each entry typically includes the IP address and corresponding MAC address of a device on the local network

14	tasklist /svc	it will display a list of running processes and their corresponding services. Each process is listed along with its Process ID (PID), Session Name, Session Number, Memory Usage, and the services it is hosting
15	sc query state=all	it will display a list of services installed on the system along with their current state, process ID (PID), and other details such as the service name, display name, and service type
16	net start	it will display a list of running services on your Windows machine
17	net use	it will display a list of currently established connections to shared resources on your Windows machine
18	net share	it will display a list of currently shared resources on your Windows machine
19	net session	it will display a list of currently active sessions on your Windows machine
20	net localgroup	it will display a list of local groups on your Windows machine
21	net localgroup administrators	it will display a list of users and groups that are members of the "Administrators" local group on your Windows machine
22	net localgroup "Remote desktop users"	it will display a list of users and groups that are members of the "Remote Desktop Users" local group on your Windows machine
23	net view	it will display a list of computers or network devices that are currently visible on the network
24	net view /domain	it will display a list of domains that are currently visible on the network
25	net user	it displays a list of user accounts on the local computer
26	net user /domain	it displays a list of user accounts available in the specified domain
27	net group	it displays a list of group accounts on the local computer
28	net group /domain	it displays a list of group accounts available in the specified domain
29	Wmic useraccount get name /format:textvaluelist	it displays a list of user account names in a text-based format where each user account is presented as a key-value pair
30	wmic useraccount list /format:textvaluelist	it displays a list of user account properties in a text-based format where each property is presented as a key-value pair
31	wmic startup list full /format:textvaluelist	it displays a list of startup programs and their properties in a text-based format where each property is presented as a key-value pair
32	wmic startup list brief /format:textvaluelist	it displays a list of startup programs and their properties in a text-based format where each property is presented as a key-value pair
33	Wmic share list brief /format:textvaluelist	it displays a list of shared resources and their properties in a text-based format where each property is presented as a key-value pair
34	Schtasks /query /fo LIST /v	it displays a list of scheduled tasks and their properties in a text-based format

35	Schtasks -v	it displays a list of scheduled tasks and their properties in a detailed format
36	dir /s /b %TEMP% | findstr /e .exe	search for executable files (files with the .exe extension) within the %TEMP% directory and its subdirectories
37	bitsadmin /list /allusers /verbose	it displays a detailed list of all BITS jobs, including their job names, state, transfer progress, priority, and other relevant information
38	ipconfig /displaydns	it displays a list of the cached DNS records, including the domain names, corresponding IP addresses, and the time to live (TTL) values
39	netstat -nat	it provides a list of established TCP connections, along with their local and remote IP addresses and port numbers
40	netstat -anbo	it provides a detailed list of active network connections, including listening ports, and the corresponding processes
41	netstat -r	it provides a list of network routes, including the destination network, subnet mask, gateway, and interface
42	quser	it provides a list of active user sessions, including the username, session ID, session state, and session type
43	dnscmd /enumzones	it provides a detailed list of DNS zones, including their names, types, and storage locations
44	systeminfo	it provides an extensive list of system information, including the computer name, operating system version, processor details, memory information, network configuration, and more
45	nslookup myip.opendns.com resolver1.opendns.com	it sends a DNS query to the OpenDNS resolver specified ("resolver1.opendns.com") asking for the IP address associated with the "myip.opendns.com" domain. OpenDNS then responds with the public IP address of the client
46	curl checkip.amazonaws.com	it sends an HTTP GET request to the checkip.amazonaws.com endpoint, which responds with the public IP address of the client
47	ping -n 1 8.8.8.8	it sends a single ICMP echo request to the specified IP address (8.8.8.8). The destination server then responds with an ICMP echo reply if it is reachable
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs"	it queries the specified Registry key and retrieves information about the recently accessed documents. The output will display the names and other details of the recently accessed files
49	Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist"	it queries the specified Registry key and retrieves information about the UserAssist settings. The output will display information about the programs and files that have been accessed by the user
50	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce"	it queries the specified Registry key and retrieves information about the programs or commands set to run once. The output will display the names and other details of the programs or commands

51	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"	it displays a list of programs that run automatically when the user logs on, along with their file paths
52	Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RunMRU"	it displays a list of the most recently used programs in the Run dialog history, along with their file paths
53	Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts"	it displays a list of file extensions for which there are associated settings or programs
54	reg query "HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR\ /s"	it queries the specified Registry key and retrieves information about USB storage devices connected to the system. The output will display details about the connected devices, such as their device IDs, manufacturer, and other relevant information
55	reg query "HKLM\SYSTEM\CurrentControlSet\Enum\USB\" /s	it queries the specified Registry key and retrieves information about USB devices connected to the system. The output will display details about the connected devices, such as their device IDs, manufacturer, and other relevant information
56	copy C:\Windows\System32\winevt\Logs\Security.evtx "%userprofile%\Desktop\res\Security.evtx"	It specifies the location where the copied file will be saved. "%userprofile%" is a system variable that represents the current user's profile folder, and "\Desktop\res\Security.evtx" specifies the "res" folder on the user's desktop where the copied file will be placed
57	copy "C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx" "%userprofile%\Desktop\res\Windows PowerShell.evtx"	it will copy the Windows PowerShell event log file from the specified source path to the specified destination path. The copied file will be saved on the user's desktop in the "res" folder with the name "Windows PowerShell.evtx"
58	copy "C:\Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx" "%userprofile%\Desktop\res\Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx"	it will copy the Remote Desktop Services Admin event log file from the specified source path to the specified destination path. The copied file will be saved on the user's desktop in the "res" folder with the name "Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%4Admin.evtx"
59	copy "C:\Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-RemoteFX-Synth3dvsc%4Admin.evtx" "%userprofile%\Desktop\res\Microsoft-Windows-RemoteDesktopServices-RemoteFX-Synth3dvsc%4Admin.evtx"	it will copy the RemoteFX Synth3dvsc Admin event log file from the specified source path to the specified destination path. The copied file will be saved on the user's desktop in the "res" folder with the name "Microsoft-Windows-RemoteDesktopServices-RemoteFX-Synth3dvsc%4Admin.evtx"
60	copy "C:\Windows\System32\winevt\Logs\Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evtx" "%userprofile%\Desktop\res\Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evtx"	it will copy the Remote Desktop Services SessionServices Operational event log file from the specified source path to the specified destination path. The copied file will be saved on the user's desktop in the "res" folder with the name "Microsoft-Windows-RemoteDesktopServices-SessionServices%4Operational.evtx"