1 ver		Command	Explanation
OS installed on your computer	1	ver	displays the version information of the Windows
specifies a set of directories where the OS looks for executable files when you enter a command assoc displays or modifies file type associations. I allows you to associate a specific file extension with a particular file type or program. 4 Wmic process get Executable Path, processid, parent processid, commandline / formattextvaluelist 5 date /t wmic /node:localhost product list full / format:textvaluelist 6 wmic /node:localhost product list full / format:textvaluelist 7 wmic product get name, version / format:textvaluelist 8 tree C\/F tree C\/F tasklist \v 10 wmic process list full / format:textvaluelist 8 tree C\/F tasklist \v wmic process list full / format:textvaluelist 10 wmic process list full / format:textvaluelist wmic process list full / format:textvaluelist specifies a set of directories when you enter a command of instance in a short fallows a percent system date in a short format: without prompting for any input it will display a list of installed products of software on your local machine, along with detailed information for each product. The output will include the name and versions. The output will include the name and version information for each installed product. 10 wmic process list full / format:textvaluelist specifies a set of displays a list of invalled products of the process of properties of each process of the process of properties of each process of the process of			OS installed on your computer
looks for executable files when you enter a command	2	path	
assoc displays or modifies file type associations. I allows you to associate a specific file extension with a particular file type or program. The output will include the executable path, process ID, pand command ling for each process ID, parent process ID, and command ling for each process ID, each process ID, each process ID, each process ID, each process or your local machine, along with the each process ID, each process ID, each process ID, each process or your system, along with various details for each process ID, each process, such as process ID, each p			
displays or modifies file type associations. I allows you to associate a specific file extension with a particular file type or program. Wmic process get ExecutablePath,processid,parentprocessid,commandline / format:textvaluelist date /t wmic /node:localhost product list full / format:textvaluelist wmic /node:localhost product list full / format:textvaluelist wmic product get name,version / format:textvaluelist ti will display a list of installed products of 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, versic publisher, install date, and more. ti will display a list of installed products of software on your local machine, along with the respective names and versions. The output will include the name and version information for each installed product. tree C:\/F 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 it will display a list of running processes or your system, along with various details for ea process. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more it will display a list of running processes or 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			_
allows you to associate a specific file extension with a particular file type or program. 4 Wmic process get ExecutablePath,processid,parentprocessid,commandline formattextvaluelist The output will include the executable path, process ID, parent process ID, and command line for each process ID, priority, and much more			
## A Wmic process get ExecutablePath,processid,parentprocessid,commandline / format:textvaluelist	3	assoc	
Wmic process get ExecutablePath,processid,parentprocessid,commandline /format:textvaluelist 5 date /t 6 wmic /node:localhost product list full /format:textvaluelist 6 wmic product get name,version /format:textvaluelist 7 wmic product get name,version /format:textvaluelist 8 tree C:\/F 1 tasklist -v 9 tasklist -v wmic process list full /format:textvaluelist			
Wmic process get Executable Path, process ID, parent process ID, and command lin ne /format:textvaluelist date /t wmic /node:localhost product list full /format:textvaluelist wmic /node:localhost product list full /format:textvaluelist wmic product get name, version /format:textvaluelist wmic product get name, version /format:textvaluelist tree C:\/F tree C:\/F tree C:\/F wmic process list full /format:textvaluelist The output will include the executable path, process ID, and command lin for each products of software on your local machine, along with the respective names and versions. The output will include the name and versions. The output will include the name and version information for each installed product. **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 **It will display a list of running processes or 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 it will display a list of running processes or 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			
ExecutablePath,processid,parentprocessid,commandline / format:textvaluelist for each process ID, parent process ID, and command line for each process and process ID, and command line for each product in a short format, without prompting for any input it will display a list of installed products as 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, versic publisher, install date, and more. 7 wmic product get name, version / format:textvaluelist software on your local machine, along with the respective name and versions. The output will include the name and version information for each installed product. 8 tree C:\/F 1 twill display a list of installed products as software on your local machine, along with the respective 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 1 twill display a list of running processes or 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 1 twill display a list of running processes or 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	Δ	Wmic process get	
Tree C:\/F	7	, -	process ID, parent process ID, and command line
displays the current system date in a short format, without prompting for any input it will display a list of installed products of 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, versic publisher, install date, and more. wmic product get name, version / format: textvaluelist tree C:\/F tree C:\/F tree C:\/F tree C:\/F tasklist-v tasklist-v displays the current system date in a short format, without products of software on your local machine, along with the respective name and versions. The output will include the name and version information for each installed product. 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 ti will display a list of running processes or your system, along with various details for eaprocess. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more wmic process list full / format: textvaluelist it will display a list of running processes or 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			
format, without prompting for any input it will display a list of installed products of 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, versic publisher, install date, and more. wmic product get name, version / format: textvaluelist tree C:\/F 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 it will display a list of running processes or your system, along with various details for each over such as the process. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more wmic process list full / format: textvaluelist it will display a list of running processes or 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 ti will display a list of running processes or 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	_	•	dignlave the current evetem date in a chort
wmic/node:localhost product list full	5	cate/t	
/format:textvaluelist 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, versic publisher, install date, and more. wmic product get name, version / format:textvaluelist tree C:\/F tree C:\/F it will display a list of installed products software on your local machine, along with the respective names and versions. The output will include the name and version information for each installed product. 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 tasklist-v it will display a list of running processes on your system, along with various details for exprocess. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more 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	c	was a doubted best are dust list full	
detailed information for each product. The output will include various properties of each product, such as installation location, versic publisher, install date, and more. 7 wmic product get name, version / format: textvaluelist 8 tree C:\/F 1 tree C:	О		
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 of software on your local machine, along with the 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		Tormatitextvaluelist	
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 of software on your local machine, along with the respective names and versions. The output will include the name and version information for each installed product. 8 tree C:\/F 1 twill 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 1 tasklist-v 1 tasklist-v 1 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 1 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			output will include various properties of each
7 wmic product get name, version / format: textvalue list it will display a list of installed products of software on your local machine, along with the respective names and versions. The output will include the name and version information for each installed product. 8 tree C:\/F 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 eaprocess. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more 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			product, such as installation location, version,
software on your local machine, along with the 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 eaprocess. 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			
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 eaprocess. 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	7	wmic product get name, version /format:textvaluelist	
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 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			
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 early process. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more 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			
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 eaprocess. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more 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			
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 eaprocess. 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	0	hua 2 C/\ /5	_
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 ear 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	8	tree C:\/F	
indicated by indentation, and files are listed underneath their respective folders 1 tasklist-v 1 it will display a list of running processes on your system, along with various details for ear 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 1 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			
underneath their respective folders it will display a list of running processes on your system, along with various details for ear process. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more 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			
your system, along with various details for ear 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			
your system, along with various details for ear process. The output will include information such as the process ID (PID), session name, memory usage, status, username, and more 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	9	tasklist -v	it will display a list of running processes on
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			your system, along with various details for each
memory usage, status, username, and more 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			
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			
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	40	1	
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	10	wmic process list full /format:textvaluelist	
range of properties for each process, such as process ID (PID), command line, creation date, executable path, parent process ID, priority, and much more			
process ID (PID), command line, creation date, executable path, parent process ID, priority, and much more			
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	inconfin fall	it will display a list of information about each
12 ipconfig /all it will display a list of information about ea network interface on your machine. The output	12	ipcomig /aii	
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	13	arp -a	
cache. Each entry typically includes the IP			
address and corresponding MAC address of a			
device on the local network			device on the local network

14 tasklist/svc it will display a list of running process. Each plisted along with its Process ID (P. Name, Session Number, Memory Usage, services it is hosting 15 sc query state=all it will display a list of services the system along with their current process ID (PID), and other details service name, display name, and service name, display name, and service name, display a list of running service name, display a list of currently connections to shared resources on your Windows machine 17 net use it will display a list of currently resources on your Windows machine 18 net share it will display a list of currently sessions on your Windows machine 19 net localgroup it will display a list of local group windows machine 20 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	process is ID), Session
listed along with its Process ID (P. Name, Session Number, Memory Usage, services it is hosting it will display a list of services the system along with their current process ID (PID), and other details service name, display name, and service name, display name, and service name, display a list of running service name, display a list of running service name, display a list of running service name display a list of currently connections to shared resources on machine it will display a list of currently resources on your Windows machine it will display a list of currently sessions on your Windows machine it will display a list of currently sessions on your Windows machine it will display a list of local grow windows machine it will display a list of local grow windows machine it will display a list of users and are members of the "Administrators" on your Windows machine	ID), Session
Name, Session Number, Memory Usage, services it is hosting it will display a list of services the system along with their current process ID (PID), and other details service name, display name, and service name, display name, and service name, display name, and service name, display a list of running service name, display a list of running service name, display a list of currently connections to shared resources on machine 17 net use 18 net share 19 net session 10 put localgroup 11 it will display a list of currently resources on your Windows machine 12 it will display a list of currently sessions on your Windows machine 23 it will display a list of local grow Windows machine 24 it will display a list of local grow Windows machine 25 it will display a list of users and are members of the "Administrators" on your Windows machine	
services it is hosting it will display a list of services the system along with their current process ID (PID), and other details service name, display name, and service name, display a list of currently your Windows machine it will display a list of currently resources on your Windows machine it will display a list of currently sessions on your Windows machine it will display a list of local grow windows machine it will display a list of local grow windows machine it will display a list of users and are members of the "Administrators" on your Windows machine	and the
15 sc query state=all it will display a list of services the system along with their current process ID (PID), and other details service name, display name, and service name, display name, and service name, display a list of running service name in the process ID (PID), and other details service name, display name, and service name, display a list of running services on will display a list of currently connections to shared resources on machine 18 net share 18 net share 19 net session 10 pet localgroup 11 will display a list of currently sessions on your Windows machine 20 net localgroup 21 net localgroup administrators 22 it will display a list of local grow Windows machine 23 it will display a list of users and are members of the "Administrators" on your Windows machine	
the system along with their current process ID (PID), and other details service name, display name, and service name, display name, and service name, display a list of running service name with will display a list of currently your Windows machine 17 net use 18 net share 19 net session 19 net session 10 net localgroup 11 it will display a list of currently resources on your Windows machine 20 net localgroup 21 net localgroup administrators 22 it will display a list of local grow windows machine 23 it will display a list of users and are members of the "Administrators" on your Windows machine	
the system along with their current process ID (PID), and other details service name, display name, and service name, display name, and service name, display a list of running service name with will display a list of currently your Windows machine 17 net use 18 net share 18 net share 19 net session 19 net session 10 net localgroup 11 it will display a list of currently resources on your Windows machine 20 net localgroup 21 net localgroup administrators 22 it will display a list of local grow Windows machine 23 it will display a list of users and are members of the "Administrators" on your Windows machine	
the system along with their current process ID (PID), and other details service name, display name, and service name, display name, and service name, display a list of running service name with will display a list of currently your Windows machine 17 net use 18 net share 19 net session 19 net session 10 net localgroup 11 it will display a list of currently resources on your Windows machine 20 net localgroup 21 net localgroup administrators 22 it will display a list of local grow windows machine 23 it will display a list of users and are members of the "Administrators" on your Windows machine	installed on
process ID (PID), and other details service name, display name, and service name, display name, and service name, display name, and service name, display a list of running service name name name name name name name nam	
service name, display name, and service name, display name, and service net start it will display a list of running service name with service services of running services it will display a list of currently connections to shared resources on machine 18 net share it will display a list of currently resources on your Windows machine 19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local grow Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	
16 net start it will display a list of running so your Windows machine 17 net use it will display a list of currently connections to shared resources on your machine 18 net share it will display a list of currently resources on your Windows machine 19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local grow Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	
your Windows machine 17 net use 18 net share 19 net session 19 net localgroup 10 net localgroup 11 net localgroup administrators 12 your Windows machine 13 it will display a list of currently resources on your Windows machine 15 it will display a list of currently sessions on your Windows machine 16 it will display a list of local grow Windows machine 17 it will display a list of local grow windows machine 18 net share 19 it will display a list of currently sessions on your Windows machine 20 net localgroup administrators 21 net localgroup administrators 22 it will display a list of users and are members of the "Administrators" on your Windows machine	
17 net use it will display a list of currently connections to shared resources on ymachine 18 net share it will display a list of currently resources on your Windows machine 19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local grow Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	21 11000 011
connections to shared resources on y machine 18 net share it will display a list of currently resources on your Windows machine 19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local grown Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	established
machine 18 net share it will display a list of currently resources on your Windows machine 19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local grown Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	
18 net share it will display a list of currently resources on your Windows machine 19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local ground Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	. 041
resources on your Windows machine 19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local grown Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	shared
19 net session it will display a list of currently sessions on your Windows machine 20 net localgroup it will display a list of local grow Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	
sessions on your Windows machine 20 net localgroup it will display a list of local grown Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	active
20 net localgroup it will display a list of local ground Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	
Windows machine 21 net localgroup administrators it will display a list of users and are members of the "Administrators" on your Windows machine	ips on your
are members of the "Administrators" on your Windows machine	-
are members of the "Administrators" on your Windows machine	groups that
on your Windows machine	
	J -
22 net localgroup "Remote desktop users" it will display a list of users and	groups that
are members of the "Remote Desktop T	
group on your Windows machine	
23 net view it will display a list of computers	
devices that are currently visible of	on the
network	
24 net view /domain it will display a list of domains the	nat are
currently visible on the network	
25 net user it displays a list of user accounts	on the local
computer computer	arrailabla in
26 net user /domain it displays a list of user accounts the specified domain	avallable III
	on the
27 net group it displays a list of group accounts local computer	on the
	availahle
28 net group /domain it displays a list of group accounts in the specified domain	, available
29 Wmic useraccount get name /format:textvaluelist it displays a list of user account in	names in a
text-based format where each user ac	
presented as a key-value pair	
30 wmic useraccount list /format:textvaluelist it displays a list of user account is	properties in
a text-based format where each prope	
presented as a key-value pair	=
31 wmic startup list full /format:textvaluelist it displays a list of startup progra	ams and their
properties in a text-based format when the standard of the sta	
property is presented as a key-value	e pair
32 wmic startup list brief /format:textvaluelist it displays a list of startup progra	
properties in a text-based format when the properties in the pro	
property is presented as a key-value	
33 Wmic share list brief /format:textvaluelist it displays a list of shared resource	
properties in a text-based format when the properties in the pro	,
property is presented as a key-value	
34 Schtasks/query/foLIST/v it displays a list of scheduled task	e pair
properties in a text-based format	e pair

	Schtasks -v	it displays a list of scheduled tasks and their
35		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	with the public IP address of the client it sends a single ICMP echo request to the
47	ping -n 1 8.8.8.8	with the public IP address of the client it sends a single ICMP echo request to the specified IP address (8.8.8). The destination
47	ping -n 1 8.8.8.8	with the public IP address of the client 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
		with the public IP address of the client 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
47	reg query	with the public IP address of the client 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 it queries the specified Registry key and
		with the public IP address of the client 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 it queries the specified Registry key and retrieves information about the recently
	reg query	with the public IP address of the client 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 it queries the specified Registry key and retrieves information about the recently accessed documents. The output will display the
	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio	with the public IP address of the client 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 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
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs"	with the public IP address of the client 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 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
	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs"	with the public IP address of the client 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 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 it queries the specified Registry key and
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs"	with the public IP address of the client 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 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 it queries the specified Registry key and retrieves information about the UserAssist
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs"	with the public IP address of the client 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 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 it queries the specified Registry key and retrieves information about the UserAssist settings. The output will display information
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs" Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio	with the public IP address of the client 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 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 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
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs" Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\UserAssist"	with the public IP address of the client 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 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 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
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs" Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\UserAssist" reg query	with the public IP address of the client 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 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 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 it queries the specified Registry key and
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs" Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\UserAssist"	with the public IP address of the client 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 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 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 it queries the specified Registry key and retrieves information about the programs or
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs" Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\UserAssist" reg query	with the public IP address of the client 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 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 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 it queries the specified Registry key and retrieves information about the programs or commands set to run once. The output will
48	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\RecentDocs" Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\Explorer\UserAssist" reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio	with the public IP address of the client 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 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 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 it queries the specified Registry key and retrieves information about the programs or

51	reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio	it displays a list of programs that run automatically when the user logs on, along with
	n\Run"	their file paths
52	Reg query "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersio n\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\CurrentVersio n\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"