

GIVE SUPER POWERS WITHOUT GIVING AWAY SUPER SECRETS

MR. ASHLEY MCGLONE

TECHNOLOGY STRATEGIST, TANIUM

TWITTER: @GOATEEPFE



#PSHSummit



OUTLINE



#PSHSummit



THE PROBLEM

- People put passwords in scripts (along with other secrets, API keys, etc.)
- Bad actors like it when you do this
- InfoSec wants to find you and do things to you
- Secrets show up in logging
- You are jeopardizing your company, your job, your livelihood when you do this



#PSHSummit



I CAN STILL SEE YOU...



-
- User land can see your script passwords...
 - Base64 encoded command, compiled EXE, secure string, etc.
 - Methods
 - PowerShell transcription and logging
 - PowerShell debugger
 - Task Manager process dump
 - Etc. Etc. Etc.



#PSHSummit



JEA - JUST ENOUGH ADMINISTRATION

- Keep secrets on the tools server behind a constrained PowerShell remoting session
- No credentials or secrets in user land scripts
- Can be interactive for operators
- Can be non-interactive for automation
- This is the way.



#PSHSummit



DEMO: USE CASE



- Help desk needs to look up data on users and computers from multiple sources.
- It is manual and takes too much time today.
- We don't want to give them credentials or console access to all backend systems.
- We don't want to add them to many security groups.
- We don't want to distribute a script with embedded credentials.



#PSHSummit



DEMO: HOW IT WORKS

- Prompt support operator for USERNAME:
 - Query Tanium for computer details where USERNAME is logged in.
 - Query Active Directory for other COMPUTERTNAME details
 - Query identity API for USERNAME passphrase
- All authentication secrets are sealed behind JEA:
 - Active Directory credential
 - Tanium credential
 - Identity solution API key



#PSHSummit





Misty Mountains

Far over the Misty Mountain cold
To Dungeons deep, and caverns old
We must away, ere break of day
To find our long, forgotten password

Songwriters: Janet Roddick, Stephen Gerard Roche, David Orien Long, David Geoffrey Donaldson, J.R.R. Tolkien

JEA – JUST ENOUGH ADMINISTRATION *SUPER GRANULAR ACCESS*

PERMISSION LAYERS

- Windows Box (firewall, groups, ACLs, etc.)
 - PSSessionConfiguration
 - JEA Module
 - AD user or group
 - Role capabilities
 - Conditional access rules

ACCOUNT OPTIONS

- 😊 Virtual Account – local admin access (computer acct on network)
- 😊 GMSA – local and network access
- 😊 Pass-through user – what is granted
- 😊 PSSC RunAsCredential – breaks JEA role capability group assignment



#PSHSummit



<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/session-configurations?view=powershell-7.1>

```
PS C:\> Get-PSSessionConfiguration
```

```
Name       : GoateeTools ←  
PSVersion  : 5.1  
StartupScript :  
RunAsUser   :  
Permission  : GOATEE\Goatee_Tools_Users AccessAllowed
```

```
Name       : microsoft.powershell ←  
PSVersion  : 5.1  
StartupScript :  
RunAsUser   :  
Permission  : NT AUTHORITY\INTERACTIVE AccessAllowed,  
              BUILTIN\Administrators AccessAllowed,  
              BUILTIN\Remote Management Users AccessAllowed
```



#PSHSummit



The diagram illustrates the structure of a Windows Host PSSessionConfiguration. It shows a hierarchy starting with 'Windows Host', followed by 'PSSessionConfiguration'. Inside this, there is a 'JEA Module' which contains two entries: 'AD User or Group 1' with 'Role Capability A', and 'AD User or Group 2' with 'Role Capability B'. To the right of the diagram, three command-line examples for 'Enter-PSSession' are provided, each with its corresponding security context and access level.

Windows Host

PSSessionConfiguration

JEA Module

AD User or Group 1

Role Capability A

AD User or Group 2

Role Capability B

Enter-PSSession -ComputerName x

Default Administrators PSSessionConfiguration
Must be a member of local Administrators
Full access to the server and commands

Enter-PSSession -ComputerName x -ConfigurationName y

Running in user or group security context with from local machine
Custom PSSessionConfiguration and experience
Access to only commands allowed in capability A

Enter-PSSession -ComputerName x -ConfigurationName y

Running in user or group security context from local machine
Custom PSSessionConfiguration and experience
Access to only commands allowed in capability B

#PSHSummit

<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/session-configurations?view=powershell-7.1>

RUNAS VIRTUAL ACCOUNTS ***BEST PRACTICE***

- Virtual accounts are temporary accounts that are unique to a specific user and only last for the duration of their PowerShell session.
- Local access only. Network access under the computer account.
- On a member server or workstation, virtual accounts belong to the local computer's Administrators group.
- On an Active Directory Domain Controller, virtual accounts belong to the domain's Domain Admins group.
- You can specify the security groups to which the virtual account will belong. On a member server or workstation, the specified security groups must be local groups, not groups from a domain. When one or more security groups are specified, the virtual account isn't assigned to the local or domain administrators group.



#PSHSummit



<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/session-configurations?view=powershell-7.1>

RUNAS GMSA (GROUP-MANAGED SERVICE ACCT)

- Use when JEA users need to access network resources such as file shares and web services.
- Give you a domain identity that is used to authenticate with resources on any machine within the domain.
- The rights are determined by the resources you're accessing.
- You don't have admin rights on any machines or services unless the machine or service administrator has explicitly granted those rights to the GMSA.
- Enables "second hop" with fresh credentials.



#PSHSummit



<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/session-configurations?view=powershell-7.1>

LOGGING

- Enable all PowerShell logging (you're already doing this, right?)
- Transcription dedicated to remoting
- Transcription, Script Block Logging, Module Logging
- Transcription
 - Notice the header information with the remote connecting user vs. RunAs account
 - `winRM Virtual Users\winRM_VA_<NUMBER>_<DOMAIN>_<SAMAccountName>`



#PSHSummit



WHY NOT USE THE NEW SECRET STORE MODULE?

It stores passwords in the local user profile. The JEA virtual account is a temporary, transient account without a persistent user profile on the server.

You would still have to secure the password to unlock the store.



#PSHSummit



LET'S BUILD IT OUT FROM SCRATCH



#PSHSummit



YOUR TURN

- This is all documented on the GitHub link to follow.
- This is non-trivial. I wish it were easier. Security is hard.
- Everything is there if you take the time to read through and adjust to your environment.
- Non-Tanium customers can adjust for their own line-of-business uses.
- Customization will be required for your environment.
- *DISCLAIMER: This example uses a private encryption key stored directly on the server.*



#PSHSummit



THE RESOURCES

GitHub with slides & scripts & setup guide from today

<http://bit.ly/PS2021JEA>



#PSHSummit

