Sign in

forgottentq / powershell Public

Notifications Fork 25 Star 38

Code Issues Pull requests Actions Projects Security Insights

powershell / captureWindows-Endpoint.ps1

37 lines (37 loc) · 2.04 KB

Code Blame Raw

```
1   # This function requires WinRM on remote machine to function properly and must be Windows 7sp1 or h
2   #
3   function captureWindows-endpoint {
4           $endpoint = $(read-host "Enter endpoint short name or FQDN")
5           $duration = $(read-host "Enter desired capture duration in seconds")
6           $date = get-date
7           $file = "$($endpoint)_$($date.Month)_$($date.Day)_$($date.year)_$($date.Hour)_$($date.Minut
8           # Remove any stale sessions remote and local
9           invoke-command -computername $endpoint -scriptblock {Remove-NeteventSession}
10          Remove-NetEventSession
11          # Start new capture
12          try {
13                  New-NetEventSession -CaptureMode SaveToFile -LocalFilePath "C:\$file" -CimSession $
14          } catch {
15                  write-host "Unable to start Event Session via CimSession on $($endpoint), not conti
16                  Break
17          }
18          Add-NetEventPacketCaptureProvider -SessionName $endpoint -Level 4 -CaptureType Physical -Ci
19          Start-NetEventSession -Name $endpoint -CimSession $endpoint
20          Sleep $duration
21          Stop-NetEventSession -Name $endpoint -CimSession $endpoint
22          try {
23                  New-Item -type Directory "C:\captures\" -ErrorAction SilentlyContinue
24                  $captures = "C:\captures\"
25          } catch {
26                  write-host "Captures directory already exists, continuing." -backgroundcolor "black
```

```
27                      $captures = "C:\captures\"
28              }
29              write-host "Copying endpoint capture file to local workstation!" -backgroundcolor "black" -
30              Copy-item "\\$endpoint\c$\$file" $captures
31              Remove-Item "\\$endpoint\c$\$file"
32              # Remove local and remote sessions.
33              invoke-command -computername $endpoint -scriptblock {Remove-NeteventSession}
34              Remove-NetEventSession
35              write-host "Opening capture directory" -backgroundcolor "black" -foregroundcolor "green"
36              ii $captures
37      }
```