JEA Presentation

1. J-J-J-JEA Power
   1. James Honeycutt
   2. Twitter: @jay\_Honeycutt
   3. LinkedIn: james-honeycutt
2. About Me
   1. 23 Years Military Service
   2. 19 Years Windows Environment
   3. SANs Mentor (GCIH/SEC504, GCWN/SEC505)
   4. Self taught PowerShell
   5. Passion for PowerShell
3. What is PowerShell JEA
   1. “Just like keys on a key chain” – Jeffery Snover
   2. “Just Enough Administration (JEA) is a security technology that enables delegated administration for anything that can be managed with PowerShell.” –Microsoft
   3. “Really cool way to empower my user and fellow admins” – James Honeycutt
   4. Allows common users to perform admin functions (when properly configured)
   5. Not a project, it is an ongoing task
4. Requirements
   1. Client   
      Win 10 1511 or higher  
      Win 8, 8.1  
      Win 7
   2. Server  
      2016  
      2012, 2012r2  
      2008r2
5. How It Works
   1. User/Admin uses PowerShell remoting to access remote server using the Session configuration file and using “Runas”
   2. A virtual Admin account is created and used during THIS SESSION ONLY
   3. The virtual admin technically has access to all command lets, but only shows the user what they are entitled to, based on the Role Capabilities File
   4. User does what they need to, exits remote pssession, and Virtual Account is deleted.
6. Role Capabilities File
   1. Controls what Command Lets, Modules, Functions, and Parameters are allowed
   2. New-PSRoleCapabilityFile -Path .\MyFirstJEARole.psrc
      1. VisibleCmdlets =
   3. @{ Name = 'Restart-Service'; Parameters = @{ Name = 'Name'; ValidateSet = 'Dns', 'Spooler' }},
   4. @{ Name = 'Start-Website'; Parameters = @{ Name = 'Name'; ValidatePattern = 'HR\_\*' }}
   5. VisibleExternalCommands = 'C:\Windows\System32\whoami.exe', 'C:\Program Files\Contoso\Scripts\UpdateITSoftware.ps1'
7. Session Configurations
   1. Controls who can log in and determines what role capability file to use.
   2. 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
   3. 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)
8. Session Configuration File
   1. New-PSSessionConfigurationFile -SessionType RestrictedRemoteServer -Path .\MyJEAEndpoint.pssc
   2. RunAsVirtualAccount = $true
   3. TranscriptDirectory = 'C:\ProgramData\JEAConfiguration\Transcripts’
   4. RoleDefinitions = @{'CONTOSO\JEA\_DNS\_ADMINS'    = @{ RoleCapabilities = 'DnsAdmin', 'DnsOperator', 'DnsAuditor’ } 'CONTOSO\JEA\_DNS\_OPERATORS' = @{ RoleCapabilities = 'DnsOperator', 'DnsAuditor’ }  'CONTOSO\JEA\_DNS\_AUDITORS'  = @{ RoleCapabilities = 'DnsAuditor' }}
9. How It All Works Together (Demo)
10. What Next
    1. Implementing is not a project, it is an ongoing task
    2. It impowers your users and fellow admins
    3. It makes them feel like………
11. References & Further Reading
    1. <https://docs.microsoft.com/en-us/powershell/jea/overview>
    2. <https://docs.microsoft.com/en-us/powershell/jea/role-capabilities>
    3. https://docs.microsoft.com/en-us/powershell/jea/session-configurations
    4. SANs SEC505:Windows Security and PowerShell Automation
    5. <https://www.youtube.com/watch?v=zftC6eDzRJY&t=1025s>
    6. <https://www.youtube.com/watch?v=f_Dd5fRXixY>