Comandos de Forense con PowerShell

Calcular HASH de fichero

Get-FileHash .\info.txt -Algorithm MD5

Analizar el Hardware de un equipo remoto

$credenciales_us=Get-Credential

$IP=”192.168.1.100”

Get-WmiObject Win32_BIOS -ComputerName ($IP) -Credential $credenciales_us

Get-WmiObject Win32_Bus -ComputerName ($IP) -Credential $credenciales_us

Get-WmiObject Win32_AutochkSetting -ComputerName ($IP) -Credential $credenciales_us

Get-WmiObject Win32_BaseBoard -ComputerName $IP) -Credential $credenciales_us

Get-WmiObject Win32_Processor -ComputerName ($IP) -Credential $credenciales_us

Get-WmiObject Win32_SystemEnclosure -ComputerName ($IP) -Credential $credenciales_us

Get-WmiObject Win32_Battery -ComputerName ($IP) -Credential $credenciales_us

Get-WmiObject Win32_Printer -ComputerName ($IP) -Credential $credenciales_us

Ver Dispositivos

$Tipo=”*USB*”

Get-PnPDevice | Where-Object Class -Like $tipo

Adaptadores de red

Get-NetAdapter

Get-NetAdapterHardwareInfo

Get-NetAdapterStatistics

Obtener Usuarios y grupos

Get-LocalUser

Get-LocalGroup

Get-LocalGroupMember

Obtener información del usuario que ha iniciado sesión

[System.Security.Principal.WindowsIdentity]::GetCurrent()

Logs

Get-EventLog -LogName System -EntryType Error, Warning -After (Get-Date).AddDays(-1)

Ver aplicaciones instaladas

Get-Package | Where-Object ProviderName -eq “Programs”

Ver actualizaciones del sistema

Get-HotFix

Get-Package | Select-Object Name | Where-Object Name -match "Actualización"

Procesos del Sistema y su ruta

Get-Process

Get-Process | Select-Object Name,Path

Get-WmiObject -Class win32_process | Select-Object Name,ExecutablePath

Conexiones y datos de red

Get-NetUDPEndpoint

Get-NetTCPConnection

Get-NetFirewallRule

Get-NetRoute

Get-DnsClientServerAddress

Get-DnsClientCache

Servicios

Get-Service

Definiciones de virus

Get-MpThreatCatalog

Artefactos

#Shellbags

Get-ChildItem HKCU:\Software\Microsoft\Windows\Shell

Get-ChildItem HKCU:\Software\Microsoft\Windows\

#Registros HIVE

Get-ChildItem HKLM:\SAM

Get-ChildItem HKLM:\SECURITY

Get-ChildItem HKLM:\SOFTWARE

Get-ChildItem HKLM:\HARDWARE

#Información sobre programas ejecutados (Prefetch)

Get-ChildItem C:\Windows\Prefetch

#Información sobre navegadores

Get-ChildItem C:\Users\user\AppData\Local\Microsoft\Windows\History

Get-ChildItem C:\Users\user\AppData\Local\Mozilla\Firefox\Profiles

#Ficheros temporales

Get-ChildItem C:\Windows\Temp

#Ficheros temporales de los usuarios

Get-ChildItem C:\Users\user\AppData\Local\Temp

#Información sobre el hardware

Get-ChildItem C:\Windows\Inf

#Información sobre USB

Get-ChildItem HKLM:\SYSTEM\ControlSet001\Enum\USB

Get-ChildItem HKLM:\SYSTEM\ControlSet001\Enum\USBSTOR

Get-ChildItem HKLM:\SYSTEM\CurrentControlSet\Enum\USB

Get-ChildItem HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR

```
Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\Windows Portable Devices\Devices'

Get-ChildItem 'HKLM:\SYSTEM\ControlSet001\Control\DeviceClasses'


#Información acerca de las acciones de instalación durante la instalación

Get-Content C:\Windows\setupact.log

#Información sobre los errores de instalación durante la instalación

Get-Content C:\Windows\setuperr.log
```

Servicios y conexiones de red UDP

```
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ 'Running') | %{

Write-Host $_.Name,$_.ProcessId,$_.State,(Get-WmiObject -Class win32_process | Where-Object ProcessId -EQ  $_.ProcessId | select name, Path, ExecutablePath, CommandLine)

Write-Host $_.Name,$_.ProcessId,$_.State,(Get-Process -Id $_.ProcessId).Name,(Get-NetUDPEndpoint | where OwningProcess -EQ $_.ProcessId | select LocalPort,RemoteAddress,RemotePort,OwningProcess)

Write-Host "#####################################################"

}
```

Servicios y Conexiones de red TCP

```
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ 'Running') | %{

Write-Host $_.Name,$_.ProcessId,$_.State,(Get-WmiObject -Class win32_process | Where-Object ProcessId -EQ  $_.ProcessId | select name, Path, ExecutablePath, CommandLine)

Write-Host $_.Name,$_.ProcessId,$_.State,(Get-Process -Id $_.ProcessId).Name,(Get-NetTCPConnection | where OwningProcess -EQ $_.ProcessId | select LocalPort,RemoteAddress,RemotePort,OwningProcess)

Write-Host "#####################################################"

}
```

Programas instalados relacionados con los procesos y servicios

```
(Get-WmiObject -Class Win32_Service | Where-Object State -EQ 'Running') | %{

Write-Host $_.Name,$_.ProcessId,$_.State,(Get-WmiObject -Class win32_process | Where-Object ProcessId -EQ  $_.ProcessId | select name, Path, ExecutablePath, CommandLine)

}
```