GIVE SUPER POWERS WITHOUT GIVING AWAY SUPER SECRETS

MR. ASHLEY MCGLONE

TECHNOLOGY STRATEGIST, TANIUM

TWITTER: @GOATEEPFE

#PSHSummit

OUTLINE

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

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.

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.

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.

DEMO: HOW IT WORKS

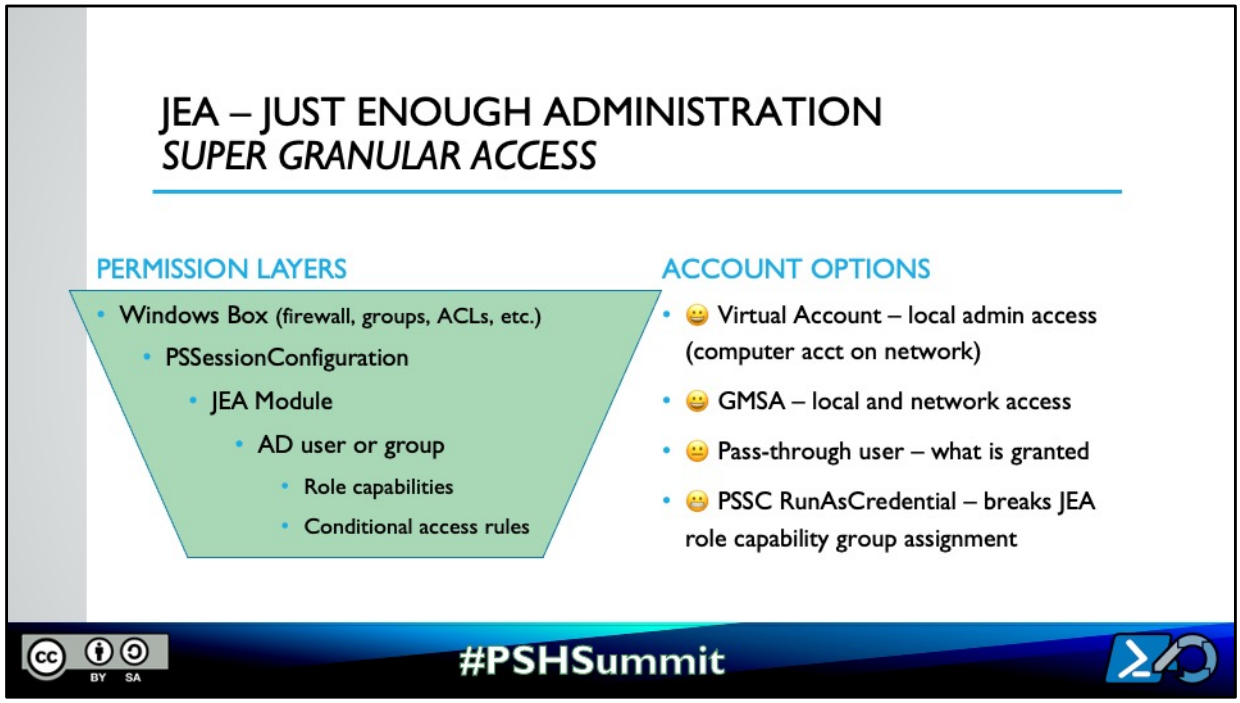
- Prompt support operator for USERNAME:
  - Query Tanium for computer details where USERNAME is logged in.
    - Query Active Directory for other COMPUTERNAME details
  - Query identity API for USERNAME passphrase

- All authentication secrets are sealed behind JEA:
  - Active Directory credential
  - Tanium credential
  - Identity solution API key

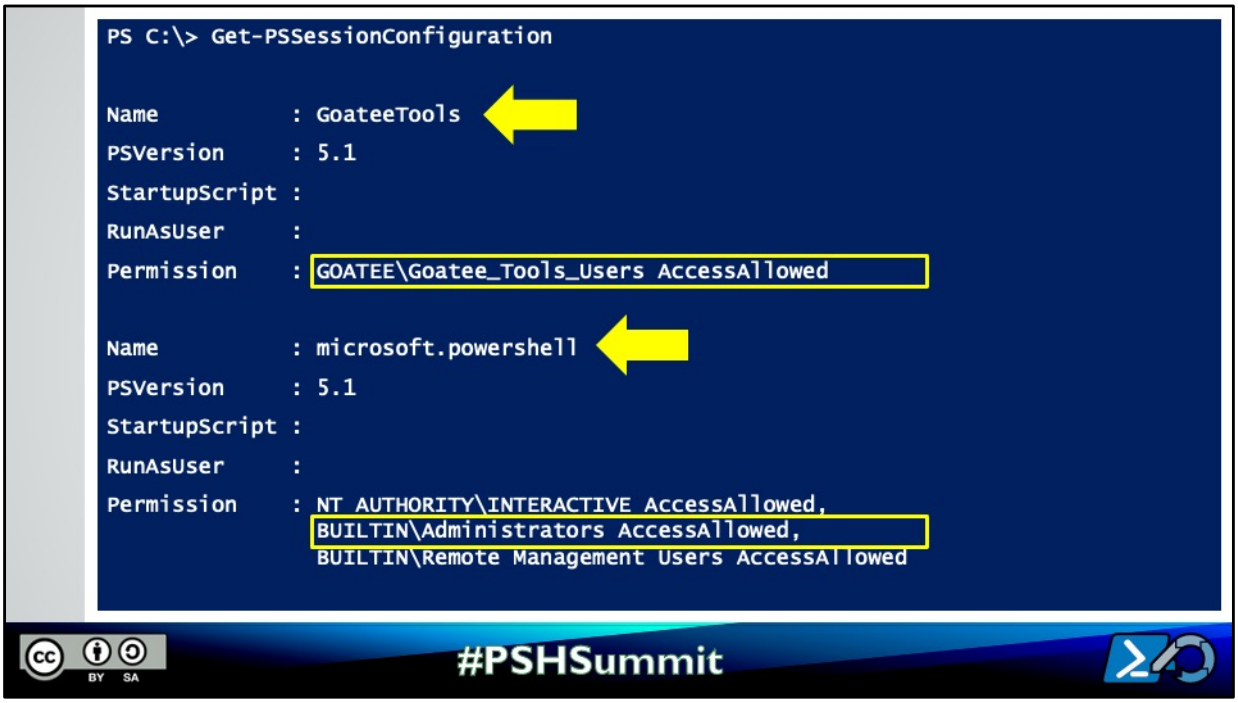
Misty Mountains

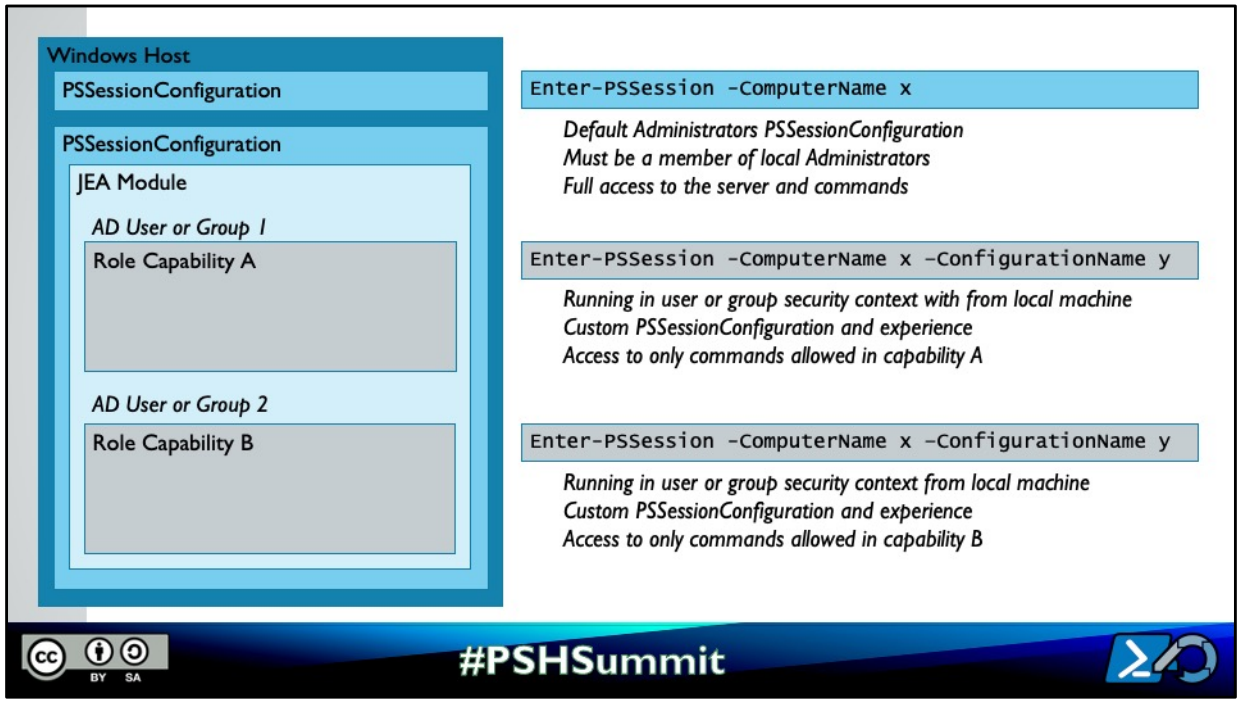
Far over the Misty Mountain cold
To Dungeons deep, and caverns old
We must away, ere break of day
To find our long, forgotten password

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

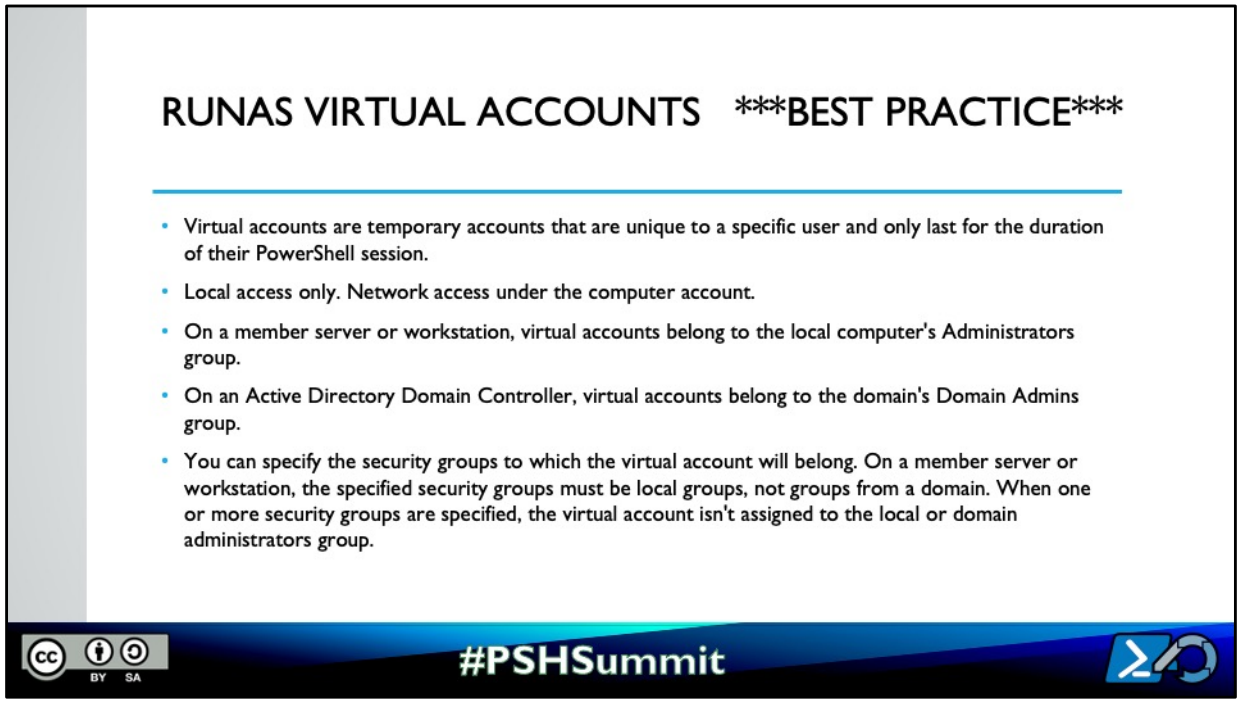


https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/session-configurations?view=powershell-7.1

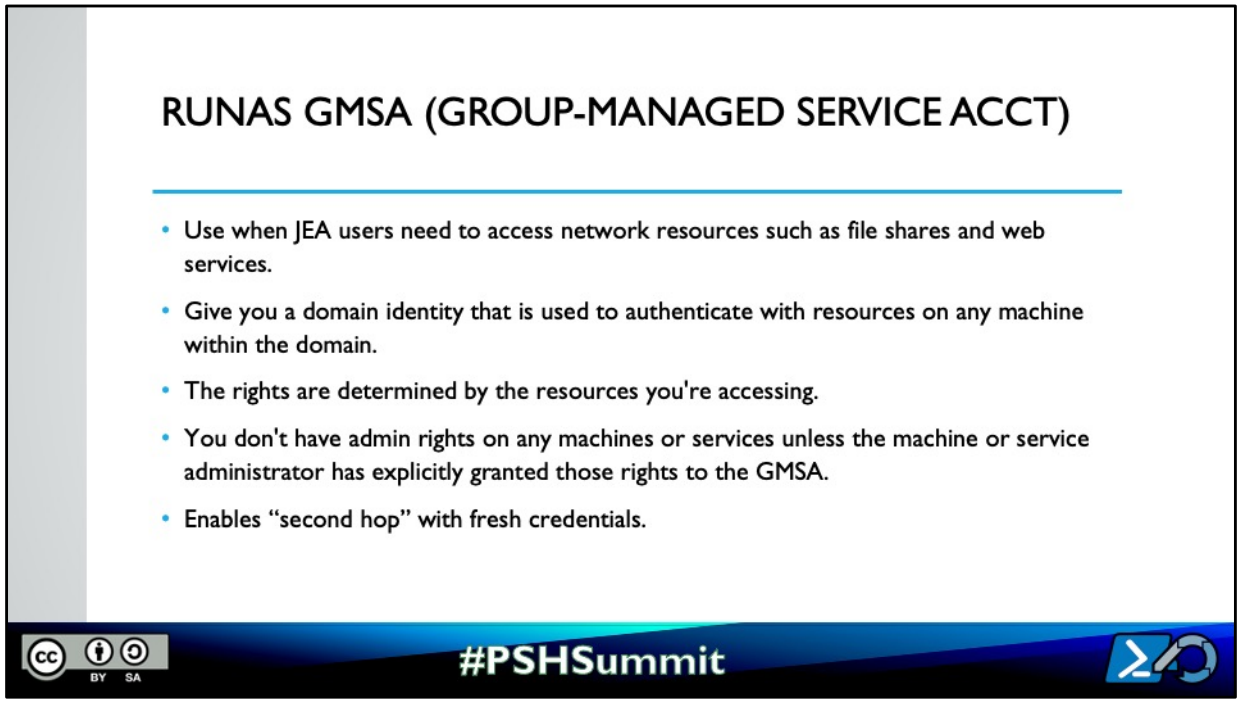

PS C:\> Get-PSSessionConfiguration
Name : GoateeTools
PSVersion : 5.1
StartupScript :
RunAsUser :
Permission : GOATEE\Goatee_Tools_Users AccessAllowed
Name : microsoft.powershell
PSVersion : 5.1
StartupScript :
RunAsUser :
Permission : NT AUTHORITY\INTERACTIVE AccessAllowed,
BUILTIN\Administrators AccessAllowed,
BUILTIN\Remote Management Users AccessAllowed
#PSHSummit



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



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



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

LOGGING

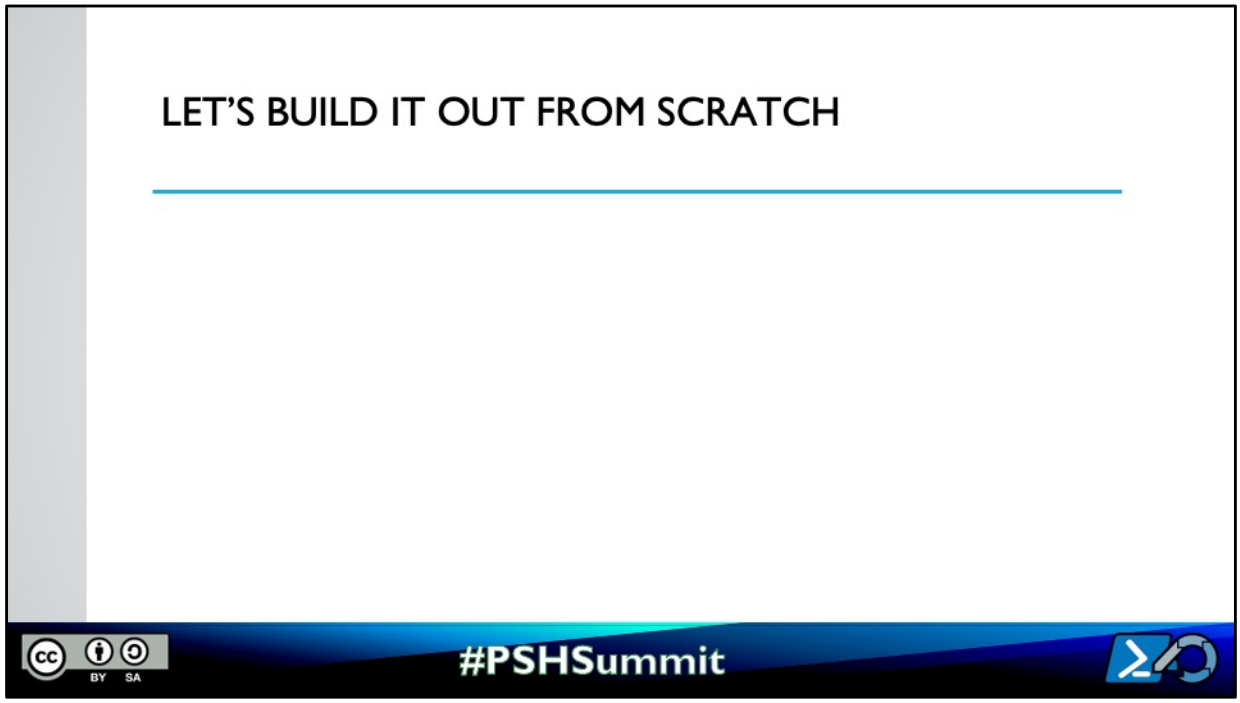
- Enable all PowerShell logging (you're already doing this, right?)
- Transcription dedicated to remoting
- Transcription, Script Block Logging, Module Logging
- Transcription
  - Notice the header information with the remote connecting user vs. RunAs account
  - `WinRM Virtual Users\WinRM_VA_<NUMBER>_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

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.

LET'S BUILD IT OUT FROM SCRATCH



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.*

THE RESOURCES

GitHub with slides & scripts & setup guide from today

http://bit.ly/PS2021JEA