🧑‍💻 **PowerShell for IT Support – Essential Commands & Use Cases**

| **Category** | **Command Example** | **What It Does / When to Use** |
| --- | --- | --- |
| 🖥️ System Info | Get-ComputerInfo | Shows full system info — OS, RAM, BIOS, etc. |
|  | Get-PSDrive -PSProvider FileSystem | Shows disk drives and space info. |
|  | (Get-CimInstance Win32\_OperatingSystem)  .LastBootUpTime | Tells how long the system has been running. |
| 🧍‍♂️ Local Users/Groups | Get-LocalUser | Lists all local user accounts. |
|  | Set-LocalUser -Name "User1" -Password (ConvertTo-SecureString "P@ssword1" -AsPlainText -Force) | Resets user password. |
|  | Add-LocalGroupMember -Group "Administrators" -Member "User1" | Adds user to Admin group. |
| 📂 File Management | Get-ChildItem C:\Logs | Lists files/folders in a directory. |
|  | Copy-Item "C:\log.txt" -Destination "D:\Backup\" | Copies files for backup. |
|  | Remove-Item C:\Temp\\* -Recurse -Force | Deletes temp files. |
| 📡 Network Tools | Get-NetIPAddress | Shows IP addresses. |
|  | Test-Connection google.com -Count 4 | Pings website — used to check internet. |
|  | Get-DnsClientServerAddress | Shows DNS server settings. |
| ⚙️ Services & Processes | Get-Process | Shows all running apps/processes. |
|  | Stop-Process -Name "notepad" | Kills frozen or unwanted apps. |
|  | Restart-Service -Name Spooler | Fixes printing by restarting print service. |
| 📜 Scripting & Logs | Get-Service > C:\Logs\Services.txt | Saves service list to file (log/reporting). |
|  | `Get-Date; Get-Process | Out-File C:\Logs\process\_log.txt` |
| 🔍 Event & System Logs | Get-EventLog -LogName System -Newest 5 | Checks for recent system errors (BSOD, restarts, etc.). |
|  | Get-WinEvent -LogName Application -MaxEvents 10 | Views application-related logs. |
| 🌐 Remote Management | Enter-PSSession -ComputerName PC001 | Connects to another PC via PowerShell (if enabled). |
| 📅 Scheduled Tasks | schtasks /create /tn "DailyCheck" /tr "powershell.exe C:\Script.ps1" /sc daily /st 09:00 | Runs a script every day at 9 AM. |

PS C:\Users\USER> pwd

Path----

C:\Users\USER

Get-History - Shows a list of past commands

| **Command** | **Platform** | **Usage Details** |
| --- | --- | --- |
| **mkdir** | **Linux** | Creates a new directory. Syntax: mkdir [directory\_name]. Example: mkdir myfolder creates a directory named myfolder. Use -p to create parent directories as needed: mkdir -p parent/child. Useful for organizing files or setting up project structures. |
| **mkdir** | **PowerShell** | Creates a new directory. Syntax: mkdir [directory\_name] or New-Item -ItemType Directory -Path [directory\_name]. Example: mkdir myfolder or New-Item -ItemType Directory -Path .\myfolder. Commonly used for scripting and automation in Windows environments. |
| **ls / dir** | **Linux / PowerShell** | Lists directory contents. Linux: ls (use ls -l for detailed view, ls -a for hidden files). PowerShell: dir or Get-ChildItem (alias ls works too). Example: ls -l or dir. Essential for navigating and inspecting file systems. |
| **cd** | **Linux / PowerShell** | Changes the current directory. Syntax: cd [path]. Example: cd /home/user/docs (Linux) or cd C:\Users\Docs (PowerShell). Use cd .. to move up one directory. Critical for navigation in CLI environments. |
| **rm / Remove-Item** | **Linux / PowerShell** | Deletes files or directories. Linux: rm [file] or rm -r [directory] (recursive). Example: rm -r oldfolder. PowerShell: Remove-Item [path] (alias rm). Example: Remove-Item -Recurse oldfolder. Use with caution to avoid data loss. |
| **cp / Copy-Item** | **Linux / PowerShell** | Copies files or directories. Linux: cp [source] [destination] (use -r for directories). Example: cp file.txt /backup/. PowerShell: Copy-Item [source] [destination] (alias cp). Example: Copy-Item file.txt C:\Backup. Useful for backups and file management. |
| **mv / Move-Item** | **Linux / PowerShell** | Moves or renames files/directories. Linux: mv [source] [destination]. Example: mv file.txt /newpath/. PowerShell: Move-Item [source] [destination] (alias mv). Example: Move-Item file.txt C:\NewPath. Key for reorganizing file systems. |
| **cat / Get-Content** | **Linux / PowerShell** | Displays file contents. Linux: cat [file]. Example: cat config.txt. PowerShell: Get-Content [file] (alias cat). Example: Get-Content config.txt. Useful for viewing logs or configuration files. |
| **grep / Select-String** | **Linux / PowerShell** | Searches text in files. Linux: grep [pattern] [file]. Example: grep "error" log.txt. PowerShell: Select-String [pattern] [file] (alias sls). Example: sls "error" log.txt. Critical for log analysis and troubleshooting. |
| **chmod** | **Linux** | Changes file permissions. Syntax: chmod [permissions] [file]. Example: chmod 755 script.sh (owner read/write/execute, others read/execute). Essential for securing files and ensuring proper access control. |
| **chown** | **Linux** | Changes file ownership. Syntax: chown [user]:[group] [file]. Example: chown admin:staff file.txt. Use -R for recursive. Key for user and group management in multi-user environments. |
| **Get-Acl / Set-Acl** | **PowerShell** | Manages file permissions. Get-Acl [path] retrieves permissions; Set-Acl [path] applies them. Example: `Get-Acl file.txt |
| **ps / Get-Process** | **Linux / PowerShell** | Lists running processes. Linux: ps aux for detailed list. PowerShell: Get-Process (alias ps). Example: `ps aux |
| **kill / Stop-Process** | **Linux / PowerShell** | Terminates processes. Linux: kill [PID] or killall [process\_name]. Example: kill 1234. PowerShell: Stop-Process -Id [PID] or -Name [process\_name]. Example: Stop-Process -Name notepad. Used for managing hung or unwanted processes. |
| **top / Get-Process + Measure-Object** | **Linux / PowerShell** | Monitors system performance. Linux: top for real-time CPU/memory usage. PowerShell: Use `Get-Process |
| **useradd / New-LocalUser** | **Linux / PowerShell** | Creates a new user. Linux: useradd -m [username] (creates home directory). Example: useradd -m john. PowerShell: New-LocalUser -Name [username] -Password [password]. Example: New-LocalUser -Name john -Password (ConvertTo-SecureString "P@ssw0rd" -AsPlainText -Force). Key for user management. |
| **passwd** | **Linux** | Changes user passwords. Syntax: passwd [username]. Example: passwd john. Used to secure user accounts. |
| **Set-LocalUser** | **PowerShell** | Modifies user properties (e.g., password). Example: Set-LocalUser -Name john -Password (ConvertTo-SecureString "NewP@ssw0rd" -AsPlainText -Force). Used for Windows user account management. |
| **ifconfig / ip / Get-NetAdapter** | **Linux / PowerShell** | Manages network interfaces. Linux: ifconfig or ip addr to view interfaces. Example: ip addr show. PowerShell: Get-NetAdapter for network details. Example: `Get-NetAdapter |
| **ping** | **Linux / PowerShell** | Tests network connectivity. Syntax: ping [host]. Example: ping google.com. Used for diagnosing network issues. |
| **netstat / Get-NetTCPConnection** | **Linux / PowerShell** | Displays network connections. Linux: netstat -tuln for listening ports. PowerShell: Get-NetTCPConnection. Example: `Get-NetTCPConnection |
| **crontab** | **Linux** | Schedules recurring tasks. Syntax: crontab -e to edit. Example: 0 2 \* \* \* /backup.sh (runs daily at 2 AM). Critical for automating backups or maintenance tasks. |
| **Scheduled Tasks (New-ScheduledTask)** | **PowerShell** | Schedules tasks in Windows. Example: New-ScheduledTask -Action (New-ScheduledTaskAction -Execute "script.ps1") -Trigger (New-ScheduledTaskTrigger -Daily -At "2AM"). Used for automation in Windows environments. |
| **find / Get-ChildItem** | **Linux / PowerShell** | Searches for files. Linux: find [path] -name [pattern]. Example: find / -name "\*.log". PowerShell: Get-ChildItem -Recurse -Include \*.log. Example: dir -r \*.log. Useful for locating files in large systems. |
| **tar** | **Linux** | Archives files. Syntax: tar -cvf archive.tar [files] (create), tar -xvf archive.tar (extract). Example: tar -zcvf backup.tar.gz /data. Used for backups and file compression. |
| **Compress-Archive / Expand-Archive** | **PowerShell** | Archives files. Example: Compress-Archive -Path files/\* -DestinationPath backup.zip or Expand-Archive -Path backup.zip -DestinationPath files. Used for Windows file archiving. |
| **systemctl / Get-Service** | **Linux / PowerShell** | Manages services. Linux: systemctl start/stop/restart [service]. Example: systemctl restart apache2. PowerShell: Get-Service, Start-Service, Stop-Service. Example: Stop-Service -Name wuauserv. Critical for service management. |

| **Command** | **Platform** | **Usage Details** |
| --- | --- | --- |
| mkdir | Linux / PowerShell | Creates a new directory. Example: mkdir logs |
| ls / Get-ChildItem | Linux / PowerShell | Lists files and directories. PowerShell: Get-ChildItem or ls (alias) |
| cd | Linux / PowerShell | Changes the current directory. Example: cd /var/log |
| pwd / Get-Location | Linux / PowerShell | Shows current working directory |
| cp / Copy-Item | Linux / PowerShell | Copies files/directories. Example: cp file1 file2 / Copy-Item file1 file2 |
| mv / Move-Item | Linux / PowerShell | Moves or renames files |
| rm / Remove-Item | Linux / PowerShell | Deletes files or directories |
| touch / New-Item | Linux / PowerShell | Creates a new empty file. PS: New-Item file.txt -ItemType File |
| cat / Get-Content | Linux / PowerShell | Displays file content |
| grep / Select-String | Linux / PowerShell | Searches text in files. Example: grep 'error' file |
| chmod | Linux | Changes file permissions |
| chown | Linux | Changes file ownership |
| top / Get-Process | Linux / PowerShell | Displays running processes |
| ps aux / Get-Process | Linux / PowerShell | Lists current processes |
| kill / Stop-Process | Linux / PowerShell | Terminates a process by PID |
| df -h / Get-PSDrive | Linux / PowerShell | Shows disk space usage |
| du -sh | Linux | Shows directory size |
| ip a / Get-NetIPAddress | Linux / PowerShell | Shows IP configuration |
| ping | Linux / PowerShell | Checks network connectivity |
| netstat -tulnp / netstat | Linux / PowerShell | Shows network connections |
| systemctl | Linux | Manages services. E.g., systemctl restart nginx |
| service | Linux | Older service control tool |
| Get-Service / Start-Service | PowerShell | Manages Windows services |
| whoami | Linux / PowerShell | Shows current user |
| sudo | Linux | Executes command as superuser |
| Invoke-Command | PowerShell | Runs command remotely |
| ssh | Linux / PowerShell | Connects to remote Linux systems |
| scp / Copy-Item -ToSession | Linux / PowerShell | Secure copy files remotely |
| cron / schtasks | Linux / PowerShell | Task scheduling. Linux: crontab -e / Windows: schtasks |
| alias / Set-Alias | Linux / PowerShell | Creates shortcut commands |
| history / Get-History | Linux / PowerShell | Shows command history |
| man / Get-Help | Linux / PowerShell | Displays manual/help for commands |