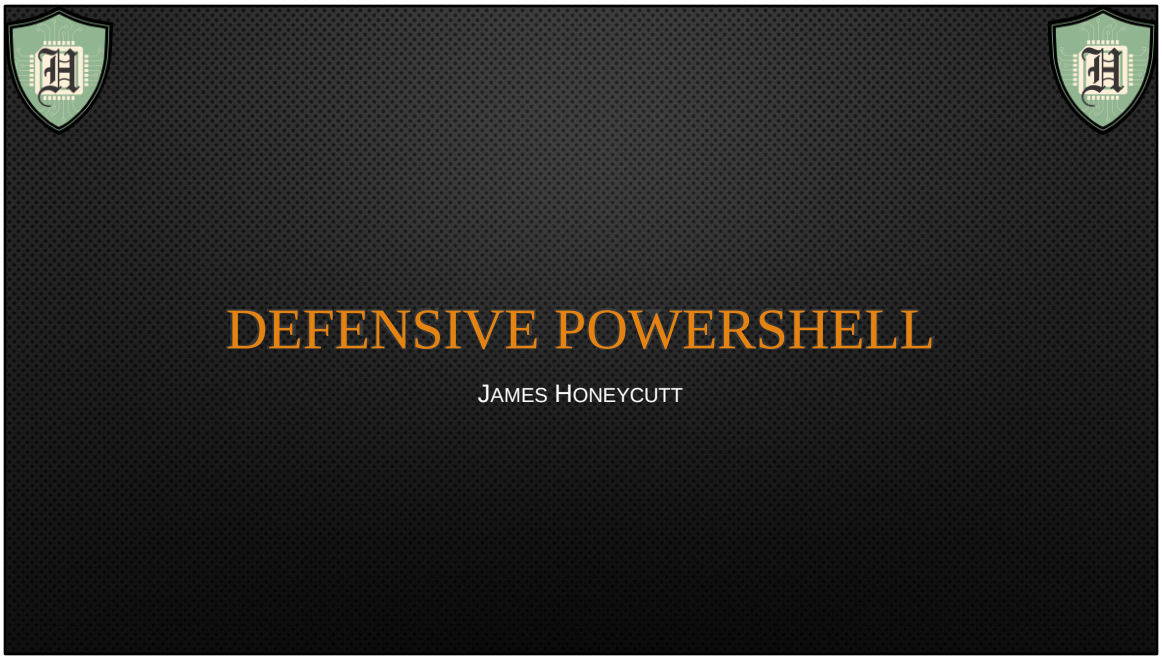
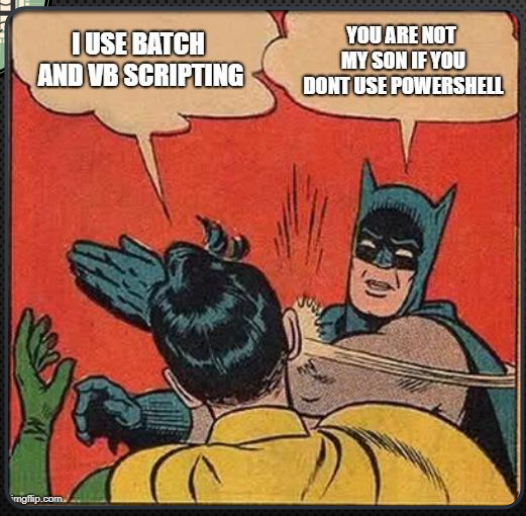


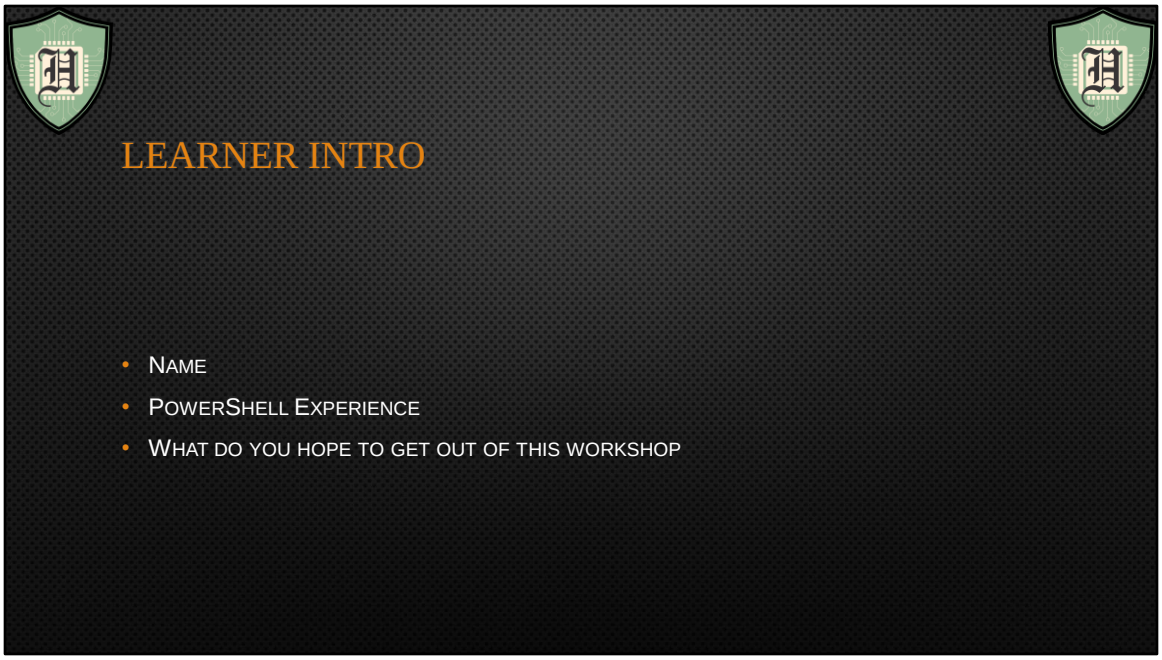
https://docs.microsoft.com/en-us/powershell/module/defender/?view=windowsserver2022-ps



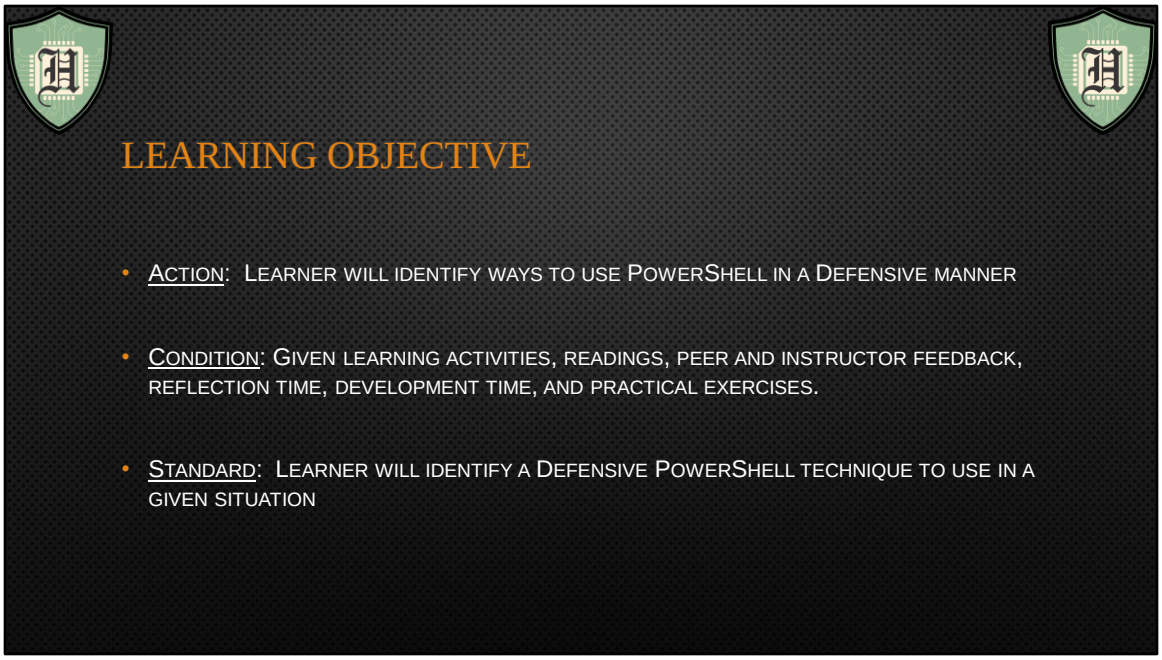
ABOUT ME

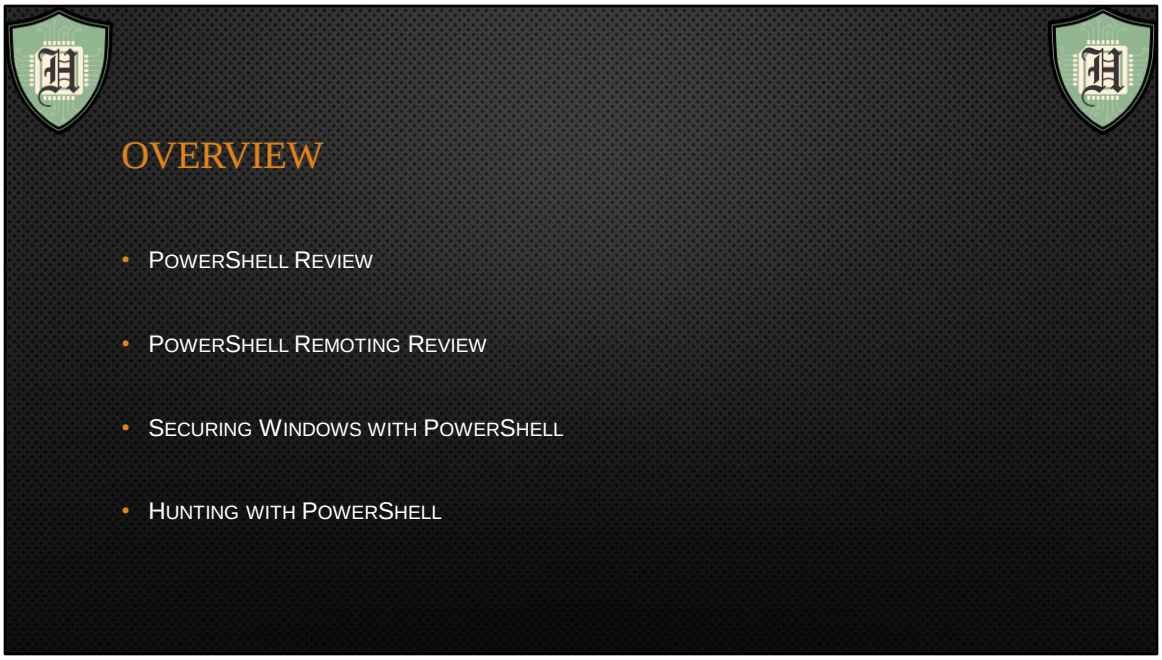
- OVER 20 YEARS IN IT/CYBER
- SELF-TAUGHT POWERSHELL BACK IN POWERSHELL V2
- POWERSHELL WAS MAIN JOB FUNCTION DURING MY LAST TWO POSITIONS

22:38 2

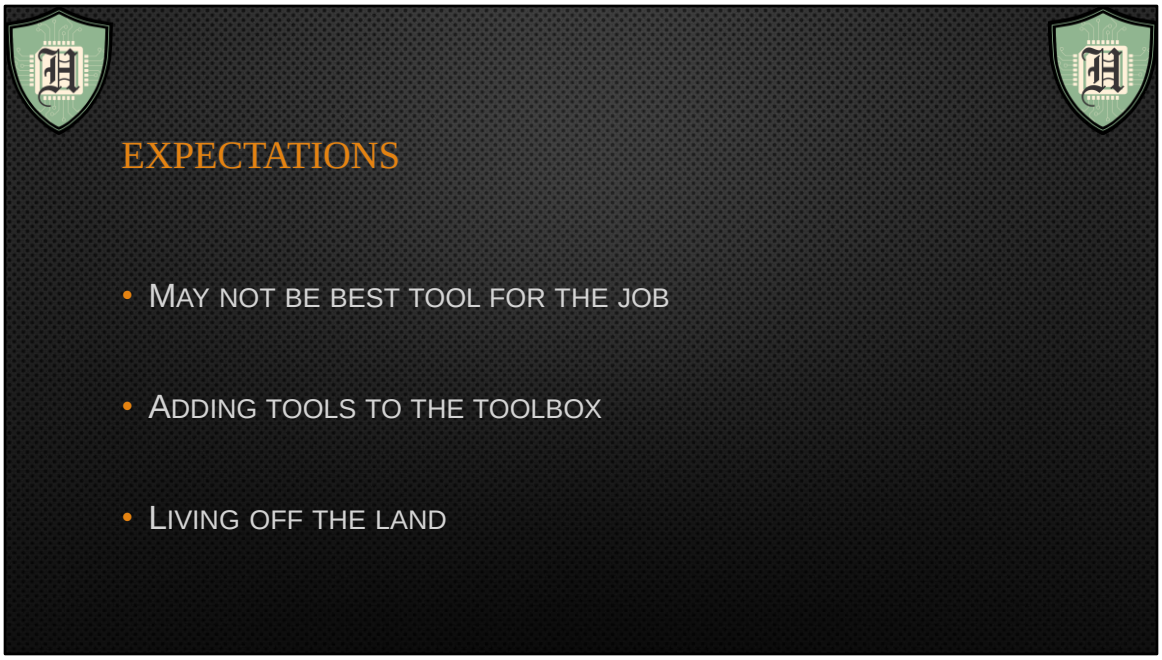

LEARNER INTRO
• Name
• PowerShell Experience
• What do you hope to get out of this workshop

INSERT MOTIVATOR HERE

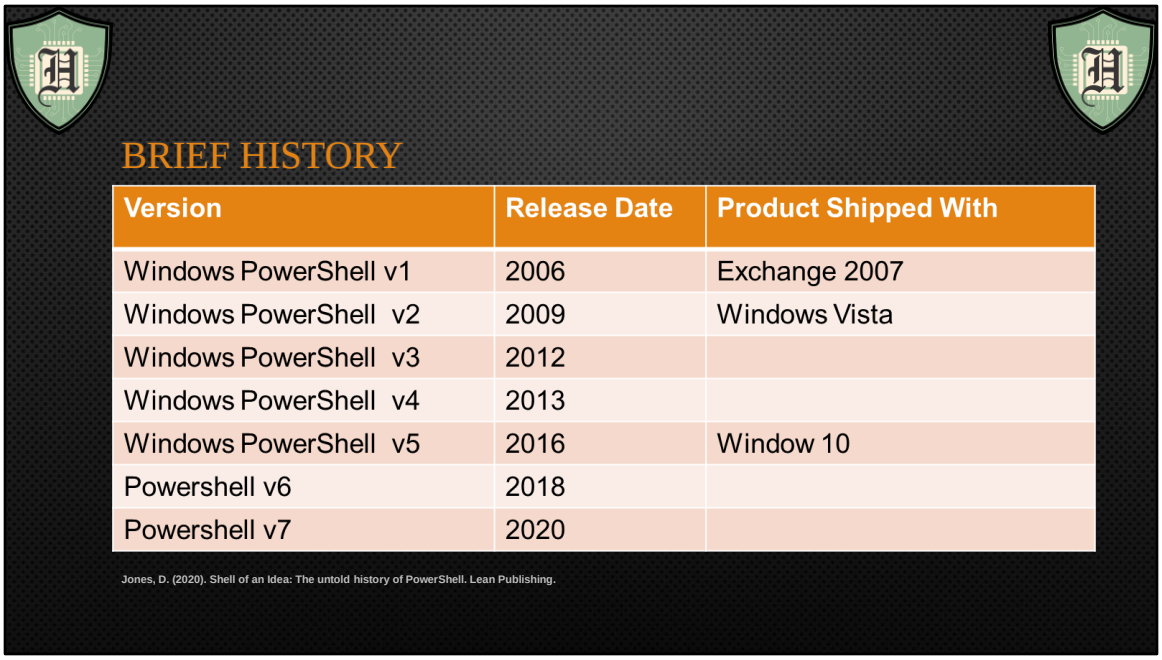

LEARNING OBJECTIVE
• ACTION: LEARNER WILL IDENTIFY WAYS TO USE POWERSHELL IN A DEFENSIVE MANNER
• CONDITION: GIVEN LEARNING ACTIVITIES, READINGS, PEER AND INSTRUCTOR FEEDBACK, REFLECTION TIME, DEVELOPMENT TIME, AND PRACTICAL EXERCISES.
• STANDARD: LEARNER WILL IDENTIFY A DEFENSIVE POWERSHELL TECHNIQUE TO USE IN A GIVEN SITUATION

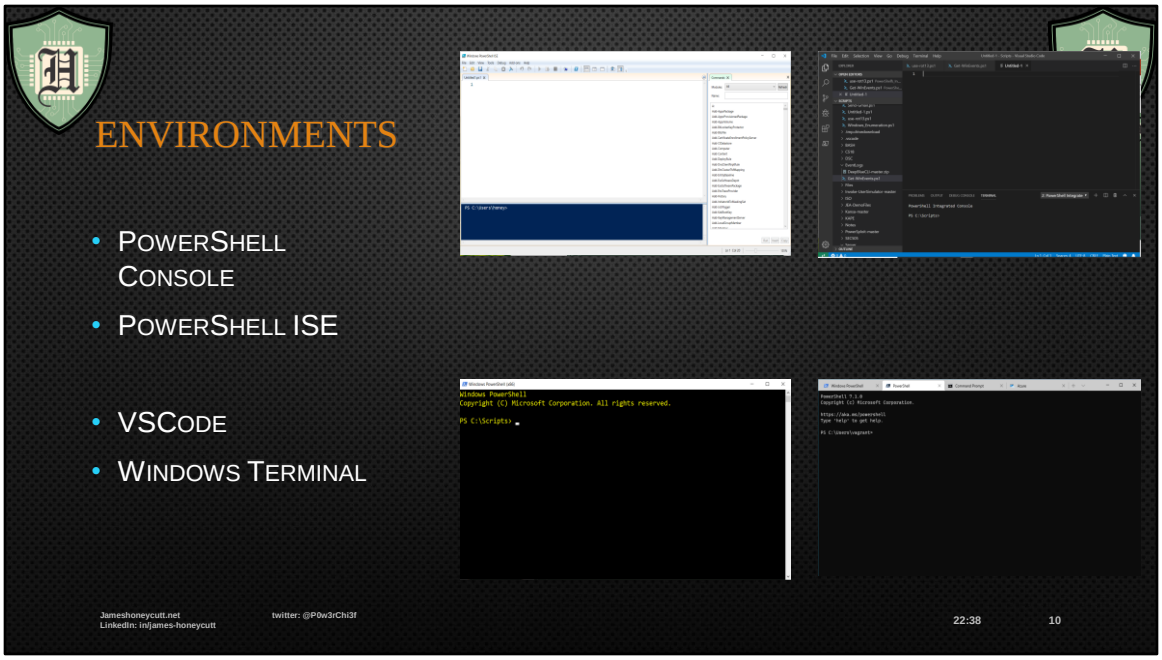

OVERVIEW
• PowerShell Review
• PowerShell Remoting Review
• Securing Windows with PowerShell
• Hunting with PowerShell


POWERSHELL REVIEW
• POWERSHELL HISTORY
• THE VARIOUS SHELL OF POWERSHELL



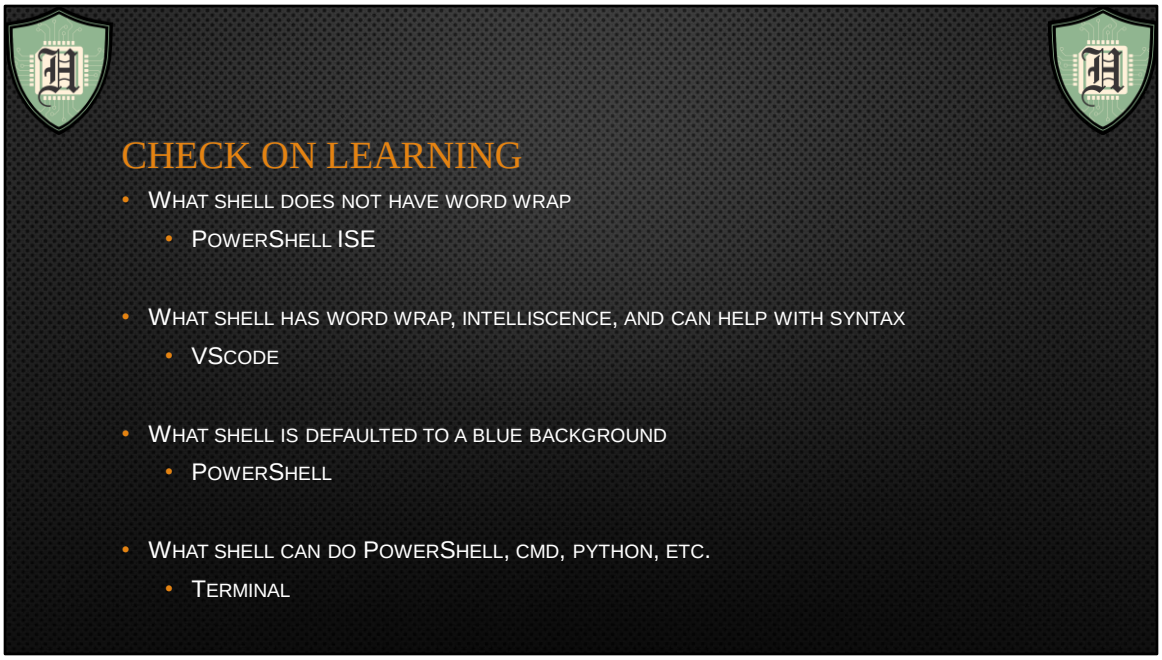
What tools do you use instead of PowerShell? Why

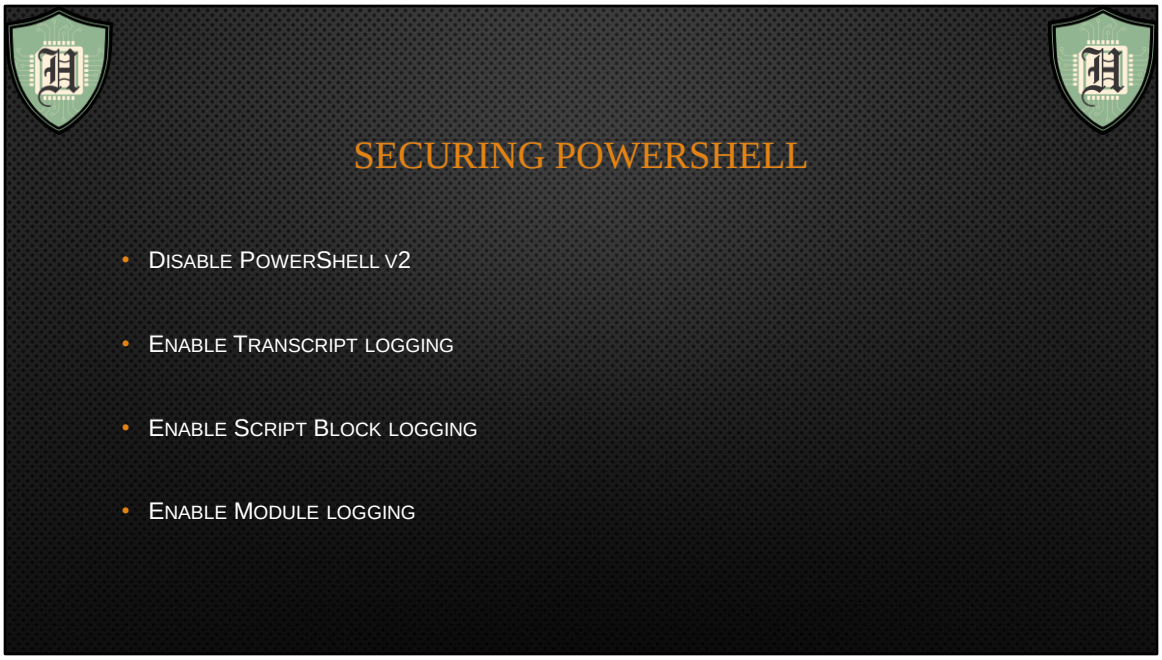

BRIEF HISTORY
Version
Release Date
Product Shipped With
Windows PowerShell v1
2006
Exchange 2007
Windows PowerShell v2
2009
Windows Vista
Windows PowerShell v3
2012
Windows PowerShell v4
2013
Windows PowerShell v5
2016
Window 10
Powershell v6
2018
Powershell v7
2020
Jones, D. (2020). Shell of an Idea: The untold history of PowerShell. Lean Publishing.



What is your go to IDE/Terminal for PowerShell? Why?

What feature did you learn from this segment.

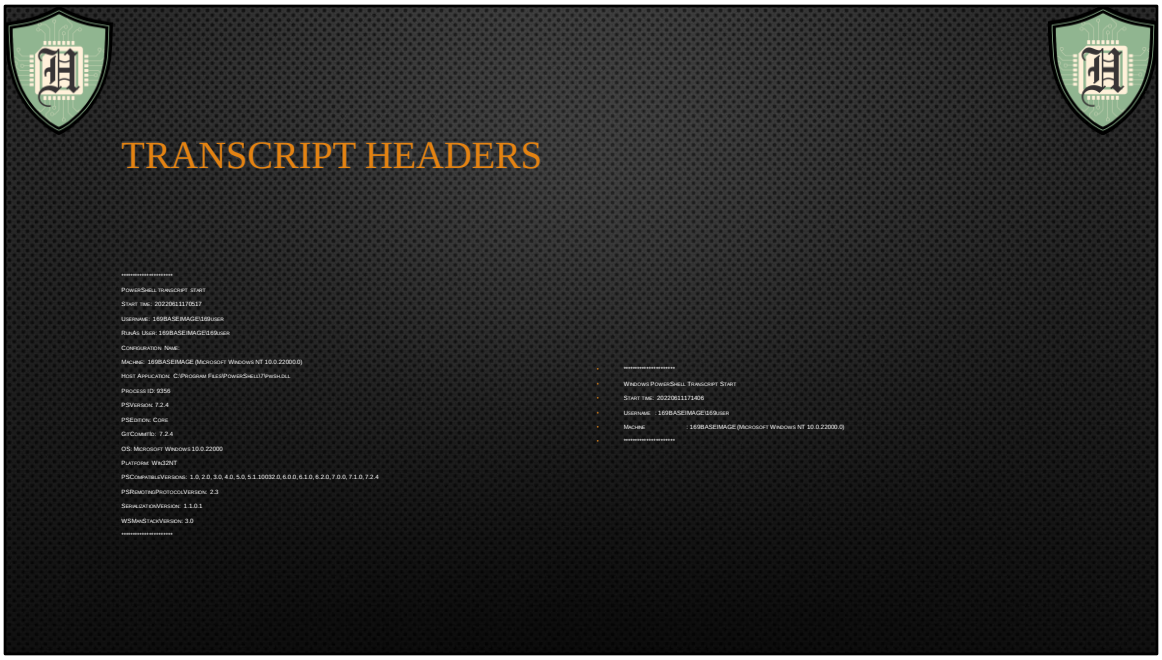

CHECK ON LEARNING
• What shell does not have word wrap
• PowerShell ISE
• What shell has word wrap, intelliscence, and can help with syntax
• VScode
• What shell is defaulted to a blue background
• PowerShell
• What shell can do PowerShell, cmd, python, etc.
• Terminal


SECURING POWERSHELL
• Disable PowerShell v2
• Enable Transcript logging
• Enable Script Block logging
• Enable Module logging


DISABLE POWERSHELL V2
• Default on Win 7, Win 8 and early Win10
• Deprecated in 2017
• PowerShell v5 can be downgraded to v2
• No logging
• PowerShell v5 is new default
• Has transcript logging (v3)
• Has script block logging (v5)
• Has event logging
• Remoting can be secured (v3)

Demo

PowerShell.exe -Version 2



powershell.exe -version 2

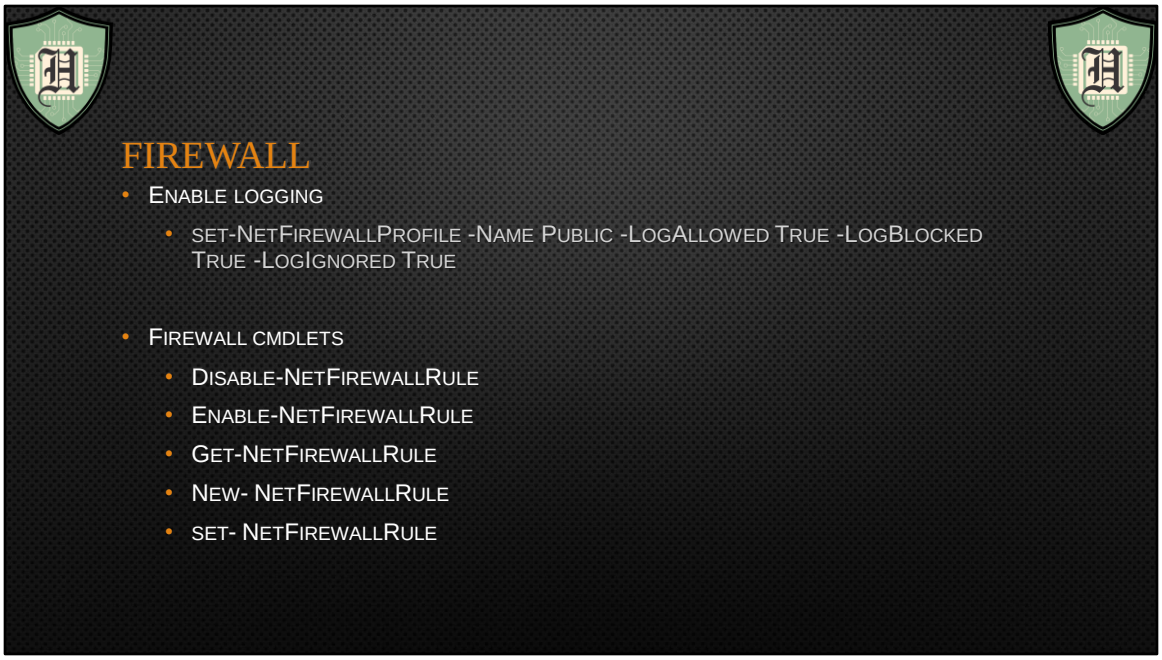
Get-childItem HKLM:\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\ -does not exist

New-Item HKLM:\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\ -Force
Set-ItemProperty HKLM:\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\ -name EnableScriptBlockLogging -Value 1

Get-Item HKLM:\SOFTWARE\WOW6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging\
Get-WinEvent -LogName Microsoft-Windows-Powershell/Operational | where {$_.id -eq 4104}

https://devblogs.microsoft.com/powershell/powershell-the-blue-team/

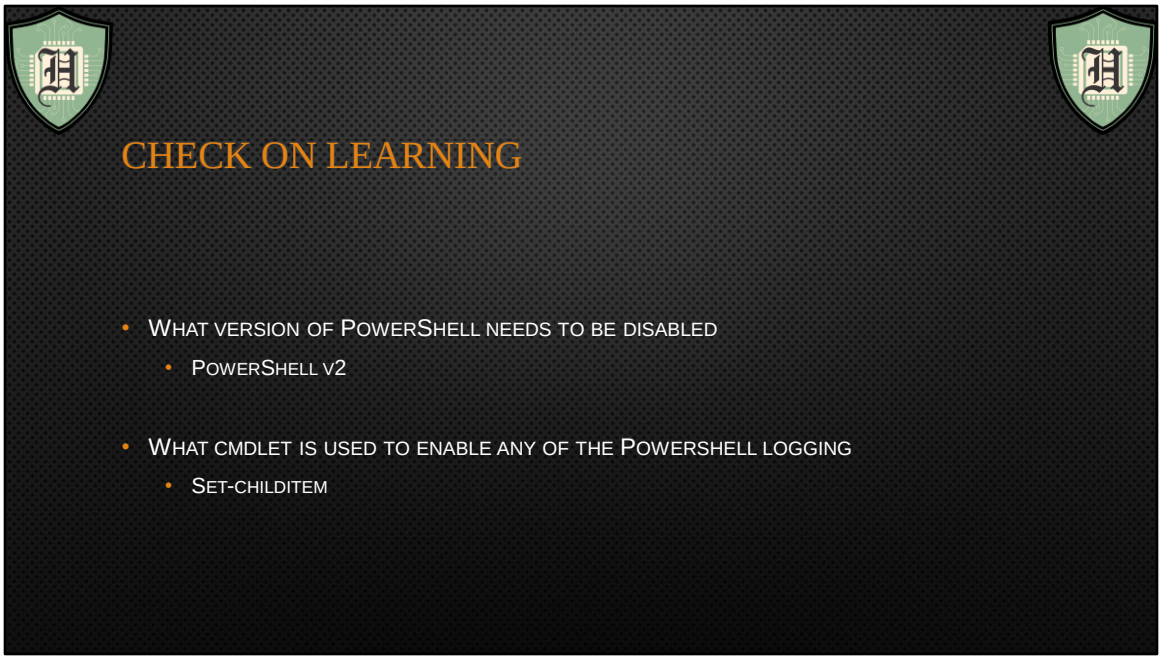

ENABLE MODULE LOGGING
• If you enable this policy setting and specify one or more modules, pipeline execution events for the specified modules are recorded in the Windows PowerShell log in Event Viewer.
• Import-Module <Module-Name>
• (Get-Module <Module-Name>).LogPipelineExecutionDetails = $true
• HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ModuleLogging → EnableModuleLogging = 1
• HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ModuleLogging\ModuleNames → * = *

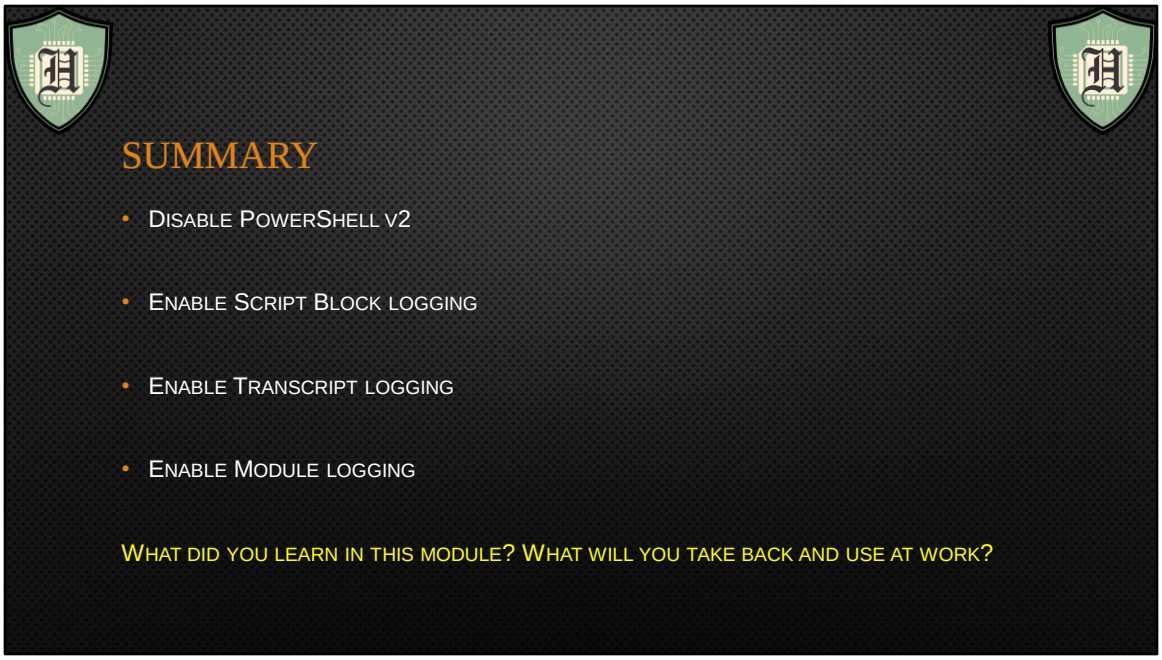


https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_non-windows?view=powershell-7

https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/secedit
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/administer-security-policy-settings#bkmk-scmtool

https://docs.microsoft.com/en-us/powershell/module/netsecurity/new-netfirewallrule?view=windowsserver2022-ps


CHECK ON LEARNING
• What version of PowerShell needs to be disabled
• PowerShell v2
• What cmdlet is used to enable any of the Powershell logging
• Set-childitem


SUMMARY
• Disable PowerShell v2
• Enable Script Block logging
• Enable Transcript logging
• Enable Module logging
What did you learn in this module? What will you take back and use at work?

ELO 4 – PARSING WINDOWS LOGS

Action: Learner will demonstrate using PowerShell to parse logs

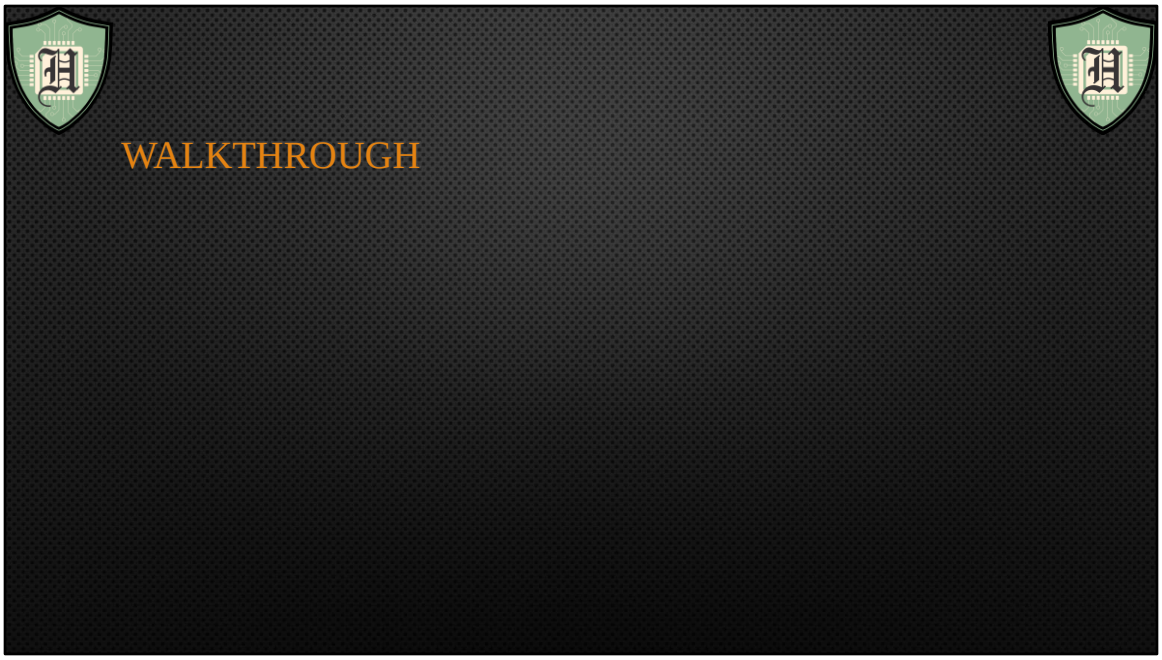
Condition: Given learning activities, readings, peer and instructor feedback, reflection time, development time, and practical exercises

Standard: Given a IOC, learner will use PowerShell to parse Windows evtx logs to locate the IOC


GET-WINEVENT VS. GET-EVENTLOG
GET-EVENTLOG
MICROSOFT.POWERSHELL.MANAGEMENT
POWERSHELL 2 - 5.1
[-NEWEST <INT32>]
[-AFTER <DATETIME>]
[-BEFORE <DATETIME>]
[-MESSAGE <STRING>]
USES A WIN32 API THAT IS DEPRECATED
GET-WINEVENT
MICROSOFT.POWERSHELL.DIAGNOSTICS
POWERSHELL 5.1 – CURRENT
[-FILTERXPATH <STRING>]
[-OLDEST]
GETS EVENT AND CLASSIC LOGS


```
Get-WinEvent -LogName Security | Where-Object {$_.id -eq "4672"} | select
@{name="MyTime";
expression={(($_.TimeCreated).ToUniversalTime()).tostring("MM/dd/yyyy
HH:mm:ss")}}, ID, LevelDisplayName, Message | select -First 150
```

```
Get-WinEvent -LogName System | Where-Object {$_.id -eq "7045"} | Select-Object -
ExpandProperty Message | Group-object | Select-Object -ExpandProperty Group
```


WALKTHROUGH

•https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.diagnostics/get-winevent?view=powershell-7.2#example-16-filter-event-log-results

•Finally did an XML Filter:
•<QueryList> <Query Id="0" Path="Security"> <Select Path="Security">*[System[(EventID=4624)]] and *[EventData[Data[@Name='IpAddress'] and (Data='172.16.12.3')]] and *[EventData[Data[@Name='IpPort'] and (Data=56842 or Data=65499 or Data=65497 or Data=50726)]]</Select> </Query> </QueryList>

CHECK ON LEARNING

- GET NUMBER OF CLEARED LOGS
- WHAT IP DID SAMIR LOGIN FROM
- WHAT WAS THE NAME OF THEIR WORKSTATION

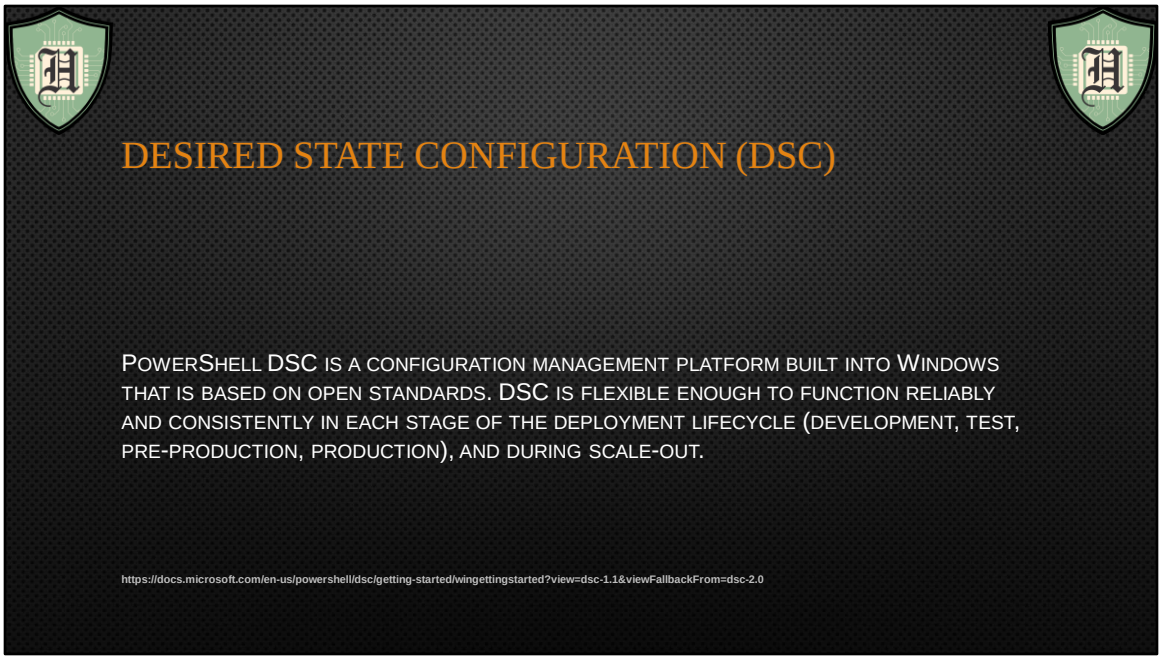
ELO 5 SUMMARY

Action: Learner will demonstrate using PowerShell to parse logs

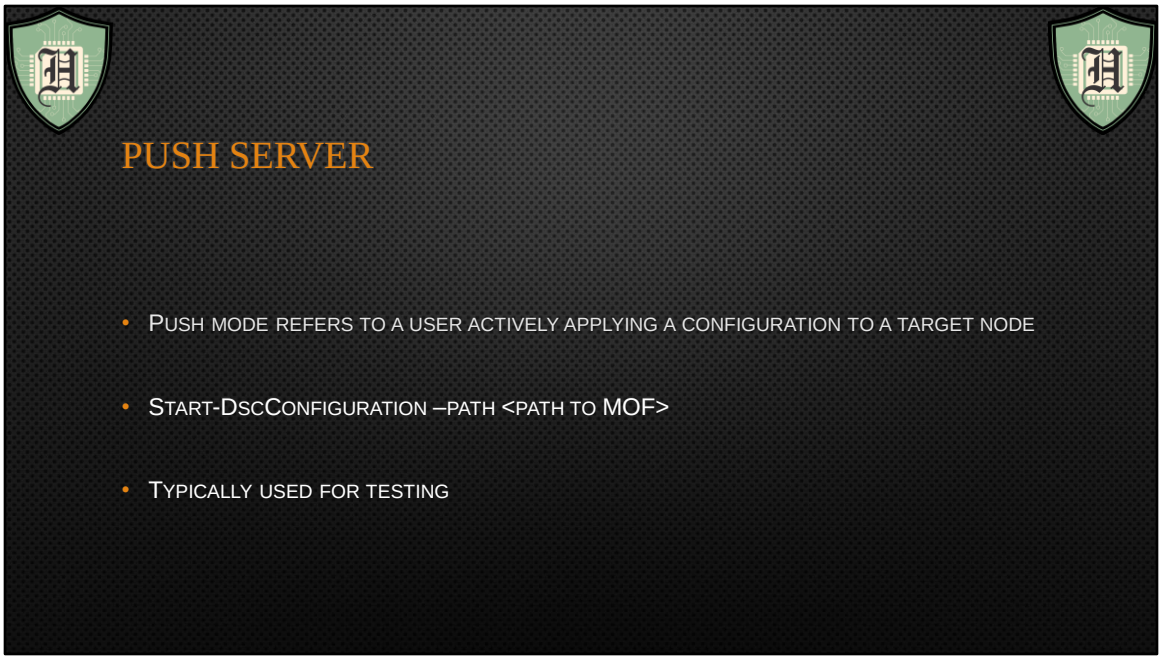
Condition: Given learning activities, readings, peer and instructor feedback, reflection time, development time, and practical exercises

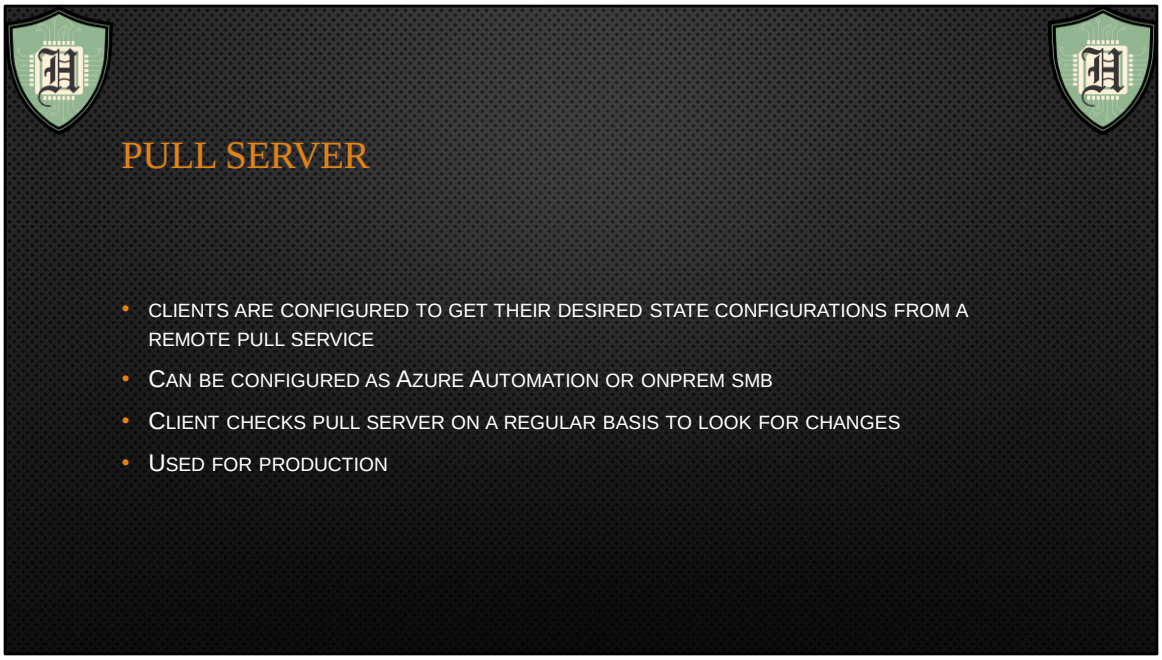
Standard: Given a IOC, learner will use PowerShell to parse Windows evtx logs to locate the IOC


DESIRED STATE CONFIGURATION OVERVIEW
• What is DSC
• DSC Components
• DSC Congiguration File
• Local Configuation Manager


DESIRED STATE CONFIGURATION (DSC)
POWERSHELL DSC IS A CONFIGURATION MANAGEMENT PLATFORM BUILT INTO WINDOWS THAT IS BASED ON OPEN STANDARDS. DSC IS FLEXIBLE ENOUGH TO FUNCTION RELIABLY AND CONSISTENTLY IN EACH STAGE OF THE DEPLOYMENT LIFECYCLE (DEVELOPMENT, TEST, PRE-PRODUCTION, PRODUCTION), AND DURING SCALE-OUT.
https://docs.microsoft.com/en-us/powershell/dsc/getting-started/wingettingstarted?view=dsc-1.1&viewFallbackFrom=dsc-2.0

Install-Module 'PSDesiredStateConfiguration' -Verbose


PUSH SERVER
• PUSH MODE REFERS TO A USER ACTIVELY APPLYING A CONFIGURATION TO A TARGET NODE
• START-DSCCONFIGURATION –PATH <PATH TO MOF>
• TYPICALLY USED FOR TESTING

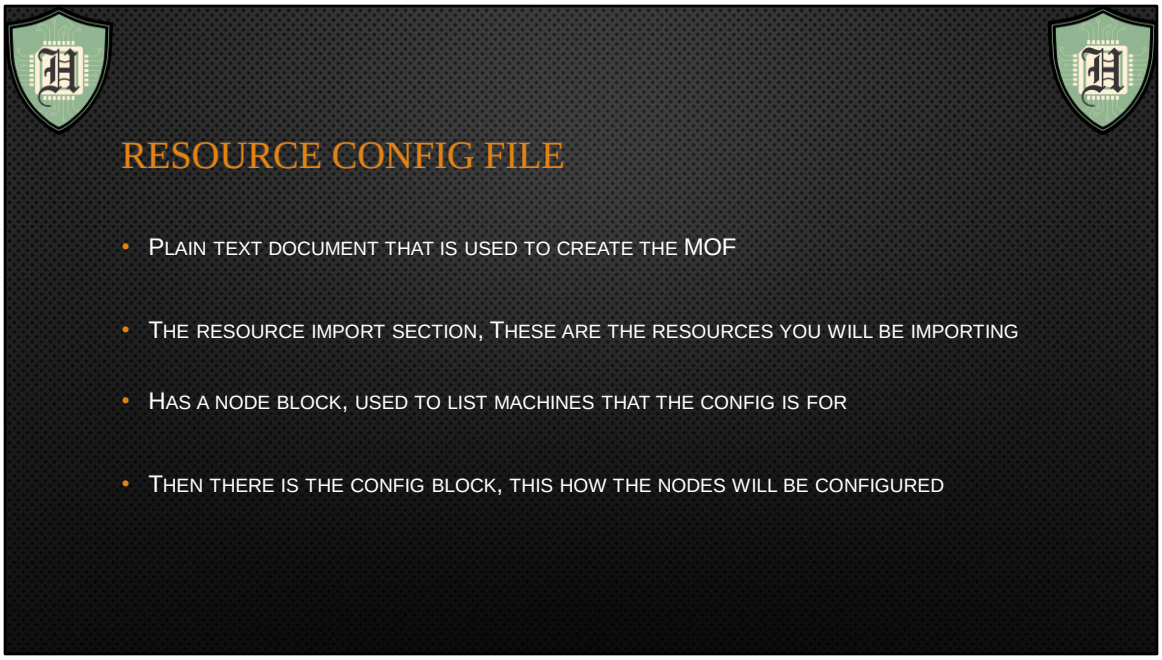


https://docs.microsoft.com/en-us/powershell/dsc/managing-nodes/metaconfig?view=dsc-1.1
https://docs.microsoft.com/en-us/powershell/dsc/pull-server/enactingconfigurations?view=dsc-1.1

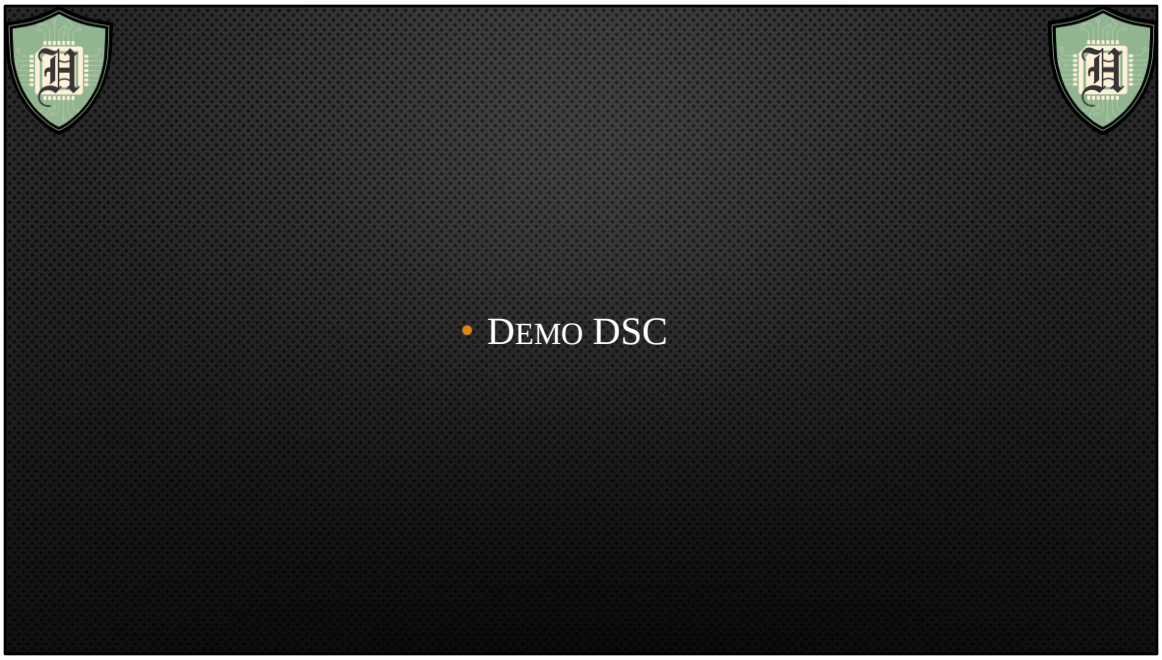
MANAGED OBJECT FORMAT (MOF)

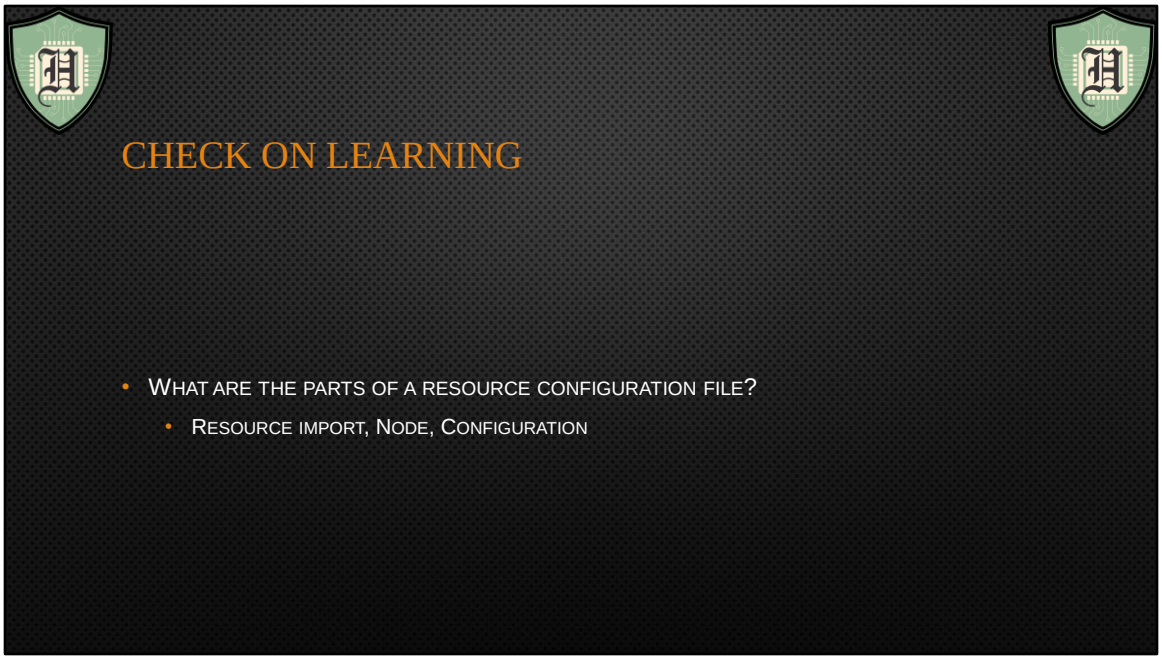
- THE LANGUAGE USED TO DESCRIBE COMMON INFORMATION MODEL (CIM) CLASSES.
- THE ACTUAL FILE THAT CONFIGURES THE MACHINES
- COMPILED BY THE RESOURCE CONFIG FILE


LOCAL CONFIGURATION MANAGER (LCM)
• LCM IS THE SERVICE THAT MANAGE DSC ON THE LOCAL MACHINE
• GET-DSCCONFIGURATION
• GET-DSCLOCALCONFIGURATIONMANAGER
• REMOVE-DSCCONFIGURATIONDOCUMENT -STAGE CURRENT –VERBOSE
• SET-DSCLOCALCONFIGURATIONMANAGER -PATH 'C:\METACONFIG\LOCALHOST.META.MOF' -VERBOSE



Get-DscResource -Module * | select Module | group Module


DEMO DSC


CHECK ON LEARNING
• What are the parts of a resource configuration file?
• Resource import, Node, Configuration

DSC SUMMARY

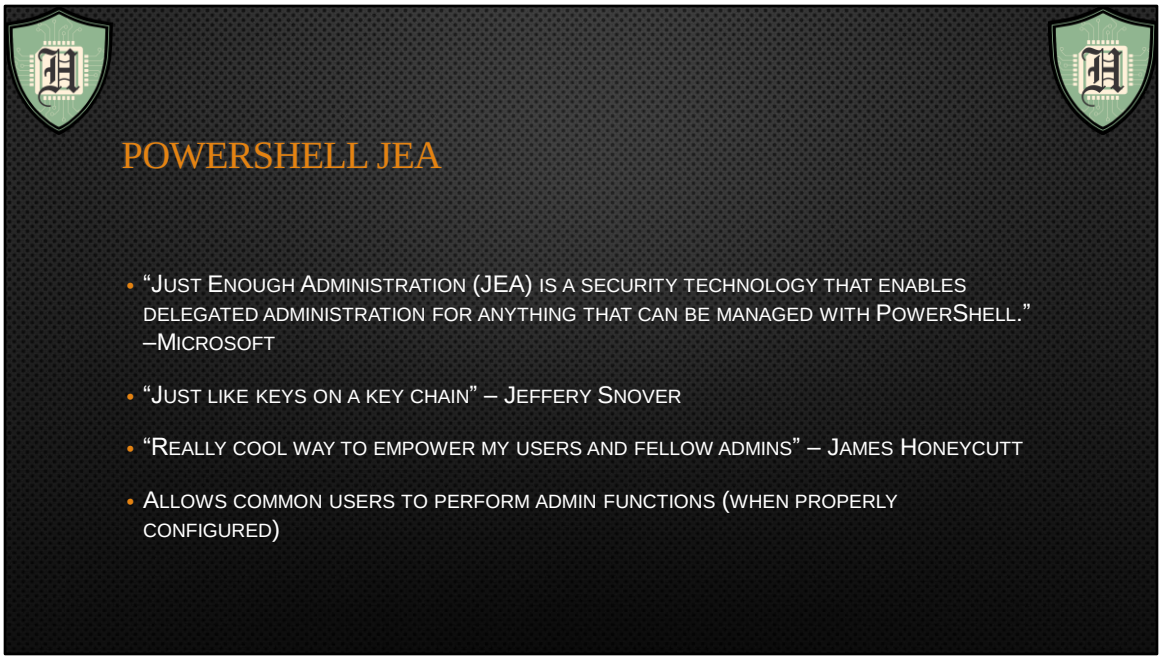
- What is DSC
- DSC Components
- DSC Congiguration File
- Local Configuation Manager

ENABLING LEARNING OBJECTIVE / LEARNING STEP ACTIVITY 4 (ELO/LSA 4)

ACTION: LEARNER WILL DESCRIBE THE PROCESS OF USING POWERSHELL JEA

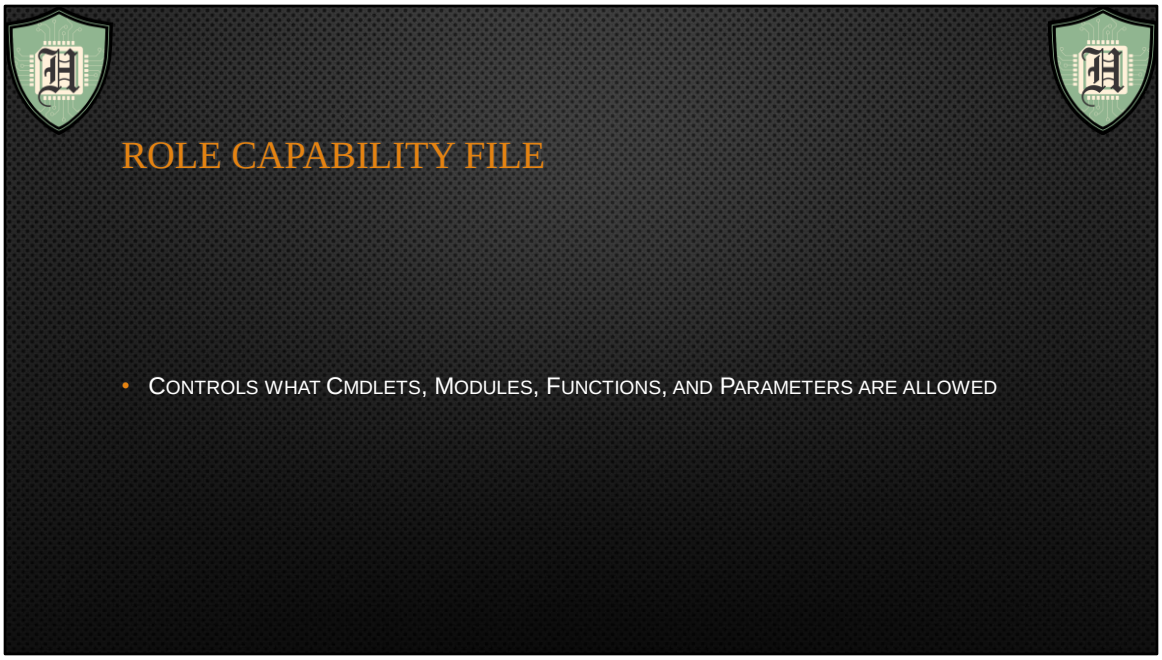
CONDITION: GIVEN LEARNING ACTIVITIES, READINGS, PEER AND INSTRUCTOR FEEDBACK, REFLECTION TIME, DEVELOPMENT TIME, AND PRACTICAL EXERCISES

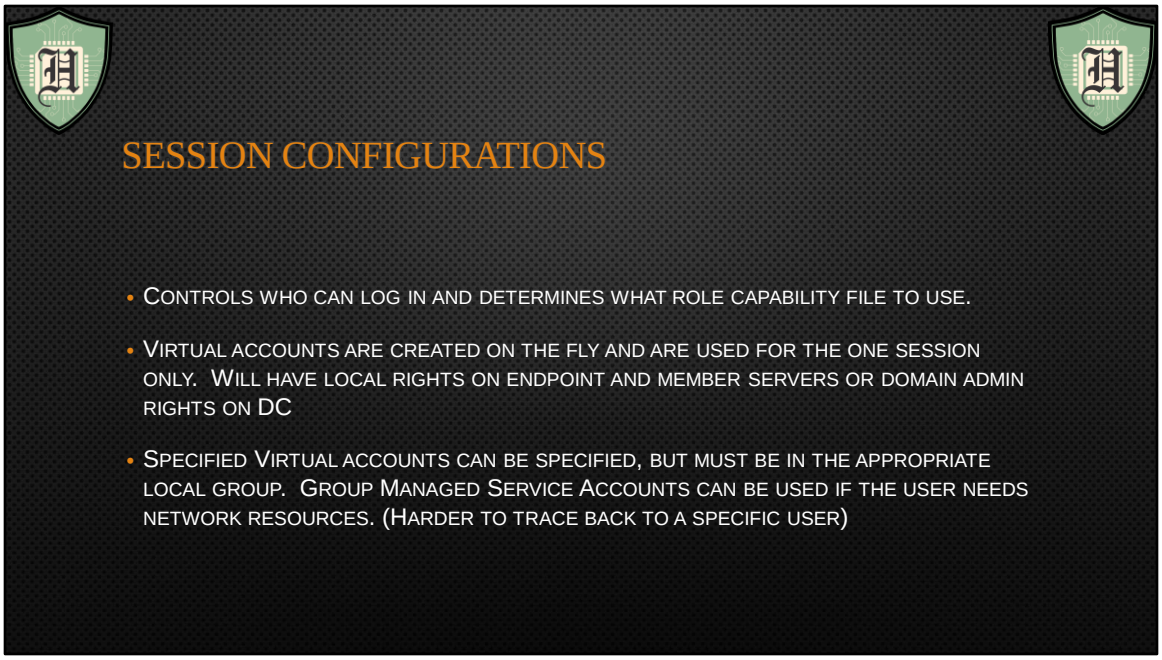
STANDARD: LEARNER WILL LIST THE STEPS NEED TO CONFIGURE POWERSHELL JEA


POWERSHELL JEA
• "Just Enough Administration (JEA) is a security technology that enables delegated administration for anything that can be managed with PowerShell." –Microsoft
• "Just like keys on a key chain" – Jeffery Snover
• "Really cool way to empower my users and fellow admins" – James Honeycutt
• Allows common users to perform admin functions (when properly configured)

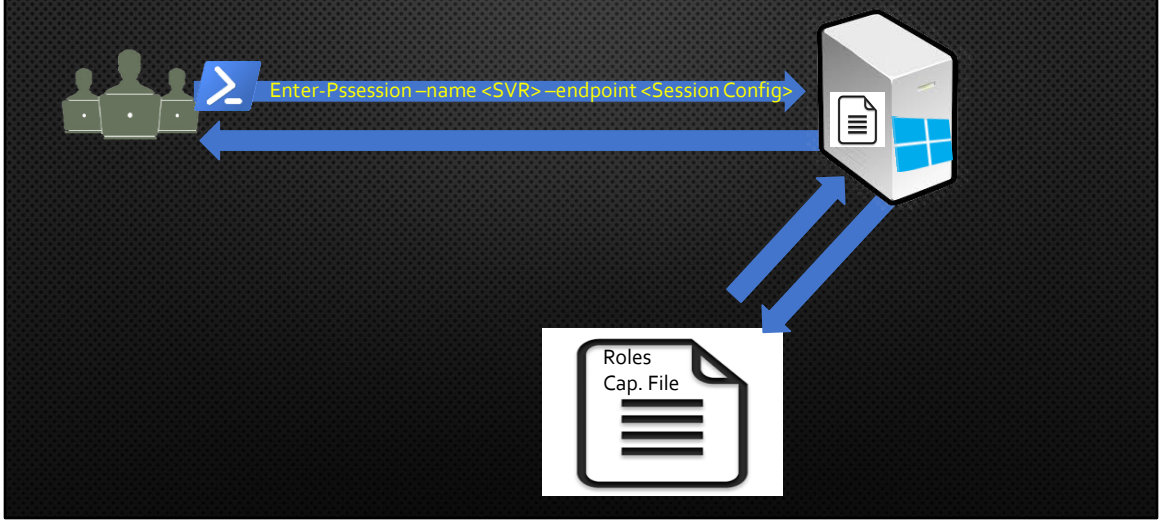
HOW DOES IT WORK

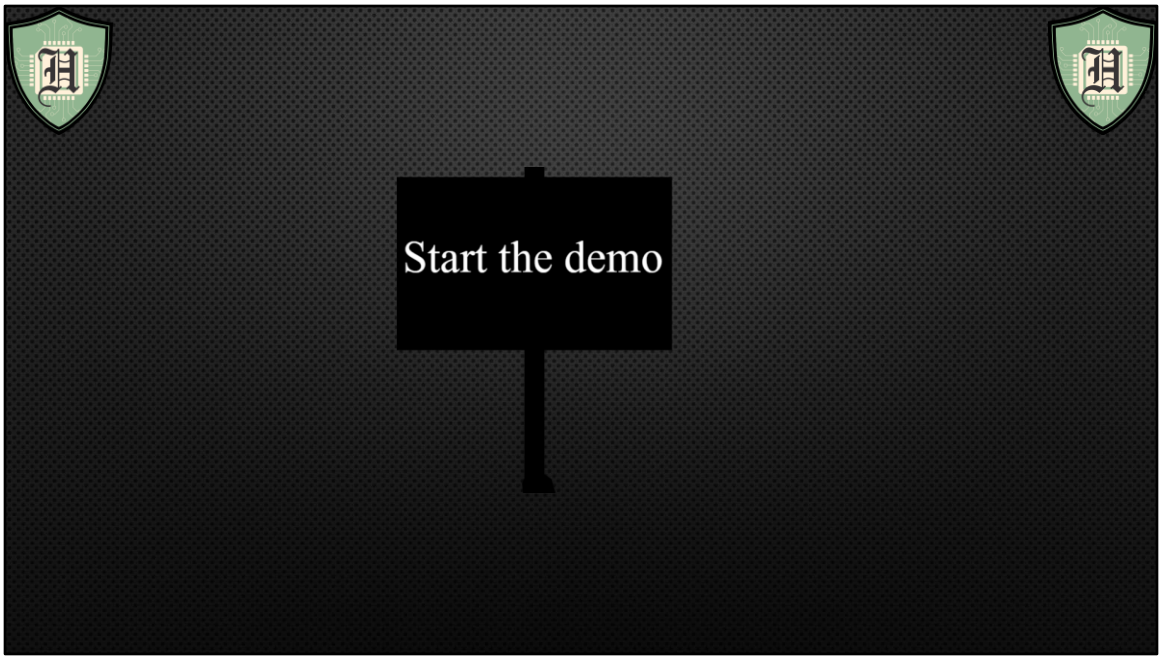
- User/Admin uses PowerShell remoting to access remote server using the Session configuration file and using "Runas"
- A virtual Admin account is created and used during THIS SESSION ONLY
- The virtual admin technically has access to all cmdlets, but only shows the user what they are entitled to, based on the Role Capabilities File
- User does what they need to, exits remote pssession

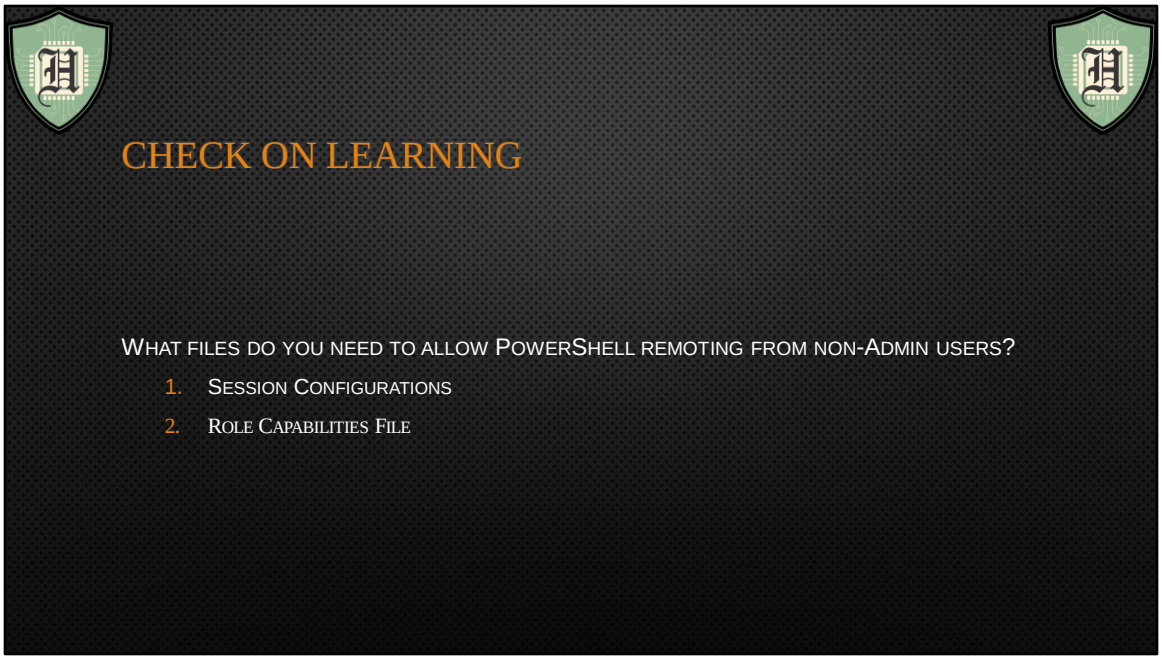

ROLE CAPABILITY FILE
• Controls what Cmdlets, Modules, Functions, and Parameters are allowed

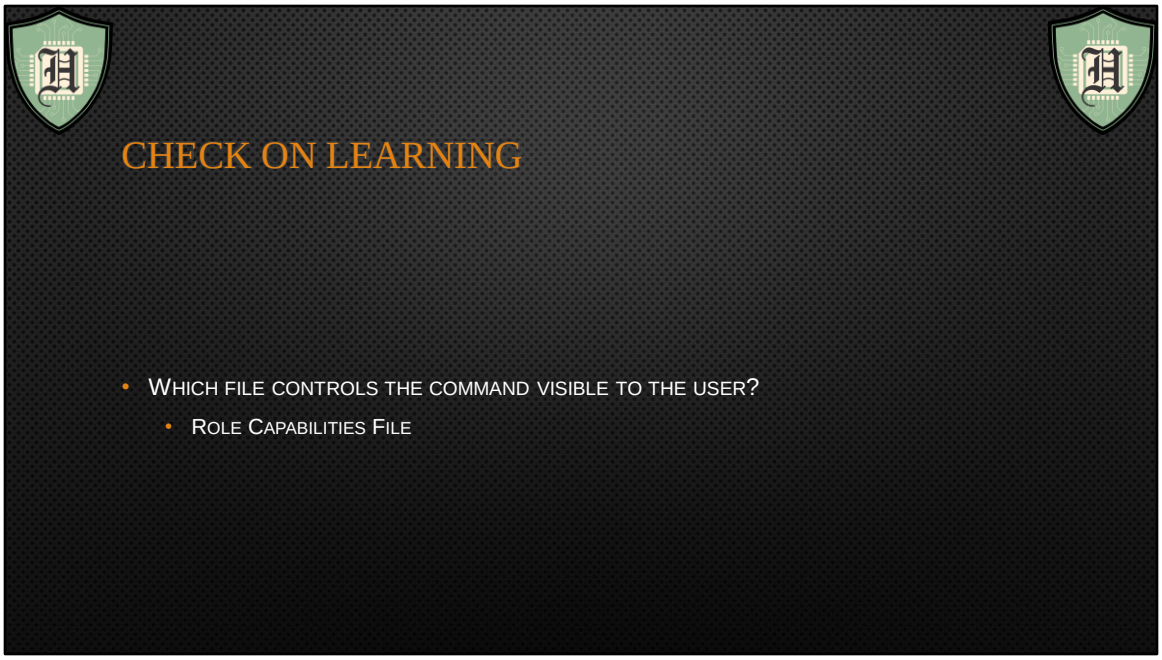

SESSION CONFIGURATIONS
• Controls who can log in and determines what role capability file to use.
• Virtual accounts are created on the fly and are used for the one session only. Will have local rights on endpoint and member servers or domain admin rights on DC
• Specified Virtual accounts can be specified, 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)

HOW IT WORKS


Enter-Pssession –name <SVR> –endpoint <Session Config>
Roles
Cap. File


Start the demo


CHECK ON LEARNING
WHAT FILES DO YOU NEED TO ALLOW POWERSHELL REMOTING FROM NON-ADMIN USERS?
1. SESSION CONFIGURATIONS
2. ROLE CAPABILITIES FILE


CHECK ON LEARNING
• WHICH FILE CONTROLS THE COMMAND VISIBLE TO THE USER?
• ROLE CAPABILITIES FILE

CHECK ON LEARNING

- WHICH FILE CONTROLS THE SESSION AND CREATES THE VIRTUAL ACCOUNTS?
  1. SESSION CONFIGURATION FILE

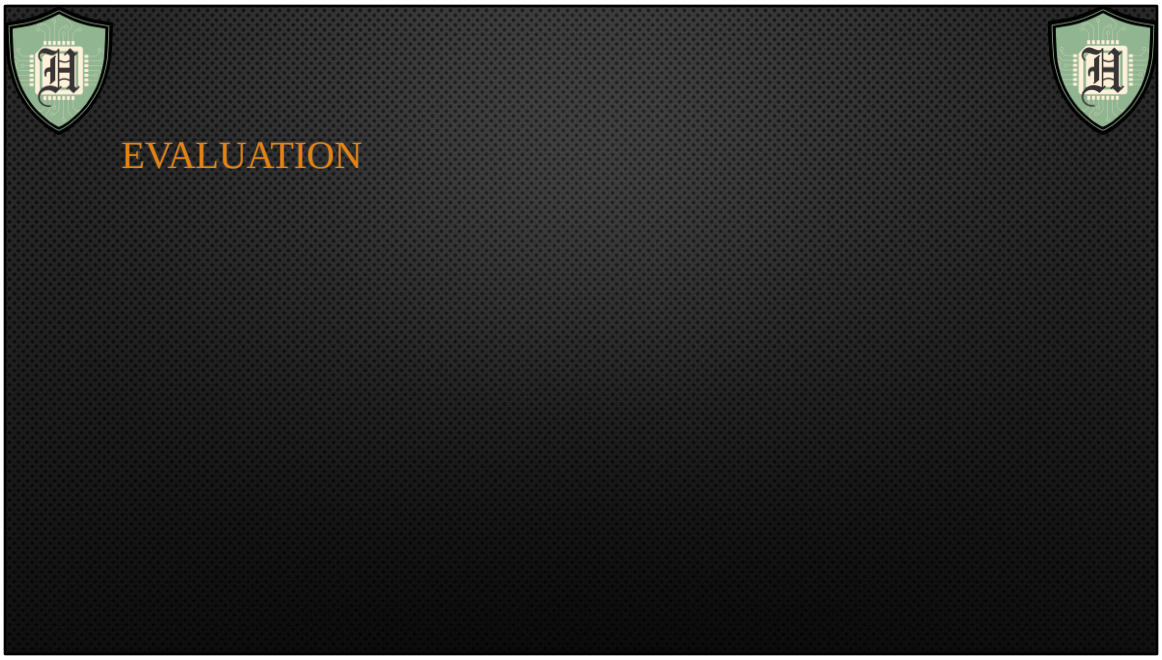
ELO 4 SUMMARY

Action: Learner will describe the process of using PowerShell JEA

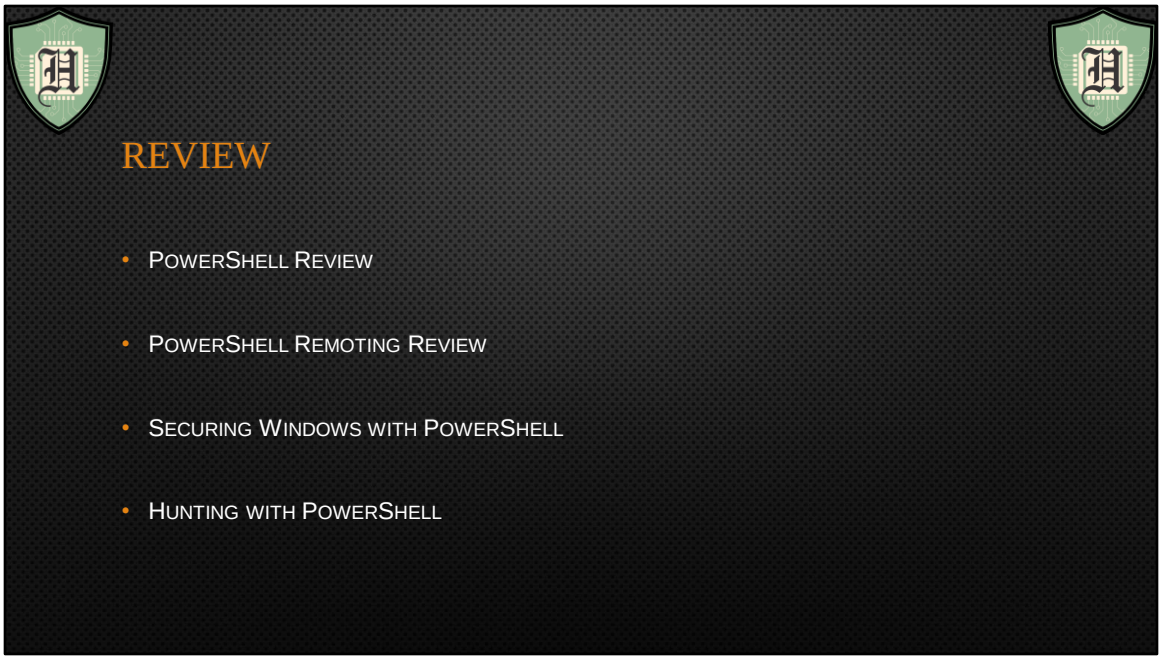
Condition: Given learning activities, readings, peer and instructor feedback, reflection time, development time, and practical exercises

Standard: Learner will list the steps need to configure PowerShell JEA

Is this something you can start using today? If so how will you use it?


EVALUATION

OVERALL CHECK ON LEARNING:


REVIEW
• PowerShell Review
• PowerShell Remoting Review
• Securing Windows with PowerShell
• Hunting with PowerShell


Any
Questions