7. Accediendo a los logs con PS

Sunday, November 8, 2020 6:19 PM

NOTA:	Para que este tipo de scripts funcione recuerda que debes cambiar tu ExecutionPolicy a **Unrestricted**

Primero observaremos un script de PS para extraer información de logs, sin utilizar Python.

Comentarios y ayuda del script

```
<#
.synopsis
EventProcessor EventLog Capture Automation Version 1.0

- User Specified Target EventLog
- User Specifies the number of newest Log Entries to Report
- User Specifies the Entry Type to target, for example warning, error, information etc.
- User Specifies the target computer or computers to extract the logs
- User Specifies the HTML Report Title

The script will produce an HTML output file containing details of the EventLog acquisition.

.Description
This script automates the extraction of information from the specified log file

.parameter targetLogName
Specifies the name of the log file to process
.parameter eventCount
Specifies the maximum number of newest events to consider in the search
.parameter eventType
Specifies the eventType of interest
.parameter targetComputer
Specifies the computer or computers to obtain the logs from
.parameter reportTitle
Specifies the HTML Report Title

.example
EventProcessor
Execution of EventProcessor without parameters uses the default settings of
eventLog system
eventType warning
eventCount 20
targetComputer the computer running the script

.example
EventProcessor -targetLogName security
This example specifies the target eventLog security
and uses the default parameters
eventType warning
eventCount 20
targetComputer the computer running the script

.example
EventProcessor -reporTitle "ACME Computer Daily Event Log Report"
This example provides a custom Report Title

.example
EventProcessor -targetLogName security -eventCount 20 -entryType warning -targetComputer Python-3
This example specifies all the parameters, targetLogName, eventCount, entryType and targetComputer
#>
```

Definición de parámetros

```
# Parameter Definition Section
param(
    [string]$targetLogName = "system",
    [int]$eventCount = 20,
    [string]$eventType="Error",
    [string]$reportTitle="Event Log Daily Report",
    [string[]]$targetComputer=$env:COMPUTERNAME
)
```

Obtenemos el día y hora del sistema

```powershell
# Get the current date and tme
$rptDate=Get-Date
$epoch=([DateTimeOffset]$rptDate).ToUnixTimeSeconds()
```

Creamos el reporte

```powershell
# Create HTML Header Section
$Header = @"
<style>
TABLE {border-width: 1px; border-style: solid; border-color: black; border-collapse: collapse;}
TD {border-width: 1px; padding: 3px; border-style: solid; border-color: black;}
</style>
<p>
<b> $reportTitle $rptDate </b>
<p>
Event Log Selection: <b>$targetLogName </b>
<p>
Target Computer(s) Selection: <b> $targetComputer </b>
<p>
Event Type Filter: <b> $eventType </b>
<p>
"@

# Report Filename Creation
$ReportFile = ".\Report-"+$epoch+".html"
```

Ejecutamos el CmdLet

```powershell
# CmdLet Pipeline execution
Get-Eventlog -ComputerName $targetComputer -LogName $targetLogName -Newest $eventCount -EntryType $eventType |
 ConvertTo-Html -Head $Header -Property TimeGenerated, EntryType, Message |
 Out-File $ReportFile
```

EventPro...

Comandos de ayuda

```
PS> Get-Help .\EventProcessorFinal.ps1
```

Administrator: Windows PowerShell (x86)

```
PS C:\Users\marle\Downloads\PS y Python> Get-Help .\EventProcessorFinal.ps1

NAME
    C:\Users\marle\Downloads\PS y Python\EventProcessorFinal.ps1

SYNOPSIS
    EventProcessor EventLog Capture Automation Version 1.0

    - User Specified Target EventLog
    - User Specifies the number of newest Log Entries to Report
    - User Specifies the Entry Type to target, for example warning, error, infor
    - User Specifies the target computer or computers to extract the logs
    - User Specifies the HTML Report Title

    The script will produce an HTML output file containing details of the EventL


SYNTAX
    C:\Users\marle\Downloads\PS y Python\EventProcessorFinal.ps1 [[-targetLogNam
    <Int32>] [[-eventType] <String>] [[-reportTitle] <String>] [[-targetComputer
    [<CommonParameters>]
```

```
DESCRIPTION
    This script automates the extraction of information from the specified log f


RELATED LINKS

REMARKS
```

```
PS> Get-Help .\EventProcessorFinal.ps1 -Full
```

```
OUTPUTS

    -------------------------- EXAMPLE 1 --------------------------

    PS C:\>EventProcessor

    Execution of EventProcessor without parameters uses the default settings of
    eventLog system
    eventType warning
    eventCount 20
    targetComputer the computer running the script




    -------------------------- EXAMPLE 2 --------------------------

    PS C:\>EventProcessor -targetLogName security

    This example specifies the target eventLog security
    and uses the default parameters
    eventType warning
    eventCount 20
    targetComputer the computer running the script
```