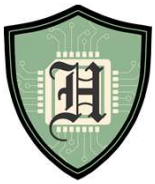
POWERSHELL JEA

(Just Enough Administration)

Presented by

James Honeycutt

About Me



- 23 Years Military Service
- 19 Years Windows Environment
- SANs Mentor (GMON/SEC511, GCWN/SEC505)
- Self taught PowerShell
- Passion for PowerShell

Twitter: @P0w3rChi3f
LinkedIn: james-Honeycutt
http://jameshoneycutt.net


SAY POWERSHELL ONE MORE TIME
imgflip.com


I USE BATCH
AND VB SCRIPTING
YOU ARE NOT
MY SON IF YOU
DONT USE POWERSHELL
imgflip.com

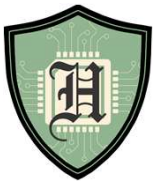
Scenario

- You work in small shop with 3 systems administrators. You IT shop has a development team of 5 people and there is a contractor who is the system owner of one server. Your development team has full admin rights to the database and web servers The SysAdmins still update and patch the database and web servers, the developers just need admin rights for development.
- The contractor remotes into his server to operate and manage the thermostats for the organization. He is just a user on the server and cannot perform any admin functions, to include restarting the machine. He likes to leave his office and drive 10-15 miles to the sysadmin to perform maintances and reboot the machine.

What is PowerShell JEA

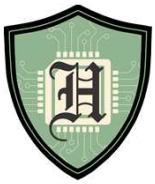
- "Just Enough Administration (JEA) is a security technology that enables delegated administration for anything that can be managed with PowerShell." –Microsoft
- "Just like keys on a key chain" – Jeffery Snover
- "Really cool way to empower my users and fellow admins" – James Honeycutt
- Allows common users to perform admin functions (when properly configured)

Requirements



Client	Server
Win 10 1511 or higher	2019
Win 8, 8.1	2016
Win 7	2012, 2012r2
	2008r2

- WMF 5 (Windows Management Framework)
- PowerShell Remoting

How does it work?

How It Works

- User/Admin uses PowerShell remoting to access remote server using the Session configuration file and using "Runas"
- A virtual Admin account is created and used during THIS SESSION ONLY
- The virtual admin technically has access to all cmdlets, but only shows the user what they are entitled to, based on the Role Capabilities File
- User does what they need to, exits remote pssession

If the roles supported by this JEA endpoint are all used to manage the local machine, and a local administrator account is sufficient to run the commands succesfully, you should configure JEA to use a local virtual account. Virtual accounts are temporary accounts that are unique to a specific user and only last for the duration of their PowerShell session. On a member server or workstation, virtual accounts belong to the local computer's Administrators group, and have access to most system resources. On an Active Directory Domain Controller, virtual accounts belong to the domain's Domain Admins group.

Role Capabilities File

- Controls what Cmdlets, Modules, Functions, and Parameters are allowed
- New-PSRoleCapabilityFile -Path .\MyFirstJEARole.psrc
- VisibleCmdlets =
  - @{ Name = 'Restart-Service'; Parameters = @{ Name = 'Name'; ValidateSet = 'Dns', 'Spooler' }},
  - @{ Name = 'Start-Website'; Parameters = @{ Name = 'Name'; ValidatePattern = 'HR_*' }}
- VisibleExternalCommands = 'C:\Windows\System32\whoami.exe', 'C:\Program Files\Contoso\Scripts\UpdateITSoftware.ps1'

https://docs.microsoft.com/en-us/powershell/jea/role-capabilities

For example, consider the role of a file server admin who wants to check which network shares are hosted by the local machine. One way to check is to use net share. However, allowing net.exe is very dangerous becuase the admin could just as easily use the command to gain admin privileges with net group Administrators unprivilegedjeauser /add. A better approach is to allow Get-SmbShare which achieves the same result but has a much more limited scope.

Session Configurations

- Controls who can log in and determines what role capability file to use.
- Virtual accounts are created on the fly and are used for the one session only. Will have local rights on endpoint and member servers or domain admin rights on DC
- Specified Virtual accounts can be specified, but must be in the appropriate local group. Group Managed Service Accounts can be used if the user needs network resources. (Harder to trace back to a specific user)

https://docs.microsoft.com/en-us/powershell/jea/session-configurations

You can open the session configuration file in any text editor. The -SessionType RestrictedRemoteServer field indicates that the session configuration will be used by JEA for secure management. Sessions configured this way will operate in NoLanguage mode and only have the following 8 default commands (and aliases) available:

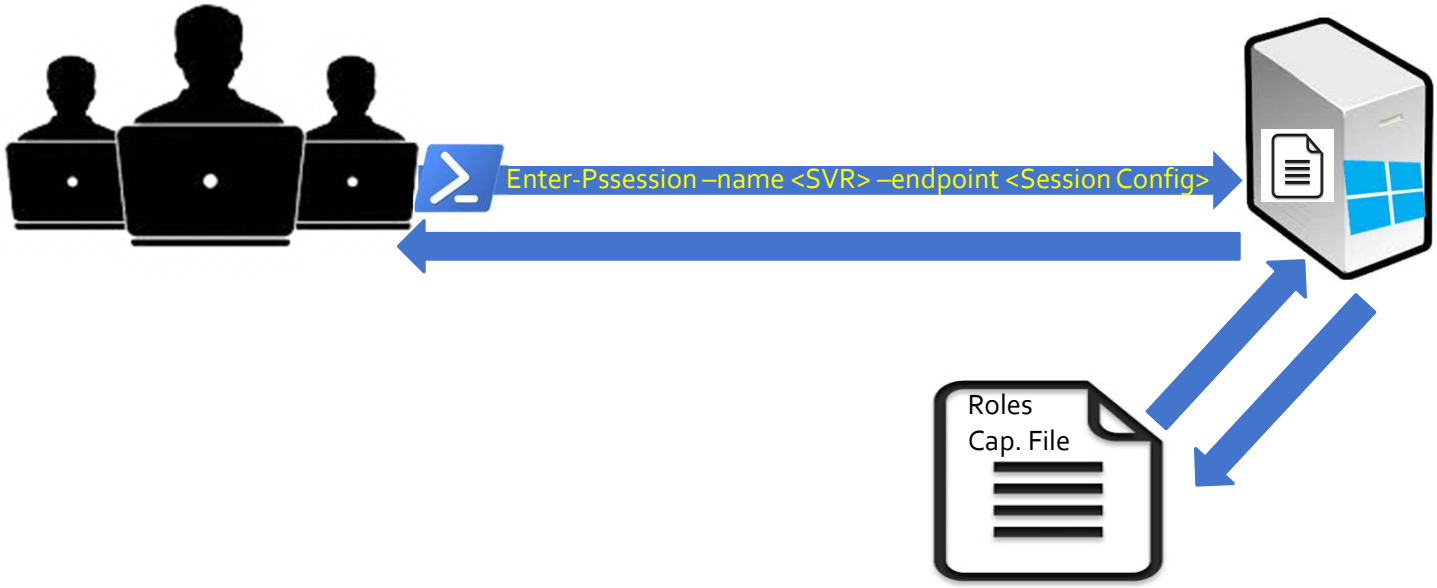
Clear-Host (cls, clear)
Exit-PSSession (exsn, exit)
Get-Command (gcm)
Get-FormatData
Get-Help
Measure-Object (measure)
Out-Default
Select-Object (select)

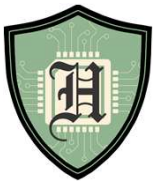
Session Configuration File

- New-PSSessionConfigurationFile -SessionType RestrictedRemoteServer -Path .\MyJEAEndpoint.pssc
- RunAsVirtualAccount = $true
- TranscriptDirectory = 'C:\ProgramData\JEAConfiguration\Transcripts'
- RoleDefinitions = @{
  - 'CONTOSO\JEA_DNS_ADMINS' = @{ RoleCapabilities = 'DnsAdmin', 'DnsOperator', 'DnsAuditor' }
  - 'CONTOSO\JEA_DNS_OPERATORS' = @{ RoleCapabilities = 'DnsOperator', 'DnsAuditor' }
  - 'CONTOSO\JEA_DNS_AUDITORS' = @{ RoleCapabilities = 'DnsAuditor' }
- }

https://docs.microsoft.com/en-us/powershell/jea/session-configurations

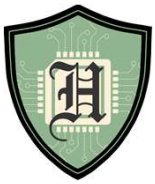
How It All Works Together



Demo Time

What Next



- Implementing is not a project, it is an ongoing task
- It empowers your users and fellow admins

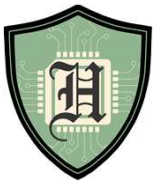
- Make them feel like

References & Further Reading

- https://docs.microsoft.com/en-us/powershell/jea/overview
- https://docs.microsoft.com/en-us/powershell/jea/role-capabilities
- https://docs.microsoft.com/en-us/powershell/jea/session-configurations
- SANs SEC505:Windows Security and PowerShell Automation
- https://www.youtube.com/watch?v=zftC6eDzRJY&t=1025s
- https://www.youtube.com/watch?v=f_Dd5fRXixY

Twitter: @P0w3rChi3f
LinkedIn: james-honeycutt
https://jameshoneycutt.net

Upcoming Talks and Classes



Jameshoneycutt.net/my-events

20 February – Unallocated Space (PowerShell JEA)

04-05 April – BsidesCharm (PowerShell Crash Course Workshop)

12 May – SANs SEC505 (Windows Security and PowerShell Automation)


THIS IS THE END OF THE PRESENTATION
ANY QUESTIONS?
IF NOT, JUST CLAP!