Powershell Cheat Sheet

Setting Environment Variable Examples

Can also use Get-Credential

- $Password = Read-Host -Prompt "Set admin password" -AsSecureString
- $UserAccount = Get-LocalUser -Name "administrator"

Calling Environment Variables Examples

$UserAccount | Set-LocalUser -Password $Password

Useful things to pipe with

- | findstr “what you want to find”
- | Format-Table
- | Format-List

User Accounts

Identify curious-looking/High Privilege accounts in the administrators group

- Related command: Get-LocalUser
- Related command: Get-LocalUser -Name user | Set-LocalUser -Password
- Related command: Get-LocalUser -Name "administrator" | Enable-LocalUser
- Related command: Get-LocalUser -Name "administrator" | Set-LocalUser -Name "administrator" -Password $Password
- New-LocalUser -Name "user" -Description "" -Password <password>

Local groups

- Related command: Get-LocalGroupMember Administrators
- Related command: Get-LocalGroupMember
- Related command: Get-LocalUser -Name user | Add-LocalGroupMember -Group "Administrators"
- Related command: Get-ACL

Domain related user commands

- Related command: Get-ADUser
- Related command: Get-ADGroupMember

Domain related group commands

- Related command: New-ADGroup -Name <Group Name> -GroupScope <domain>
- Related command: Add-ADGroupMember -Identity <New group> -Members user1,user2,user3
- Related command: Remove-ADGroupMember -Identity <Group name>

Domain GPO

Related command: Gpupdate /force

Related command: gpresult (will display options)

Processes **(focus on those running with high privileges)**

Identify abnormal processes/vulnerable

- Related command: Get-Process

Services

Identify abnormal/vulnerable services

- Related command: Get-Service | Format-Table
- Related command: Stop-Service <service name>
- Related command: Start-Service <service name>

Scheduled tasks

Identify curious-looking scheduled tasks [search for task scheduler in start menu search]

- Related command: Get-ScheduledTask

Extra startup items

Identify users' autostart folders

- Related command: Get-CimInstance -ClassName Win32_StartUpCommand
-

Auto-start reg key entries

Check below registry keys for malicious autorun configurations

Get-ChildItem

- HKLM:\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM:\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM:\Software\Microsoft\Windows\CurrentVersion\RunonceEx

Listening and active TCP and UDP ports

Identify abnormal listening and active TCP and UDP ports

- Related command: Get-NetTCPConnection
- Related command: Get-NetUDPEndpoint

File Shares

All available file shares of a machine should be justified

- Related command: Get-SMBShare
- Related command: Get-FileShare
- Related command: Get-SMBServerConfiguration

Firewall Settings

Examining current firewall settings to detect abnormalities from a baseline

- Get-FirewallProfile
- Related command:Get-NetFirewallRule -Action Allow -Direction Inbound -Enabled True |Format-Table

Systems connected to the machine

Identify NetBIOS over TCP/IP activity

- Related command: nbtstat -S

Open sessions/Logged on Users

Knowing who has an open session with a machine is very important

- Related command: gwmi Win32_LoggedOnUser | Select Antecedent
- Related command: Get-SMBOpenFile

Log entries

Identify curious-looking events

- Related command: Get-EventLog -LogName -Security -Source bacon (must be done with admin privileges, piping findstr is highly advised)

Networking Commands

Related command: route print
Related command: Get-NetNeighbor -AddressFamily IPv4
Related command: Get-NetIPConfiguration

Other useful commands

Web requests

Invoke-WebRequest -Uri <IP_Address or web domain> -Outfile <filename>