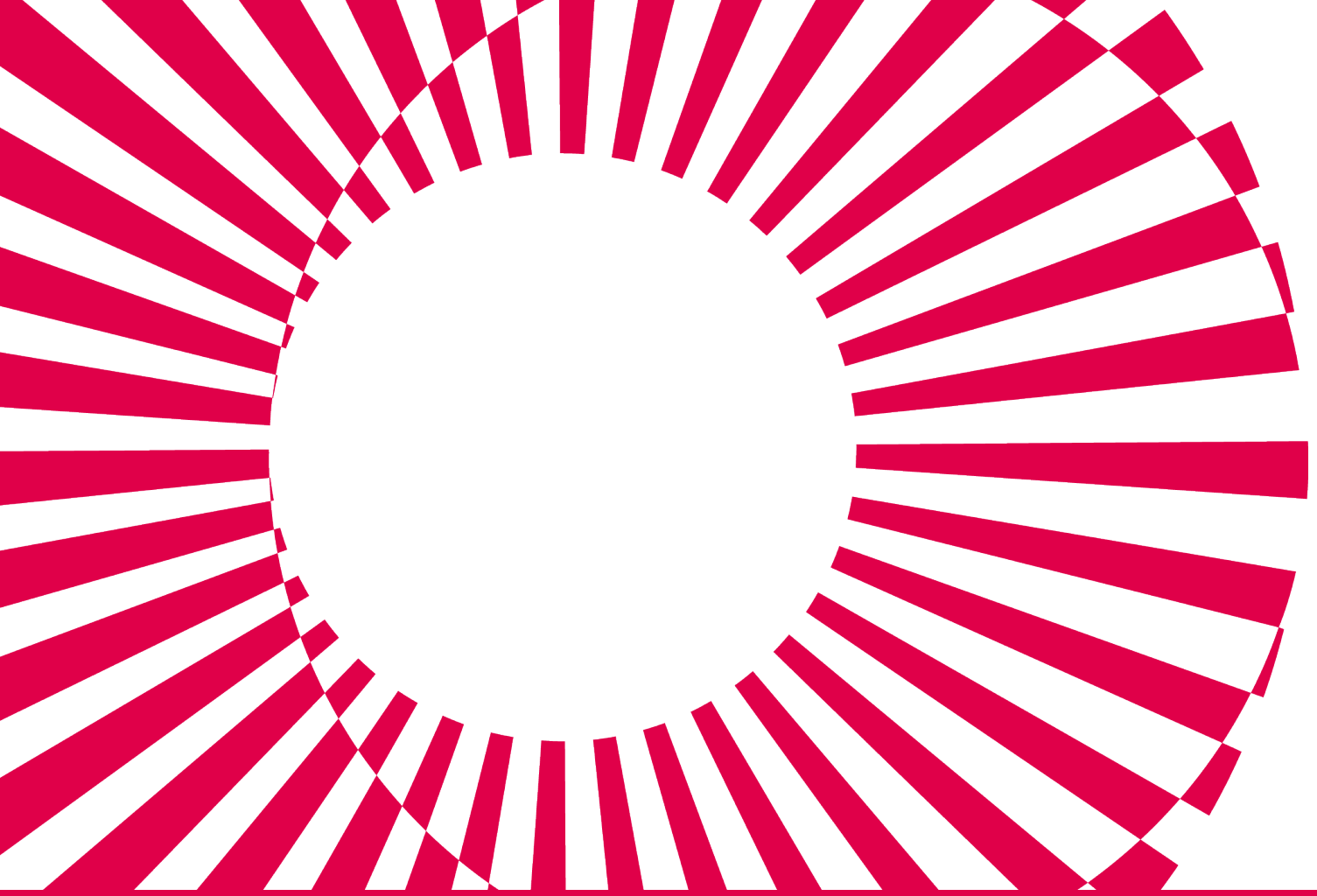

# PowerShell

UC Leuven Limburg

MOVING MINDS

UC Leuven Limburg
MOVING MINDS

# De basis

- Objecten: instantie van iets
  - Proces
  - Service
  - Get-member
- Pipeline: output (object) van een commando wordt input van het volgende commando
  - Get-process | Where {$_.CPU –gt 50}
- Data providers
  - Geven toegang tot data

UC Leuven Limburg
MOVING MINDS

# De basis

- Variabelen
  - $Tofste_vak = BS2
  - Niet hoofdlettergevoelig

- cmdlet
  - PowerShell script/commando
  - Bestaat uit een combi werkwoord-zelfstandig naamwoord
    - Get-Verb
  - Get-command => alle cmdlet, aliases, functies
  - Get-Help <cmdlet>
  - Help <cmdlet>

UC Leuven Limburg
MOVING MINDS

# Hoe gebruiken

- PowerShell

- **PowerShell ISE** => Visual Studio Code
  - Update-Help

UC Leuven Limburg
MOVING MINDS

# Modules

- Uitbreidingsset voor PowerShell
  - Get-module
  - Help get-module
  - Import-Module ActiveDirectory
  - Get-command -Module ActiveDirectory

UC Leuven Limburg
MOVING MINDS

# Krijg data "uit" PS

- Write-Host
- Write-File

UC Leuven Limburg
MOVING MINDS

# Scripting logica

- **If**
- **ForEach-Object**
  - Get-process| get-member
  - Get-process| ForEach-Object {$_.id}
- **While**

```
$myint = 1
DO {
Write-Host "Starting loop number $myint" $myint
$myint++
Write-Host "Now my integer is" $myint
} While ($myint -le 5)
```

UC Leuven Limburg
MOVING MINDS

# Nuttig

- Get-Process | Export-csv Path c:\test.csv
- $Processen = Import-csv –-Path c:\test.csv
- Get-Process | Sort-Object -Property CPU

UC Leuven Limburg
MOVING MINDS

# Getting HELP

- PowerShell kan te veel om alles te kennen/kunnen
- Update-Help
- Help
- Get-Help <cmdlet> [-detailed|-full]
- Get-help processes

UC Leuven Limburg
MOVING MINDS

# Script

- Script
  - Opeenvolging van commando's die uitgevoerd worden
  - Extentie .ps1
  - PowerShell Gallery
  - Gebruik ALTIJD commentaar, ja ALTIJD!
- Start je script in een PowerShell venster met .\script.ps1
- Uitvoer van scripts kan "disabled" zijn via de execution-policy
  - Get-executionpolicy
  - Set-executionpolicy unrestircted

# Advanced functions

```
function Get-ReconData
{
[CmdletBinding()]
Param ( [string[]] $computername )
BEGIN { Write-Output "Gathering reconnaissance on $computername" }
PROCESS {
foreach ($computer in $computername)
{
  $os = Get-WmiObject -class Win32_OperatingSystem -computerName $computer
  $comp = Get-WmiObject -class Win32_ComputerSystem -computerName $computer
  $prop = @{'Computer
            'OSVersion
            'SPVersion
            'FreeMem
            'OSType'=
            'Domain'=
            'Status'=$
  $sysinfo = New-Objec
  Write-Output $sysinfo
}
END {}
}
```

```
PS C:\Users\demo.SOMETESTORG> cd Documents
PS C:\Users\demo.SOMETESTORG\Documents> . .\getrecondata.ps1
PS C:\Users\demo.SOMETESTORG\Documents> Get-ReconData -computername Win10Client
Gathering reconnaissance on Win10Client


Domain       : sometestorg.com
OSVersion    : 10.0.15063
OSType       : 18
FreeMem      : 2146496
ComputerName : Win10Client
SPVersion    : 0
Status       : OK
```

UC Leuven Limburg
MOVING MINDS

# Desired state configuration

- Configureer machines a.d.h.v. code
- PS1-file met keyword configuration
- Alternatief
  - Ansible
  - Puppet

```
Configuration MyAwesomeWebsite {

    Import-DscResource -ModuleName PsDesiredStateConfiguration

    Node 'localhost' {
        WindowsFeature WebServer {
            Ensure = "Present"
            Name   = "Web-Server"
        }
        File WebsiteGoodies {
            Ensure = 'Present'
            SourcePath = 'c:\PStemp\index.html'
            DestinationPath = 'c:\inetpub\wwwroot'
        }
    }
}
MyAwesomeWebsite
```

UC Leuven Limburg
MOVING MINDS

# Leerstof

- Boek 6