

Creating a Triage Script to Collect System Information



Liam Cleary

Microsoft MVP and Microsoft Certified Trainer at SharePlicity

@helloitsliam | www.helloitsliam.com



Overview

Goal: Collect Information and Artifacts from Host

- Create a PowerShell triage script
- Create a HTML report of results
- Save retrieved information as artifacts





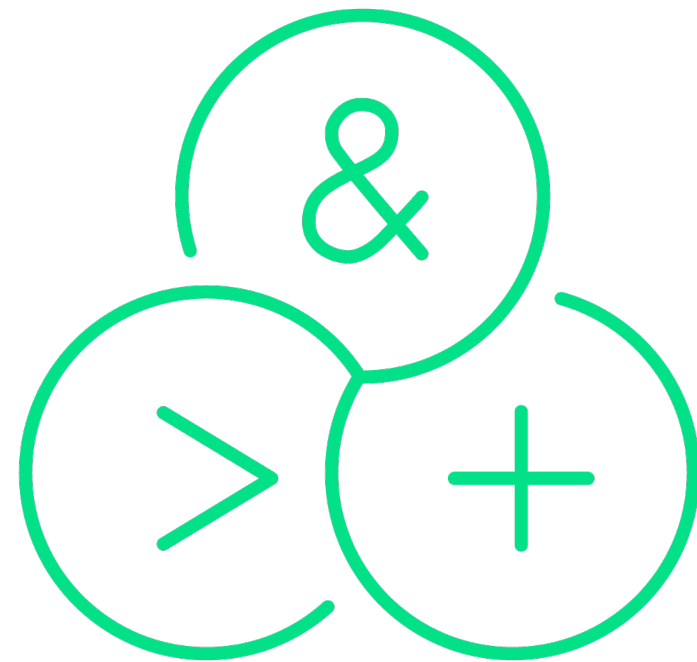
Script Tasks



Script Tasks



Define Variables



**Create
Supporting
Functions**



**Define
Commands for
Retrieving Data**



**Create Output
Functions**



Task 1: Define Variables

```
$currentLocation = Get-Location  
$logoPath = "$currentLocation\Assets\Logo.png"  
$reportName = "Report.html"  
$reportLocation = ".\Report\  
$sysinternalsPath = ".\Assets\Sysinternals"
```



Task 2: Create Supporting Functions



Create HTML document



Check if PowerShell command exists



Retrieve system information using a function instead of multiple commands



Retrieve host entries



Convert XML data into HTML



Task 3: Define Commands for Data Retrieval

Retrieve memory information

```
$MemoryInfo = Get-CimInstance -ClassName Win32_OperatingSystem | `
    Select-Object FreePhysicalMemory, TotalVisibleMemorySize | `
    ConvertTo-Html -Fragment
```

Retrieve audit policy information

```
$AuditPolicyInfo = auditpol /get /category:* | Out-String
```

Retrieve PowerShell command history

```
Get-History | Select-Object -First 10 | `
    ConvertTo-Html -Property Id, CommandLine, ExecutionStatus, ExecutionTime -Fragment
```

Retrieve timezone

```
tzutil /g
```



Task 4: Export to CSV Logs

```
function Export-CsvLogs {  
    [CmdletBinding()]  
    Param(  
        [string]$OutPath,  
        [string]$Info,  
        [string]$FileName  
    )  
  
    $item = @{ FileName = $FileName; Content = $Info }  
  
    Add-content "$OutPath/$($item.FileName)" -Value $item.Content  
}
```



Task 4: Export to HTML Document

```
$contentSets = @(
    @{ Title = "Computer Information"; Content = $ComputerInfo }
    @{ Title = "Memory Information"; Content = $MemoryInfo }
)
```

```
New-HtmlDocument `
    -FilePath "$reportLocation$reportName" `
    -ContentSets $contentSets `
    -Css $css
```



Demo

Create a Triage Script to Collect System Information

Execute the Triage Script



Summary

Goal: Collect Information and Artifacts from Host

- Created a PowerShell triage script
- Created a HTML report
- Saved retrieved information as artifacts



Up Next:

Using PowerForensics to Perform Disk Analysis

