Command	**Purpose**	**Category**
netstat	Display current TCP/IP network connections and protocol statistics	Recon
tasklist	TaskList displays all running applications and services with their Process ID (PID) This can be run on either a local or a remote computer.	Recon
reg query	Read registry keys and values	Recon
dir	Display a list of files and subfolders	Recon
findstr	Search for a text string in a file (or multiple files). FINDSTR supports more complex regular expressions.	Recon
dsquery	Search for AD Objects	Recon
dsadd	Add AD Object	Recon/AOO
dsmod	Modify AD Object	Recon/AOO
dsget	Display AD Object	Recon
dsmove	Move AD Object	Recon/AOO
DSRM	Delete AD Object	Recon/AOO
CSVDE	Import or export AD info in CSV format	Recon/AOO
LDIFDE	Edit AD Objects, extend schema, import or export AD information	Recon/AOO
AdFind	Command line Active Directory query tool (JoeWare)	Recon
net.exe	The NET Command is used to manage network resources via the NetBIOS protocol	Lateral Movement/Recon/AOO
net view	View file and printer shares	AOO
net use	Connect to a file/print Share (Drive Map)	AOO
net user	Add, remove, and make changes to the user accounts on a computer	AOO
net account	View the current password & logon restrictions for the computer (plus machine role: Server/ Workstation)	AOO
net group	Add, edit, delete a group	AOO
net share	Create file and printer shares	AOO
net session	Manage user sessions	AOO
net file	Manage open files	AOO
net print	Manage Network Print jobs	AOO
net computer	Network configuration (Workstation/Server)	AOO
net config	Network configuration (Workstation/Server)	AOO
net time	Manage Network Time	AOO
net start	Start a service	AOO
net stop	Stop a service	AOO
net pause	Pause a service	AOO
net continue	Resume a service	AOO
cmd.exe	Launch the Windows Command Prompt	AOO
smb://	Connect to a shared resource via SMB	Lateral Movement
echo	Print arguments (strings) to stdout	Lateral Movement
ipconfig	Configuration of network interfaces	Lateral Movement
C$	Windows (NetBIOS) Admin Share for the C drive (will have a similar share for each drive letter)	Lateral Movement
IPC$	Null File Share (used for inter-process communication via named pipes)	Lateral Movement
ADMIN$	The folder in which Windows is installed is shared as admin$	Lateral Movement
runas	Allows a user to run specific tools and programs under a different username to the one that was used to logon to a computer interactively	Lateral Movement
psexec	Lets you execute processes on other systems, complete with full interactivity for console applications, without having to manually install client software. Uses include launching interactive command-prompts on remote systems and remote-enabling tools like IpConfig that otherwise do not have the ability to show information about remote systems.	Lateral Movement
powershell.exe	Launch the Windows Powershell Console	AOO

powershell IEX		
(New-Object Net.Webclient).DownloadString		
Invoke-		
Invoke-Mimikatz		
-DumpCreds		
"/c "	Switch that often preceeds a command (renamed command prompts, powershell, etc)	Program Execution/AOO
Inveigh		
Import-Module	Used in PS to import a module	AOO
Get-Module	Used in PS to list commands imported	AOO
Find-AVSignature	Powersploit	AOO
Invoke-DllInjection	Powersploit	AOO
Invoke-ReflectivePEInjection	Powersploit	AOO
Invoke-Shellcode	Powersploit	AOO
Invoke-WmiCommand	Powersploit	AOO
Get-GPPAutologon	Powersploit	AOO
Get-GPPPassword	Powersploit	AOO
Get-Keystrokes	Powersploit	AOO
Get-MicrophoneAudio	Powersploit	AOO
Get-TimedScreenshot	Powersploit	AOO
Get-VaultCredential	Powersploit	AOO
Get-VaultCredential	Powersploit	AOO
Invoke-CredentialInjection	Powersploit	AOO
Invoke-Mimikatz	Powersploit	AOO
Invoke-NinjaCopy	Powersploit	AOO
Invoke-TokenManipulation	Powersploit	AOO
Out-Minidump	Powersploit	AOO
VolumeShadowCopyTools	Powersploit	AOO
Import-Module AntivirusBypass	Powersploit	AOO
Get-Command -Module AntivirusByp	Powersploit	AOO
Import-Module CodeExecution	Powersploit	AOO
Get-Command -Module CodeExecuti	Powersploit	AOO
Import-Module Exfiltration	Powersploit	AOO
Get-Module Exfiltration	Powersploit	AOO
Import-Module Mayhem	Powersploit	AOO
Get-Command -Module Mayhem	Powersploit	AOO
Import-Module Persistence	Powersploit	AOO
Get-Command -Module Persistence	Powersploit	AOO
Get-System	Powersploit	AOO
PowerUp	Powersploit	AOO
Import-Module Privesc	Powersploit	AOO
Get-Command -Module Privesc	Powersploit	AOO
Get-ComputerDetails	Powersploit	AOO
Get-HttpStatus	Powersploit	AOO
Invoke-Portscan	Powersploit	AOO
Invoke-ReverseDnsLookup	Powersploit	AOO
PowerView	Powersploit	AOO
Import-Module Recon	Powersploit	AOO
Get-Command -Module Recon	Powersploit	AOO
Out-CompressedDll	Powersploit	AOO
Out-EncodedCommand	Powersploit	AOO
Out-EncryptedScript	Powersploit	AOO
Remove-Comments	Powersploit	AOO
Import-Module ScriptModification	Powersploit	AOO
Get-Command -Module ScriptModifi	Powersploit	AOO
CodeExecution.tests	Powersploit	AOO
Exfiltration.tests	Powersploit	AOO
PowerSploit.tests	Powersploit	AOO
Privesc.tests	Powersploit	AOO

Recon.tests	Powersploit	AOO
PowerSploit	Powersploit	AOO
sc query	Show status	Recon/AOO
sc queryEx	Show extended info - pid, flags	Recon/AOO
sc start	START a service	Recon/AOO
sc stop	STOP a service	Recon/AOO
sc pause	PAUSE a service	Recon/AOO
sc create	Create a service	Recon/AOO
sc config	Permanently change the service configuration	Recon/AOO
sc delete	Delete a service (from the registry)	Recon/AOO
sc control	Send a control to a service	Recon/AOO
psservice	View and control services	Recon/AOO
subinacl	Display or modify Access Control Entries (ACEs) for file and folder Permissions, Ownership and Domain	Recon/AOO
wmic	Windows Management Instrumentation Command	Recon/AOO
openfiles	Query or display open files, disconnect files opened by network users	Recon/AOO
systeminfo	List system configuration	Recon
regsvr	Command-line utility in Microsoft Windows operating systems for registering and unregistering DLLs and ActiveX controls in the Windows Registry	Malware Execution