THE SECURITY REX
TECH MADE EASY. TECH MADE SECURE.

POWERSHELL

File and Directory Management

Get-ChildItem	Lists files and directories in a path.
Copy-Item	Copies files and directories.
Move-Item	Moves files and directories.
Remove-Item	Deletes files and directories.
New-Item	Creates new files or directories.
Rename-Item	Renames files and directories.
Test-Path	Checks if a path exists.
Set-Content	Writes content to a file.
Get-Content	Reads content from a file.
Get-ItemProperty	Retrieves file or directory properties.

System Administration

Get-Service	Lists system services.
Start-Service	Starts a service.
Stop-Service	Stops a service.
Restart-Service	Restarts a service.
Set-Service	Modifies service properties.
Get-Process	Lists running processes.
Stop-Process	Terminates a process.
Get-EventLog	Retrieves event log entries.
New-EventLog	Creates a new event log.
Clear-EventLog	Clears event log entries.

Persona Management

Get-LocalUser	Lists local users.
New-LocalUser	Creates a new local user.
Remove-LocalUser	Removes a local user.
Add-LocalGroupMember	Adds a user to a local group.
Get-LocalGroupMember	Lists members of a local group.
New-LocalGroup	Creates a new local group.
Remove-LocalGroup	Removes a local group.
Get-ADUser	Retrieves AD user information.
New-ADUser	Creates a new AD user.
Get-ADGroup	Lists Active Directory groups.

Active Directory

Get-ADComputer	Lists AD computers.
New-ADComputer	Creates a new AD computer.
Remove-ADComputer	Removes an AD computer.
Enable-ADAccount	Enables an AD account.
Disable-ADAccount	Disables an AD account.

Environment and Variables

Get-Variable	Lists variables.
Set-Variable	Sets variable values.
Remove-Variable	Removes variables.
$env	Accesses environment variables.
Clear-Host	Clears the console.
Clear-Variable	Clears variable values.

Data Management

Import-Csv	Imports data from a CSV file.
Export-Csv	Exports data to a CSV file.

Network and Connectivity

Test-Connection	Tests network connectivity.
Test-NetConnection	Tests connectivity to a specific port.
Get-NetAdapter	Lists network adapters.
New-NetIPAddress	Sets a new IP address.
Remove-NetIPAddress	Removes an IP address.
Add-Printer	Adds a printer.
Remove-Printer	Removes a printer.
Test-WSMan	Tests WS-Management connectivity.
Invoke-RestMethod	Sends HTTP requests.

Automation

New-ScheduledTaskTrigger	Creates a scheduled task trigger.
Register-ScheduledTask	Registers a new scheduled task.
Start-ScheduledTask	Starts a scheduled task.
Stop-ScheduledTask	Stops a scheduled task.
Get-ScheduledTask	Lists scheduled tasks.
Unregister-ScheduledTask	Removes a scheduled task.
New-ScheduledTaskAction	Creates a scheduled task action.
Enable-ScheduledTask	Enables a scheduled task.
Disable-ScheduledTask	Disables a scheduled task.

Security and Permissions

Get-Acl	Retrieves ACL of a file or directory.
Set-Acl	Sets the Access Control List.
Get-NTFSAccess	Retrieves NTFS permissions.
Grant-NTFSAccess	Grants NTFS permissions.
Revoke-NTFSAccess	Revokes NTFS permissions.
Get-ADPermission	Retrieves AD permissions.
Set-ADPermission	Sets AD permissions.
Get-EffectiveAccess	Checks effective permissions.

Registry Configurations

Get-Item	Retrieves registry keys and values.
Set-Item	Sets registry keys and values.
New-ItemProperty	Creates a new registry property.
Get-ItemProperty	Retrieves registry properties.
Get-ItemPropertyValue	Retrieves a registry property value.
Set-ExecutionPolicy	Sets the script execution policy.
Get-ExecutionPolicy	Retrieves the script execution policy.
Get-WinEvent	Retrieves Windows event log data.
Set-ItemProperty	Modifies registry properties.

Scripting and Functions

New-Module	Creates a new module.
Import-Module	Imports a module.
Remove-Module	Removes a module.
New-ScriptBlock	Creates a script block.
Invoke-Expression	Invokes a string as a command.
Get-Command	Retrieves available commands.
Get-Help	Provides help for cmdlets.
Get-Module	Lists loaded modules.
Measure-Command	Measures execution time of a script.

Miscellaneous

Read-Host	Reads input from the user.
Write-Host	Writes output to the console.
Out-File	Sends output to a file.
Out-Null	Discards output.
ConvertTo-Json	Converts objects to JSON format.
ConvertFrom-Json	Converts JSON to objects.
Test-Path	Checks if a path exists.
Invoke-Command	Run commands remotely.