Powershell

Documentation

- PowerStallion PowerShell backdoor.
- GitHub
    - https://github.com/jrussellfreelance/powershell-scripts
    - https://github.com/Azure/azure-docs-powershell-samples/tree/master/virtual-machine
    - https://github.com/mattifestation/PowerShellArsenal
    - https://github.com/clymb3r/PowerSploit
    - https://github.com/clymb3r/PowerShell
    - https://github.com/lazywinadmin/PowerShell
    - https://github.com/PowerShell/PowerShell
    - https://github.com/MicrosoftDocs/PowerShell-Docs
    - https://github.com/MicksITBlogs/PowerShell
- https://docs.microsoft.com/en-us/powershell/
- Tutorial: PowerShell Documentation - PowerShellhttp://www.dispatchertimer.com/tutorial/windows-powershell-tutorial/
- https://docs.microsoft.com/en-us/learn/
- https://mva.microsoft.com/
- Cheat sheet 1: https://ramblingcookiemonster.files.wordpress.com/2012/09/powershell-basic-cheat-sheet2.pdf
- Cheat sheet 2: https://ramblingcookiemonster.files.wordpress.com/2012/09/powershell-cheat-sheet.pdf
- https://docs.microsoft.com/en-us/powershell/scripting/gallery/how-to/finding-packages/search-syntax?view=powershell-7

Powershell Commands

Finding Help

- **Show example:** help [string of command] -examples
- **To show online help:** help dir -online
- **To show full help:** help dir -full

- **To update help files:** update-help
- **Show GUI for command:** show-Command -Name [command string]
- **Show powershell version:** $PSVersionTable

Computer administration

- **Set display resolution:** set-displayresolution
- **Set time:** set-timezone “pacific standard time”
- **Set date:** Set-date
- **Display date:** Get-date
- **Display Resolution:** Get-displayresolution
- **Display hostname:** hostname
- **Change hostname:** Rename-computer -newname [NAME] -restart
- **Show running services:** Get-Service | Where-Object {$_.Status -eq "Running"}
- **Open explorer:** ii .
- **Open explorer:** Start-Explorer
- **View event log:** Get-EventLog
- **Show processes:** get-process | sort cpu -descending | Select-Object -first 10
- **Display content of csv, txt files:** Get-Content -path [string of path]
- **To select and display objects:** Select-Object
- **To sort:** sort-object
- **Display windows features:** Get-WindowsFeature
- **Display Configuration info:** Get-dscconfigurationstatus
- **Display disk drives:** Get-Disk
- **Display volumes:** Get-Volume
- **Display properties:** Get-ItemProperty
- **Display Permissions:** Get-ACL
- **CMD**
    - Netstat -b
    - Netstat -e
- **To create a directory:** New-Item “PATH" –type directory
- **To share a directory on a network:** New-SMBShare –Name “Shared” –Path “C:\Shared” `
- **To copy an item:** Copy-Item [-Path] <String[]> [[-Destination] <String>]
- **Edit shared folder permissions:** Grant-SmbShareAccess
- **To show performance counter info:** Get-Counter -ListSet memory | select -expand counter
- **Show VM memory info:** Get-VMMemory -ComputerName NAME -vmname NAME
- **Set VM memory:** Set-VMMemory -Computer -vmname -startupbytes #MB
- **Confirm secure boot:** Confirm-SecureBootUEFI
- **Show host memory info:** Get-WmiObject -class "Win32_PhysicalMemoryArray"
- **To shutdown:** shutdown /s /t 0
- **Get number of processes:** (get-process).count

- **Get service:** Get-Service <name>
- **Start-Service**

Networking

- **Display IP & interface info:** Get-NetIPAddress
- **More IP info:** Get-NetIPConfiguration
- **Set IP address:** New-netipaddress -InterfaceAlias [ALIASNAME] -IPaddress [IPADDRESS] -Prefixlink [SUBNETLENGTH] -defaultgateway [GATEWAY]
- **Display DNS info:** Get-DnsClientServerAddress
- **Set DNS servers:** Set-DNSclientserveraddress -InterfaceAlias [INTERFACE]-serveraddress ("IP", "IP2")
- **Display firewall rules:** Get-netfirewallrule | ft
- **Display firewall rules:** Get-netfirewallrule | ft displayname,displaygroup
- **Display firewall rules**: Get-NetFirewallRule -displaygroup "GROUP NAME"
- **Completed open firewall inbound:** New-netfirewallrule -displayname "allow all traffic" -direction inbound -action allow
- **Completed open firewall outbound:** New-netfirewallrule -displayname "allow all traffic" -direction inbound -action allow
- **Add computer to domain:** Add-Computer -DomainName "DOMAIN-NAME" -Restart
    - Set DNS to domain DNS prior to attempting to add to domain
- **Domain Controller Manager:** dsac.exe

Remote Administration

- **To configure remote server:** sconfig
- **Enable remoting to server, run from server:** Enable-PSRemoting
- **Enter remote session:** Enter-PSSession -computername -credential
- **Create Virtual Machine:** New-VM -computername NAME -name NAME -generation 2 -memorystartupbytes -newVHDpath -newvhdsizebytes -switchname
- **Remote with only IP:** Enter-PSSession -ComputerName -Credential \Administrator
    - Enter-Pssession -ComputerName 192.168.1.1 -Credential 192.168.1.1\administrator
- **To start VM:** Start-VM
- To restart VM:
- **Display VMs:** Get-VM
- **Powershell Direct:** Enter-PSSession -vmname [VMNAME]
- **Show SMB sessions:** Get-SMBSession
- **Show logged in user:** query user
- **Log users off:** Invoke-RDPUserLogoff -UnfiedSessionID [#]
- **To enable nesting (virtualization on a virtual machine in hyperv):** Set-VMProcessor -vmname [name] -ExposeVirtualizationExtensions $true

- **To enable MAC spoofing on VM:** Get-VMNetworkAdapter -VMName [NAME] | Set-VMNetworkAdapter -MacAddressSpoofing on
- **To get VM integration services:** Get-VMIntegrationService
- **To enable VM integration service:** Enable-VMIntegrationService
- **To view VM resource metering:** Enable-VMResourceMetering -computername -vmname
    - Measure-VM -computername -vmname | fl
    - Measure-VM -computername -vmname | select -expand networkmeteredtrafficreport
- **Host resource protection:** Set-VMProcessor -computername -vmname -enablehostresourceprotection $true
- **Export-VM** // **Import-VM**
- **New-VHD**
- **Add-VMHardDiskDrive**
- **Test-VHD**
- **Optimize-VHD**
- **Resize-VHD**
- **Checkpoint-VM**
- **New-VMSwitch**
- **Get-NetAdapter**
- **New-NetIPAddress**
- **New-NetNat**
- **Add-NetNATStaticMapping**
- **Add-VMNetworkAdapter**
- **Set-VMNetworkAdapterIsolation**
- **Set-VMNetworkAdapter -DynamicMacAddress or -StaticMacAddress**
- **Get-NetAdapterVmq**
- **To add IP to trusted hosts:** Set-Item WSMan:\localhost\Client\TrustedHosts <IP address> -Force
- **Add user to local admin group:** Add-LocalGroupMember -Group -Member

Containers

- **To inspect module:** -Name DockerMsftProvider -Path <path>
    - **To download:** Install-Module -Name DockerMsftProvider -Repository PSGallery -Force
    - **To install:** Install-Package -Name docker -ProviderName DockerMsftProvider
- **Versioning:** Docker version

- Powershell

    - set-displayresolution
    - set-timezone “pacific standard time”
    - Set-date
    - Get-date
    - Get-displayresolution
    - Get-netipaddress
    - IP addressing
        - New-netipaddress -InterfaceAlias ALIASNAME -IPaddress IPADDRESS -Prefixlink SUBNETLENGTH -defaultgateway
        - Get-netipconfiguration
        - Set-DNSclientserveraddress -InterfaceAlias ethernet0 -serveraddress (“IP”, “IP2”)
        - Hostname
            - Rename-computer -newname NAME -restart
        - LIcense = slmgr.vbs
    - enable-psremoting
    - Firewall
        - Get-netfirewallrule | ft
        - Set-netfirewallfule
        - Get-netfirewallrule | ft displayname,displaygroup
        - getfirewallrule -displaygroup “DISPLAY GROUP NAME”
        - New-netfirewallrule -displayname “allow all traffic” -direction outbound -action allow
- Windows powershell dsc
    - Documentation in powershell
    - Get-dscconfigurationstatus
    - Get-windowsfeature
- To add a computer to a domain using powershell
    - Add-Computer -DomainName “DOMAIN” -Restart
- Managing server core
    - Remote systems administration toolkit
    - Enter-PSsession NAME
- Powershell
    - Enable-PSRemoting
    - Format-volume
    - Get-PSDrive
    - Get-PSDrive -PSProvider ‘FileSystem’
    - Open powershell session as another user: start powershell -credential ""
    - Enter-PSSession -ComputerName anaheim-server -Credential BCWIREROPE\ryan
    - Show running services: Get-Service | Where-Object {$_.Status -eq "Running"}
    - Get-content -path
- Get-smbshare

- Get-smbsession
- New-smbshare
- General computer setup
    - set-displayresolution
    - set-timezone “pacific standard time”
    - Set-date
    - Get-date
    - Get-displayresolution
    - Get-netipaddress (view IP information on a nano server)
    - enable-psremoting
- Installation
    - Install-WindowsFeature Failover-clustering -comp IP.ADDRESS
    - Install-WindowsFeature -Name AD-Domain-Services
    - Get-WindowsFeature comp NAME
    - Disable-WindowsOptionalFeature disables optional features from an image
    - Linux VM to support Secure Boot: Set-VMFirmware to ensure that UEFI CA can be used
    - Set-VMProcessor: enables nested virtualization
- Networking
    - IP addressing
        - New-netipaddress -InterfaceAlias ALIASNAME -IPaddress IPADDRESS -Prefixlink SUBNETLENGTH -defaultgateway
        - Get-netipconfiguration
        - Set-DNSclientserveraddress -InterfaceAlias ethernet0 -serveraddress (“IP”, “IP2”)
        - Hostname
            - Rename-computer -newname NAME -restart
        - LIcense = slmgr.vbs
        - New-netipaddress
        - Set-dnsclientserveraddress
        - Add-computer
            - Add computer to domain: Add-Computer -DomainName “DOMAIN” -Restart
    - Firewall
        - Get-netfirewallrule | ft
        - Set-netfirewallfule
        - Get-netfirewallrule | ft displayname,displaygroup
        - getfirewallrule -displaygroup “DISPLAY GROUP NAME”
        - New-netfirewallrule -displayname “allow all traffic” -direction outbound -action allow
- Migration
    - Set-VMHost

        - HyperV host configuration, including authentication and performance options
        - Kerberos must be enabled for migration without needing to sign in
    - Enable-VMMigration: live migration support config on the host
    - Move-VM: begins the migration after Set-VMHost has been specified

- Update-Help
- Get-Help
- Get-eventlog = use this for identifying logs with certain event ID on the server
- Get-Process = shows running processes
- Get-Command = shows available commands
- Set-Location = change the shell's current location
- Get-ChildItem
- New-Item
- Get-Command = gcm
- -noun *event* ; -verb
- gcm *start*
- Invoke-item = opens that particular file
- Del = delete
- Help *remot*
- help about_remote_troubleshooting
- Enter-pssession \ exit-pssession
- C:\PS>add-pssnapin windows.serverbackup
- Get-WBSummary
- get-help exa
- Get-service
- get-executionpolicy
- convertto-html
- export-csv
- select-object
- get-eventlog
- stop-process
- psdrive
- set-executionpolicy unrestricted
- get-service | sort-object status | format-table | export-csv "path.csv"
- Using export-csv cmdlet
    - https://technet.microsoft.com/en-us/library/ee176825.aspx
- Office 365 commands
    - Connect-msolservice
    - get-msolUser
    - Msonline
- cmd.exe commands that also work in powershell
    - dir

    - cd
    - ping localhost
    - Ipconfig
    - Nslookup
- Useful Scripts
    - Get-EventLog -LogName Security -computername ANAHEIM-SERVER -InstanceId 4625 -Newest 50 | Export-Csv C:\seclog3172015.csv
    - Get failed login attempts from server
    - Change seclog3172015.csv to the applicable date
- Invoke-Command
    - https://docs.microsoft.com/en-us/powershell/module/Microsoft.PowerShell.Core/Invoke-Command?view=powershell-7
- https://www.hongkiat.com/blog/windows-powershell-commands/
- https://github.com/lazywinadmin/PowerShell
- Simple Menu
    - https://github.com/jrussellfreelance/powershell-scripts/blob/master/network-tools-install-modules.ps1
    -

Categories

- AD
- Azure
- Exploit
- O365
- Tool

Desired Scripts

- Warn on backup failure with extremely specific info
    - Fix backup error if possible

Evolve VM Domain

Network: 172.21.176.0/20
Default gateway: 172.21.176.1
Broadcast: 172.21.191.255
Netmask: 255.255.240.0
Hosts: 172.21.176.1 - 172.21.191.254
evolve.io
DSRM: $Rheav28042*

Server

IPv4 Address. . . . . : 192.168.155.2
Subnet Mask . . . . . : 255.255.240.0
Default Gateway . . . . . : 192.168.144.1

- Evolve-DC
  - Local User: Administrator
  - Password: $Rheav28042*
  - 172.21.176.2/20
- Evolve-Win10-01
  - Local User: ryan
  - Password: $Rheav28042*
  - 172.21.176.12/20
- Evolve-Win7-01
  - Local User: ryan
  - Password: $Rheav28042*
- User Data
  - User
    - Bob
    - Red2020
  - User
    - George
    - Blue2020
- Groups
  - Production
  -

To Do

- Create git txt(?) of useful simple commands with explanations
- Find useful scripts
- Only push scripts if they work in lab or other environment
- Clean this doc
- Back everything up
- Write better scripts for BC specifically