Windows Domain Hardening

Darren LaCasse

Disclaimer

- All material presented is my own unless otherwise specified.
- Don’t take this as the one and only way to do this
  - Your organization is unique, maybe…
  - YMMV

Agenda

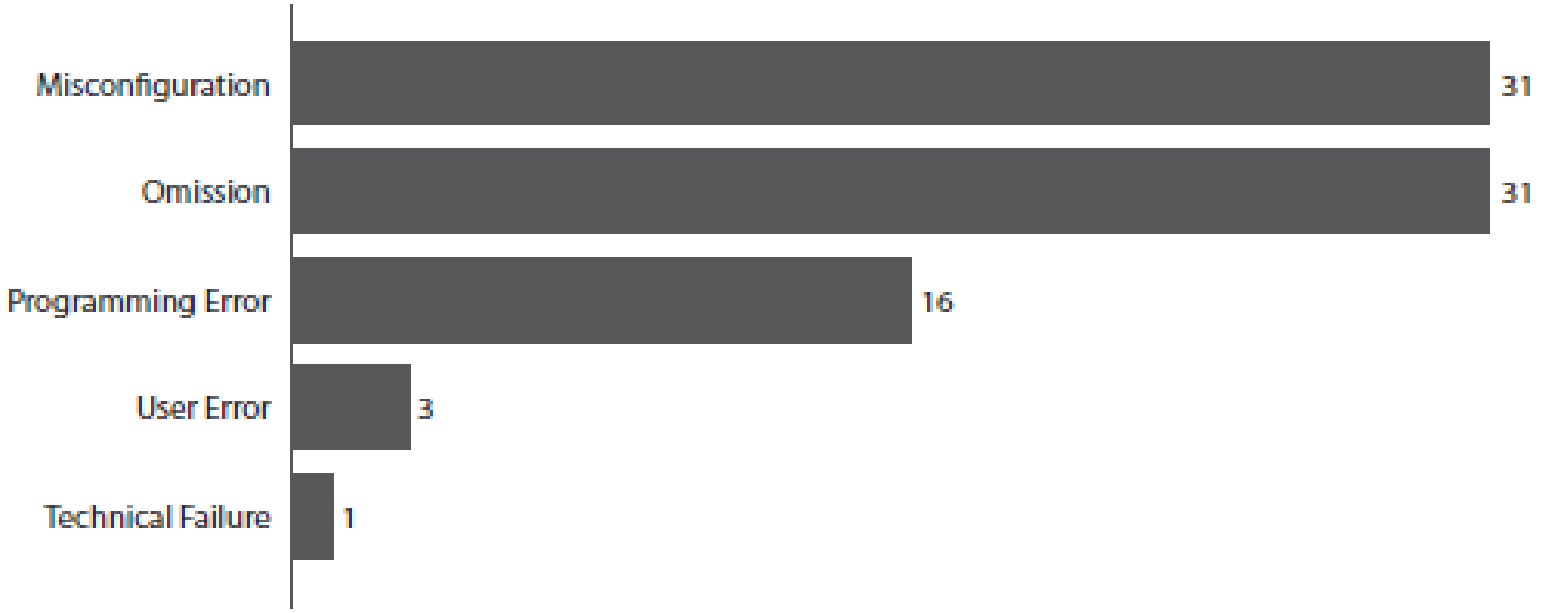
- Hardening 101
- Hardening Challenges
- Configuration/Monitoring Tools
- Demo

Why do we care?

- Improves system security
  - Systems configured with minimum necessary services
- Improves system availability
  - All systems configured the same
  - Help desk has a single configuration to support
  - Problem on 1 system can be avoided on the rest

No really, why do we care?

Figure 21. Types of error by number of breaches



Verizon DBIR 2010

Common Hardening Tasks

- Apply OS and application patches
- Disable “Administrator” account
- Password requirements
  - Length
  - Complexity
  - Expiration
  - Lockout
- Install Antivirus
- Disable services

SecMN

- Start
  - Ce
  - NS
  - Mic

2.2.6 Set 'Allow log on locally' to 'Administrators' (Scored)

Profile Applicability:

- Level 1 - Domain Controller
- Level 1 - Member Server

Description:

This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the The recommended state for this setting is: `Administrators`.

Rationale:

Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

Audit:

Navigate to the UI Path articulated in the Remediation section and confirm it is set as prescribed.

Remediation:

To implement the recommended configuration state, set the following Group Policy setting to `Administrators`.

```
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights
Assignment\Allow log on locally
```

Impact:

If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. If you have installed optional components such as ASP.NET or Internet Information Services, you may need to assign Allow log on locally

Default Value:

Administrators, Users, Backup Operators

References:

1. CCE-37659-0

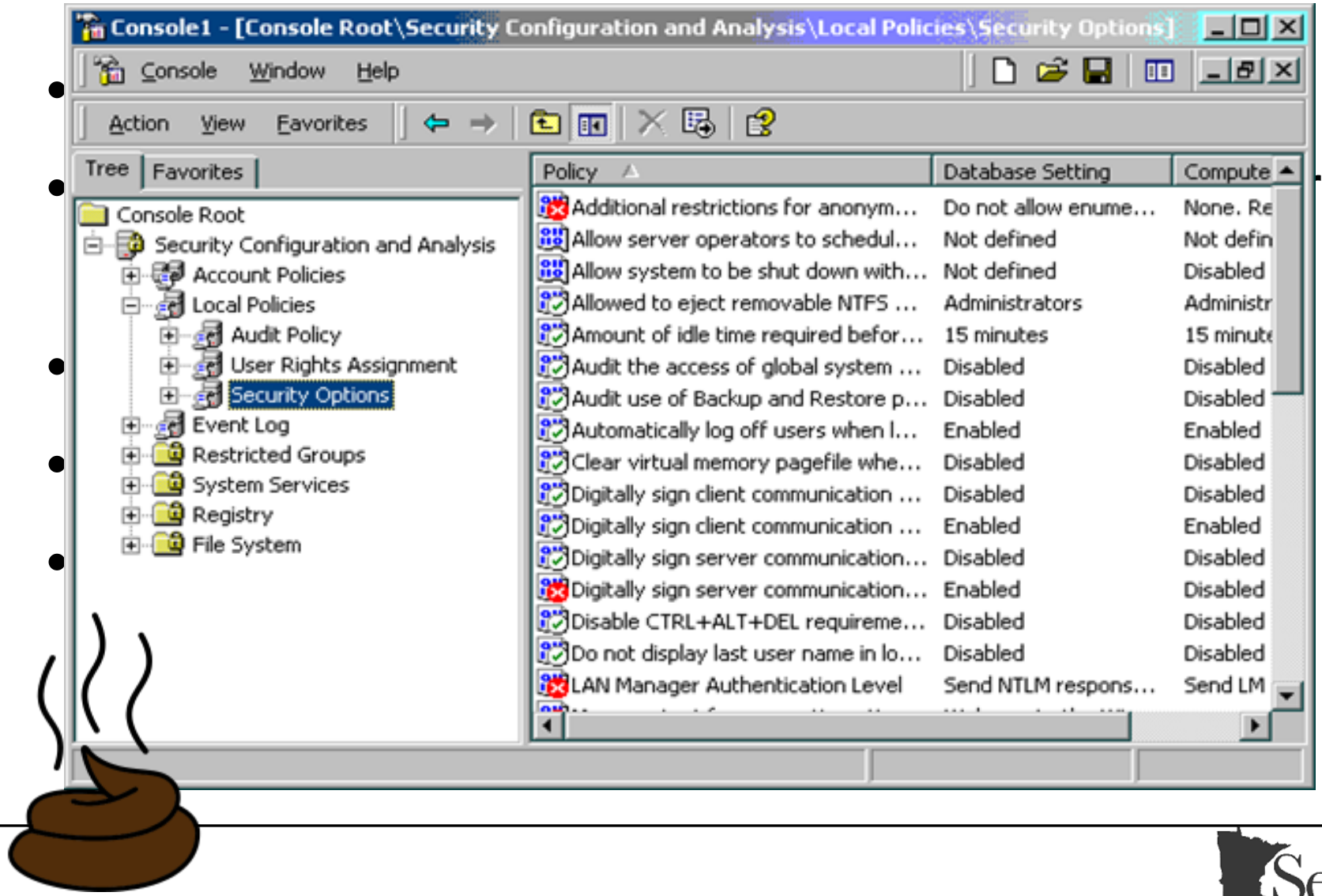
System Hardening Methods

- Manual
  - Human error
  - Personnel must know where the current baseline is
  - Not reasonable with large # of systems
- Automatic
  - Always the same
  - Removes human error

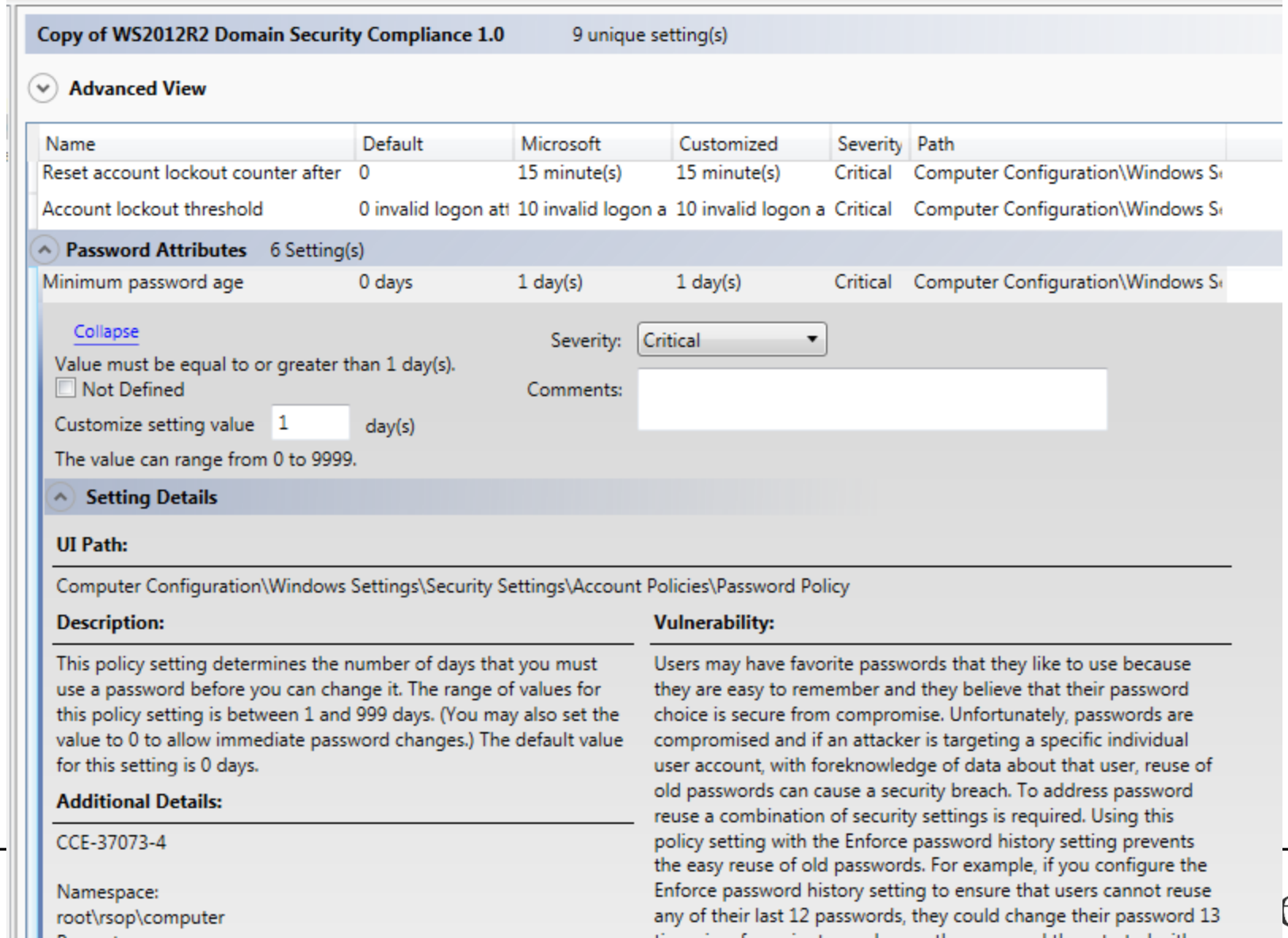
Hardening Tools

- Microsoft Security Configuration and Analysis Tool (SCAT)
- Microsoft Security Compliance Manager (SCM)
- PowerShell Desired State Configuration (DSC)

SCAT


Console1 - [Console Root\Security Configuration and Analysis\Local Policies\Security Options]
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Console Root
Security Configuration and Analysis
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Event Log
Restricted Groups
System Services
Registry
File System
Policy
Database Setting
Compute
Additional restrictions for anonym...
Do not allow enume...
None. Re
Allow server operators to schedul...
Not defined
Not defin
Allow system to be shut down with...
Not defined
Disabled
Allowed to eject removable NTFS ...
Administrators
Administr
Amount of idle time required befor...
15 minutes
15 minute
Audit the access of global system ...
Disabled
Disabled
Audit use of Backup and Restore p...
Disabled
Disabled
Automatically log off users when l...
Enabled
Enabled
Clear virtual memory pagefile whe...
Disabled
Disabled
Digitally sign client communication ...
Disabled
Disabled
Digitally sign client communication ...
Enabled
Enabled
Digitally sign server communication...
Disabled
Disabled
Digitally sign server communication...
Enabled
Disabled
Disable CTRL+ALT+DEL requireme...
Disabled
Disabled
Do not display last user name in lo...
Disabled
Disabled
LAN Manager Authentication Level
Send NTLM respons...
Send LM

Security Compliance Manager



Security Compliance Manager

- Gives us baselines from MS for
  - Operating Systems
  - Applications
    - IIS
    - DNS
    - DHCP
    - Internet Explorer
    - MS Office
- Doesn’t provide a way to apply to systems

Desired State Configuration (DSC)

- PowerShell feature
  - If you can PowerShell you can use DSC
- DSC you to configure and report on practically anything on the system
  - Registry
  - Files
  - Configurations
  - Services
  - Software

https://technet.microsoft.com/en-gb/library/dn249912.aspx

Computers are hard…

- DSC works great if you aren't on a consumer OS
- DSC works great if you have SCCM or SCVMM

How to DSC

- Write a DSC script (I tried and failed)

```
configuration TestScript {
 param ()
 Node Localhost
 {
   # Create a Test File
   File CreateTestFile
   {
     Ensure          = "Present"
     DestinationPath = "C:\Tempa\example.txt"
     Contents        = “Example."
     Type            = "File"
   }
 }
}
# Create MOF Files
HelloWorld -OutputPath C:\Temp\TestScript
# Start DSC Configuration
Start-DscConfiguration -Path C:\Temp\TestScript -ComputerName Localhost -Verbose -Wait
```

```
PS C:\Windows\system32> configuration HelloWorld {
 param ()
 Node Localhost
 {
   # Create a Test File
   File CreateTestFile
   {
     Ensure          = "Present"
     DestinationPath = "C:\ScriptimusExMachina\example.txt"
     Contents        = "Hello World."
     Type            = "File"
   }
 }
}

# Create MOF Files
HelloWorld -OutputPath C:\ScriptimusExMachina\HelloWorld

# Start DSC Configuration
Start-DscConfiguration -Path C:\ScriptimusExMachina\HelloWorld -ComputerName Localhost -Verbose -Wait



    Directory: C:\ScriptimusExMachina\HelloWorld


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
-a---         6/17/2015   2:31 PM       1306 Localhost.mof
VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, ''methodName' = SendConfigurationApply,'c
The client cannot connect to the destination specified in the request. Verify that the service on the destination
commonly IIS or WinRM. If the destination is the WinRM service, run the following command on the destination to an
    + CategoryInfo          : ConnectionError: (root/Microsoft/...gurationManager:String) [], CimException
    + FullyQualifiedErrorId : HRESULT 0x80338012
    + PSComputerName        : Localhost

VERBOSE: Operation 'Invoke CimMethod' complete.
VERBOSE: Time taken for configuration job to complete is 6.025 seconds



PS C:\Windows\system32>
```

https://scriptimus.wordpress.com/2015/04/14/powershell-desired-state-configuration-getting-started/

SecMN

Check Against the Configuration

- Test-DscConfiguration

```
PS C:\Temp\confout\SetServices> Test-DscConfiguration
True
```

  - Returning the value of “True” means the single value in our MOF is met
  - If we change the text in example.txt then we get this

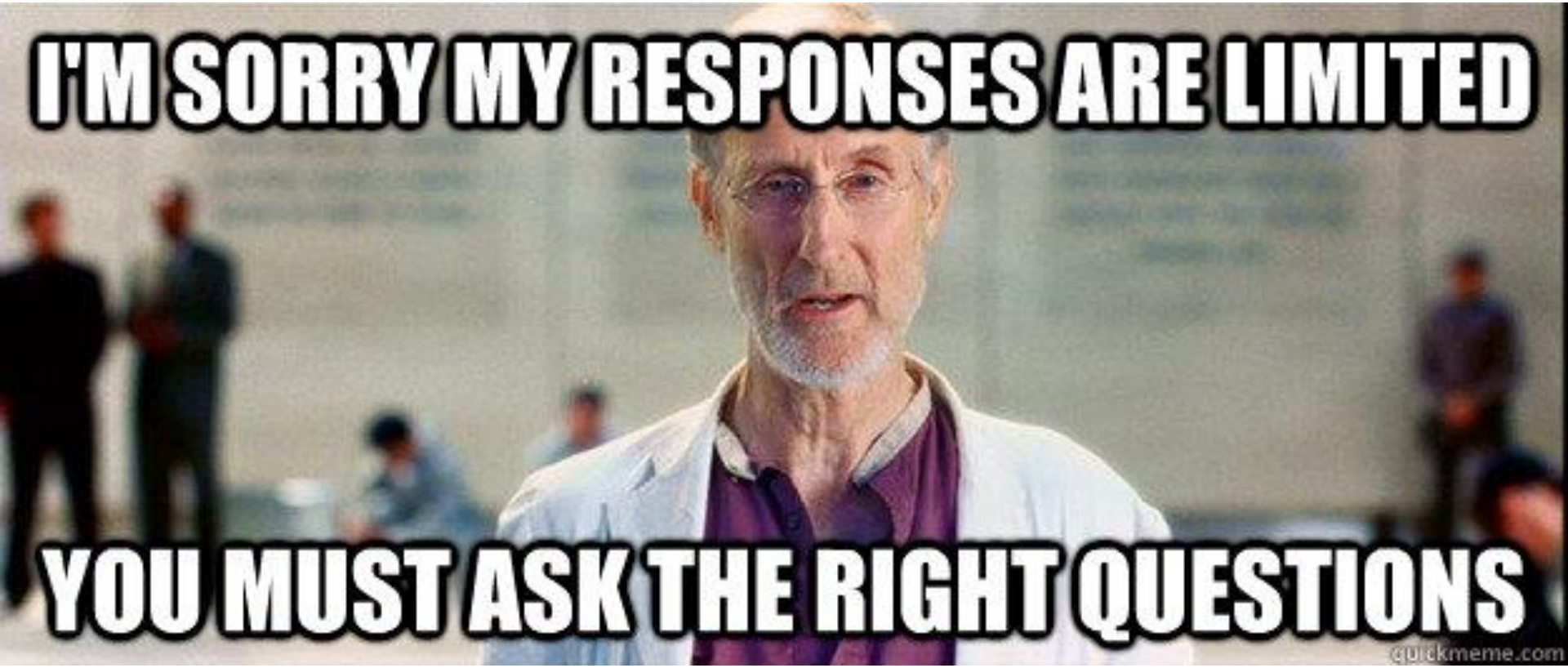
```
PS C:\Temp\confout\SetServices> Test-DscConfiguration
False
```

You configured one value, GREAT…

- Where you can go from here
  - Convert your orgs baseline to DSC syntax
    - Lots of time the first go
  - Output per system with values that are “False”
  - Startup scripts?
  - Buy SCCM?
  - GPO health!
  - Remove local admin rights

Tell me there is something else!

- Chef
  - https://www.chef.io/
- Puppet
  - https://puppetlabs.com/
- Nessus
  - http://www.tenable.com/products/nessus-vulnerability-scanner


I'M SORRY MY RESPONSES ARE LIMITED
YOU MUST ASK THE RIGHT QUESTIONS
quickmeme.com