Powershell Virtual Academy

Contents

[tools: 2](#_Toc400967911)

[deel II 2](#_Toc400967912)

[basic commands: 2](#_Toc400967913)

[deel III 3](#_Toc400967914)

[advanced (parameters): 3](#_Toc400967915)

[Deel IIII 4](#_Toc400967916)

[greater then, select property's, info about property's, extra property's, sorting: 4](#_Toc400967917)

[Deel V 5](#_Toc400967918)

[piplining inputs like serviceController in gm can be used in stop-process 5](#_Toc400967919)

[Deel VI 6](#_Toc400967920)

[remoting 6](#_Toc400967921)

[secure telnet 6](#_Toc400967922)

[Deel VII 7](#_Toc400967923)

[icm dc,s1,s2 {Get-Volume} | sort sizeremaining | select -Last 3 7](#_Toc400967924)

# tools:

ping ipconfig, calc, notepad, mspaint

# deel II

## basic commands:

cls -> clear-host

cd -> set-location

dir, ls -> get-childitem

type, cat -> get-content

copy, cp -> copy - item

get-alias ->>>

gal >

gal g\* -> all get commands

man -> help

update-help -Force

save help

get-help

\* -> wildcard

get-help get-service (-Detailed) (-full) (-online) (-showwindow)

# deel III

## advanced (parameters):

Get-Service -Name b\*, c\*

Get-Service -Name bits, bfe -> gsv bits,bfe

Get-EventLog -LogName system -Newest 3 -EntryType error

Get-Service | Export-Csv C:\Users\Nick\Desktop\service.csv

notepad C:\Users\Nick\Desktop\service.csv

bv: malware bestrijden

get-process | export-climxml -Path c:\good.xml

notepad

calc

compare-Object -ReferenceObject (import-climxl c:\good.xml) -Difference (get-process) -propery name

Get-Context c:\test.txt

get-service | converto-html -property name,status | out-file c:\test.html

get-service | converto-html -property name,status | kan ook verder mee werken

export = convert + export

get-service | stop-service -whatif

get-service | stop-service -confirm

V2 problems

cd\

get-Module -> currently loaded modules

get-adcomputer - filer \*

get-Module -> automaticly loaded module activeDirectory

# Deel IIII

## greater then, select property's, info about property's, extra property's, sorting:

Get-Process | where handles -gt 999

Get-Process | where handles -gt 999 | sort handles

Get-Service -name BITS | get-member -> gives info like property's or methods

get-service | select -propery name,status -> just select certain property's

Get-ChildItem | select -Property name, length | sort length (-Descending)

Get-EventLog -LogName System -Newest 5 | select -Property EventID, TimeWritten, Message

get a file like romeo and julia

$x = [xml](cat .\romeoandjulia.xml)

cast to xml, work with xml files

$x.play -> overview of xml

$x.play.act -> overview of acts

$x.play.act[0].scene[0].speech

$x.play.act.scene.speech | group speaker | sort count

filters ( before sort)

get-service | where {$\_.status -eq "Running" -and $\_.name -like "b\*"}

get-service | where {$PSitem.status -eq "Running"}

each service is assigned in $\_ or PSitem

# Deel V

## piplining inputs like serviceController in gm can be used in stop-process

get-service | gm vs get-help get-service -full

bv get-process calc | dir

Get-AdComputer -filter \* | select -Property name, @{name='computername'; expression={$PSitem.name}}

Get-AdComputer -filter \* | select -Property name, @{n='computername'; e={$PSitem.name}}

make existing "name" change to computername so it accepts

soooooo...

Get-AdComputer -filter \* | select -Property @{n='computername'; e={$PSitem.name}} | get-service -name bits

CAST adcomputer to a string

Get-adcomputer -filter \* | select -ExpandProperty name

Get-WmiObject -class win32\_bios -computerName (get-adcomputer -filter \* | select -ExpandProperty name)

Get-WmiObject -class win32\_bios -computerName (get-adcomputer -filter \* ).name

Get-ADcomputer -filter \* | get-wmiobject win32\_bios -computerName {$\_.Name}

# Deel VI

## remoting

## secure telnet

enter-PSSession -ComputerName dc

invoke-command -computerName cd,s1,s2 {get-eventlog -logname system -new 3}

install-windowsFeature WindowsPowerShellwebAcces

install -PsawaWebapplication -UsetestCertificate

add -PswaAuthorizationRule \* \* \*

everyone can do anything

start iexplore https://pwa/pswa -> put in credentials and dc

Get-Volume

icm dc,s1,s2 {Get-Volume} | sort sizeremaining

# Deel VII

## icm dc,s1,s2 {Get-Volume} | sort sizeremaining | select -Last 3

cd .\Iloveyou.ps1

C:Scipts\Iloveyou.ps1