JEA

Just **E**nough **A**dministration

PowerShell

about_Presenter

Martin Schvartzman

Senior Premier Field Engineer @ Microsoft

Blog: http://aka.ms/pstips

PowerShell

about_Agenda

- Scenario Overview
- Goals
- Use Cases
- What are Session Configurations?
- What are Delegated Endpoints?
- What are Constrained Endpoints?
- What is JEA?
- Setting up JEA
- Tips for JEA

PowerShell

about_Scenario_Overview

- Admin permissions should not be binary
- Too many people have too much access on too many servers
- If a hacker gets the password to a service account or admin account, then they have access to hundreds of servers (lateral traversal, pass-the-hash)
- Role Based Access Control (RBAC) is usually application specific
- How do I delegate server-level administration on an Active Directory Domain Controller without granting Domain Administrator access?

PowerShell

about_Goals

- Reduce the number of full admins
- Limit movement of full admin accounts
- Granular control over admin actions
- Log all admin actions

PowerShell

about_Use_Cases

- Auditors needing read-only access to systems
- Service desk tasks (account resets, etc.)
- NOC tasks (service resets, etc.)
- Hosted environments with multi-tenant administration
- Delegated administrative tasks

PowerShell

about_What_Are_Session_Configurations

- PSRemoting connects to endpoints called **session configurations**
- Default endpoints specify local Administrator access
- You can create your own **endpoints**

```
PS C:\> Get-PSSessionConfiguration | ft Name

Name
----
microsoft.powershell
microsoft.powershell.workflow
microsoft.powershell32
microsoft.windows.servermanagerworkflows
MySessionConfig

PS C:\> Enter-PSSession -ComputerName MS1 -ConfigurationName MySessionConfig
```

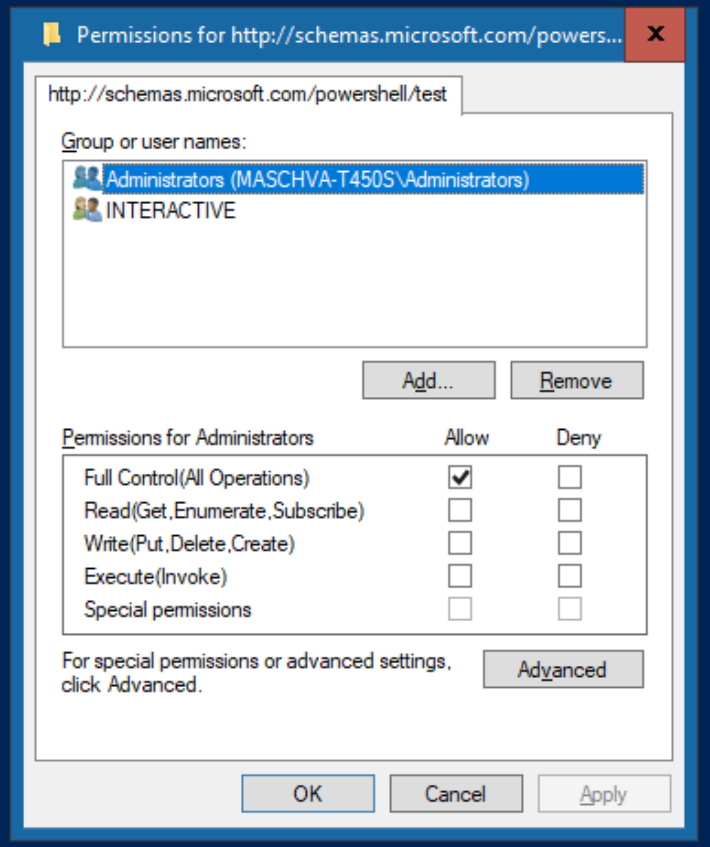
PowerShell

about_What_Are_Delegated_Endpoints

- Set-PSSessionConfiguration `
  -RunAsCredential
  - Endpoint runs in the context of another user

- Set-PSSessionConfiguration `
  -ShowSecurityDescriptorUI
  - Connection now requires a lower privileged account

- This enables an intentional
  "elevation of privilege"



PowerShell

about_What_Are_Constrained_Endpoints

- New-PSSessionConfigurationFile
  - -LanguageMode
  - -VisibleCmdlets
  - -VisibleFunctions
  - -Visible…

PowerShell

about_What_Is_JEA

- JEA – Just Enough Administration
- Uses PowerShell **constrained endpoints** to limit administration
- Allows **specific users** to perform **specific tasks** on **specific servers** without giving them full administrator rights
- Removes administration privilege from as many user accounts as possible while still allowing them to do their job (*principle of least privilege*)
- Role-based access control (RBAC) platform through Windows PowerShell

PowerShell

about_Prerequisites

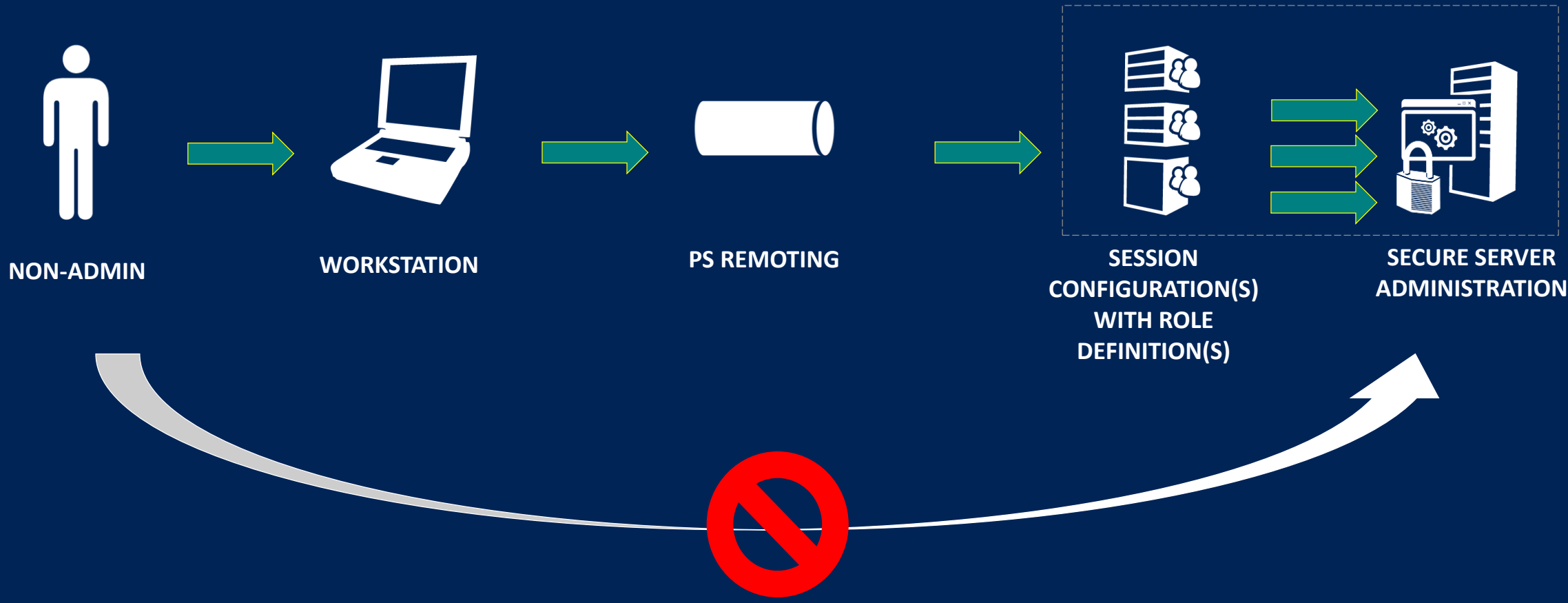
Server Operating System	JEA Availability
Windows Server 2016	Preinstalled
Windows Server 2012 R2	Full functionality w/ WMF 5.1
Windows Server 2012	Full functionality w/ WMF 5.1
Windows Server 2008 R2	Full functionality w/ WMF 5.1

```
PS C:\> $PSVersionTable.PSVersion
Major  Minor  Build  Revision
-----  -----  -----  --------
5      1      14393  1000

PS C:\> Enable-PowerShellRemoting #(if required)
```

PowerShell

about_What_Is_JEA (continued)



PowerShell

about_Setting_Up_JEA

- Create a Role Capability File
  - Visible cmdlets, functions, aliases, external commands, etc.
- Create a Configuration File
  - Language Mode, RunAsVirtualAccount, Mount user drive
- Register the Configuration
  - RunAsCredential, Permissions

PowerShell

about_Setting_Up_JEA: Role Capability File

- Create a Role Capability File (*.psrc) that will identify what cmdlets, functions, providers, & external programs can be used.
- Remember: Least Privileged Access

1. **Identify** the commands users are using to get their jobs done.
2. **Restrict** the scope of the cmdlets to only allow specific parameters or parameter values.
3. **Create** custom functions to replace complex commands or commands which are difficult to constrain.

PowerShell

about_Setting_Up_JEA: Configuration File

- Create a Session Configuration file (*.pssc) that defines the global settings of all roles on the endpoint
- Create a skeleton pssc file with:

```
New-PSSessionConfigurationFile -SessionType`
     RestrictedRemoteServer -Path .\TestJEAendpoint.pssc
```

- Edit with Notepad

PowerShell

about_Setting_Up_JEA: Register the Configuration

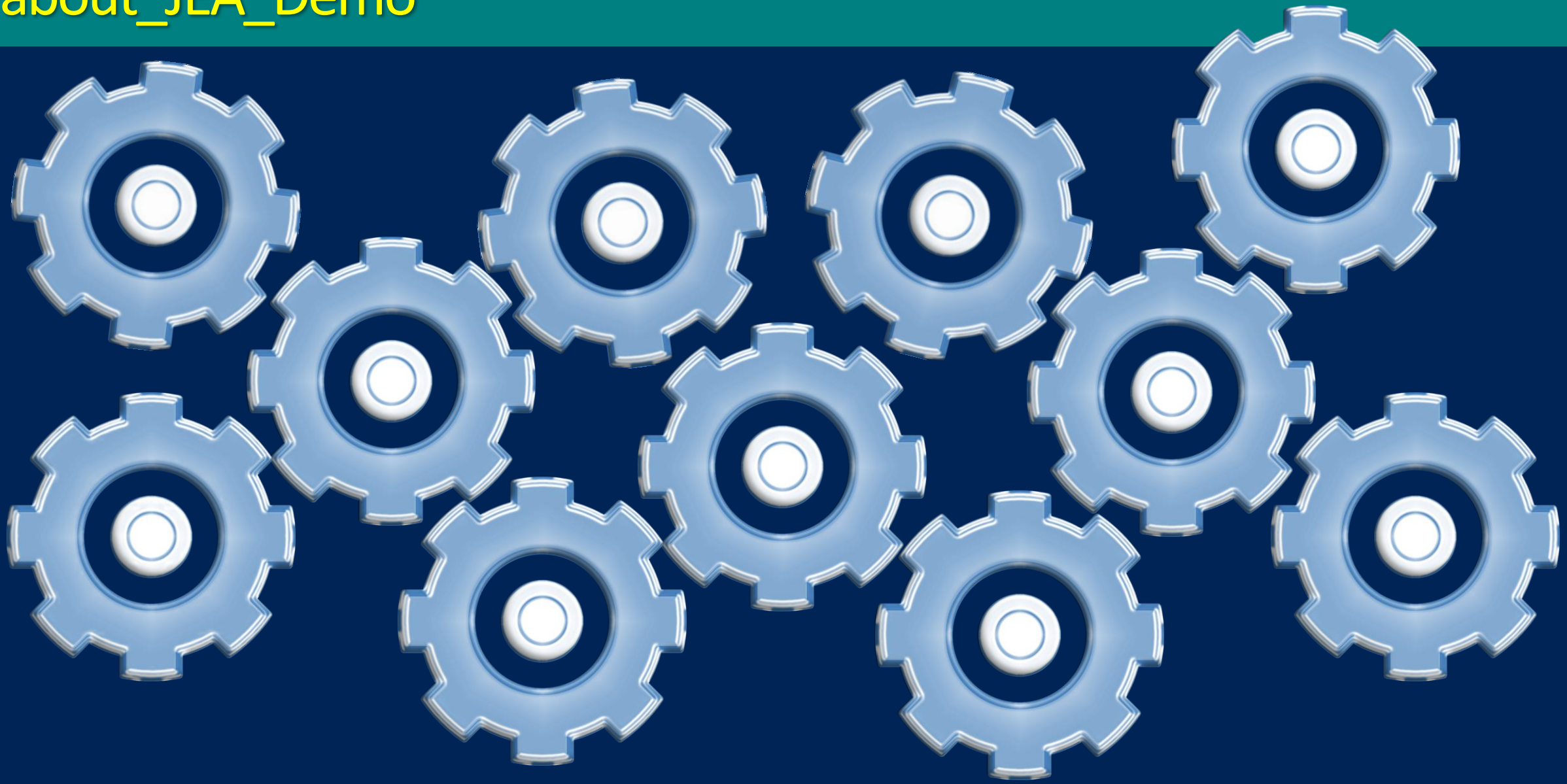
- Once roles and session configurations are defined, the endpoint must be registered
- Choose a name for the endpoint, and register it using:

```
Register-PSSessionConfiguration -Path .\TestJEAendpoint.pssc `
 -Name 'JEAendpoint' –Force
```

- If a pssc file is updated, the JEA endpoint must be unregister/re-registered

PowerShell

about_JEA_Demo



PowerShell

about_Tips_For_JEA

- Use DSC to configure JEA Endpoints
- Enable PowerShell Module Logging & Script Block Logging
- Use Windows Event Forwarding for greater security
- Enable PowerShell Transcription
- Set permissions on the transcript directory
- Audit RunAs authentications in **Microsoft-Windows-WinRM/Operational**, EventID **193**

```
Request for user S-1-5-21-3841426147-920288206-1542301449-1611 (CONTOSO\Alice)
will be executed using WinRM virtual account S-1-5-94-1452785133
```

about_Tips_For_JEA (continued)

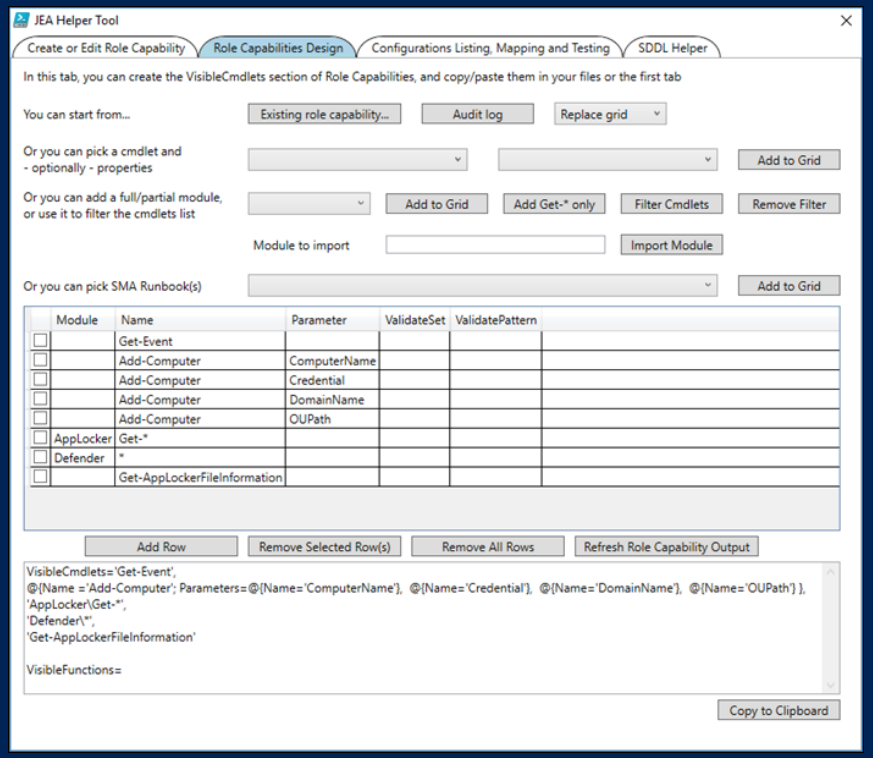
- Beware of dangerous commands to allow:
  - Granting the connecting user admin privileges to bypass JEA

    Add-ADGroupMember, Add-LocalGroupMember, net.exe, dsadd.exe
  - Running arbitrary code to bypass protections

    Start-Process, New-Service, Invoke-Item, Invoke-WmiMethod, Invoke-CimMethod, Invoke-Expression, Invoke-Command, New-ScheduledTask, Register-ScheduledJob
- Remember: None of this matters if you do not take away admin rights and remote desktop access to the servers

about_Tips_For_JEA (continued)

- **JEA Helper Tool 2.0**
  - Helper tool that builds the Role Capability and Session Configuration files
  - Performs simple file validation



https://gallery.technet.microsoft.com/JEA-Helper-Tool-20-6f9c49dd

PowerShell

about_More_Information

- Just Enough Administration Samples and Resources
  http://aka.ms/JEA
- Microsoft Distinguished Engineer Jeffrey Snover on JEA
  JEAhttp://powershell.org/tag/JEA
- Just Enough Administration (JEA) Infrastructure: An Introduction
  https://gallery.technet.microsoft.com/Just-Enough-Administration-6b5ad370
- TechNet Virtual Labs - Managing Windows Server 2016 (JEA, DSC, NANO)
  https://technet.microsoft.com/en-us/virtuallabs/default.aspx


Microsoft