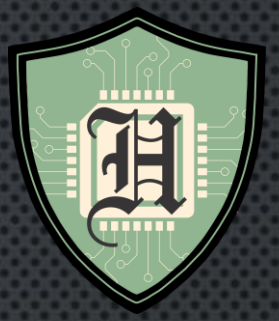
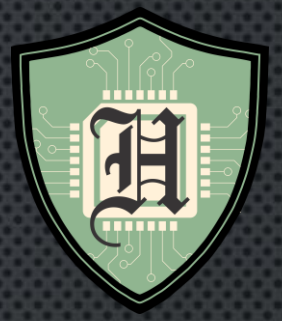
POWERSHELL CRASH COURSE

PRESENTED BY: JAMES HONEYCUTT



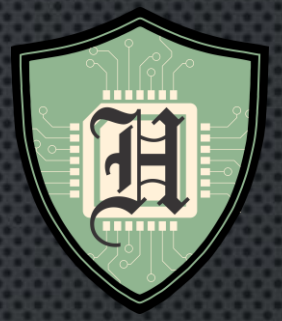
Remote PowerShell

- -ComputerName
- Remote PowerShell
  - Similar to Telent and SSH
  - Uses WS-Man protocol (Web Services for Management)
  - WinRM is MS implementation of WS-MAN
  - Must configure WinRM on machines that will receive remote PS connections
  - XML format of object is sent back to originating machine



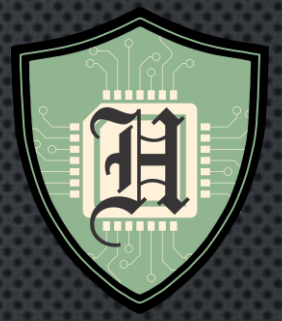
ENTER-PSSESSION

- Type commands directly on connected server
- Must use real name. By default it will not let you use IP or other DNS alias
- Profile scripts don't carry over
- Execution policy still exists
- Exit-PSSession ends the session
  - Closing the terminal ends the session
  - Avoid remote chains



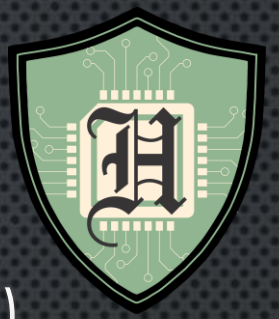
INVOKE-COMMAND

- One-to-many
- PowerShell talks to up to 32 computers at once
- Can use -throttle to talk to more than 32
- -command is alias for –scriptblock
- To use a list of compuers use:
  - get-content computers.txt
  - get-adcomuters
  - -computername



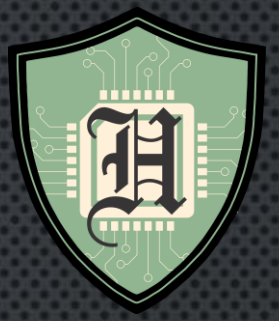
INVOKE-COMMAND vs. COMPUTERNAME

- ComputerName
  - computers are contacted sequentially and could take longer
  - does not contain a PSComputerName property so results my be hard to separate
  - connection is not made with WinRM
  - Processing is done on local computer; so all records are brought across the wire then filtered
  - Results are live and don't need to be serialized or deserialized (fully functional Objects)



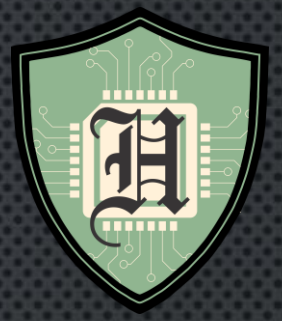
INVOKE-COMMAND VS. COMPUTERNAME (CONT.)

- Invoke-command
  - Computers are contacted in parallel; command could run more quickly
  - Output contains a PSComputerName property so results are more distinguishable
  - Is used over WinRM; so firewall rules can be enabled
  - Queries and filters on remote computer then results are sent back to local machine
  - Results need to be serialized and deserialized before and after transmitting over the wire (snapshot results) (limited objects)



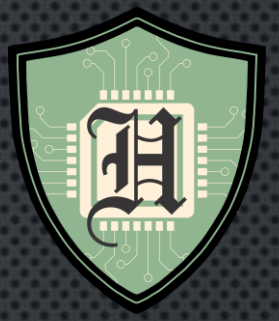
SESSIONS

- New-PSSession
  - Can be used to connect to several machines and stored as a variable
- Disconnect-PSSession
- Connect-PSSession
- Remove-PSSession
- Enter-PSSession –session
- Invoke-command –session



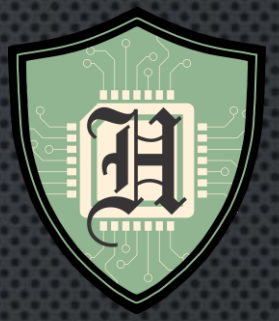
REMOTING WITH SSH

- THE WINDOWS MACHINE MUST HAVE BOTH SSH CLIENT AND SERVER INSTALLED.
- CONFIGURATION CHANGES NEED DONE TO SSH_CONFIG ON BOTH WINDOWS AND LINUX
- [-HOSTNAME <STRING>] [-USERNAME <STRING>] [-KEYFILEPATH <STRING>]



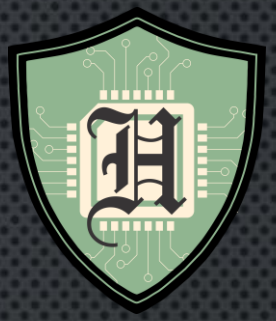
IMPLICIT REMOTING: IMPORTING A SESSION

- $SESSION = NEW-PSSESSION -COMP SERVER-R2
  - ESTABLISH A REMOTE CONNECTION TO SERVER WITH ADTOOLS INSTALLED
- INVOKE-COMMAND -COMMAND { IMPORT-MODULE ACTIVEDIRECTORY } SESSION $SESSION
  - TELL THE REMOTE COMPUTER TO LOAD THE AD MODULE
- IMPORT-PSSESSION -SESSION $SESSION -MODULE ACTIVEDIRECTORY -PREFIX REM
  - IMPORT THE AD POWERSHELL MODULE AND PREFIX THE COMMANDS WITH REM



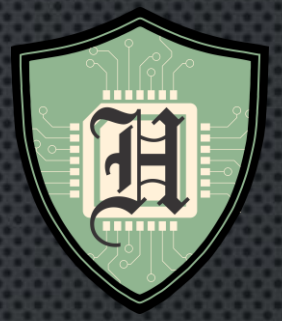
ADVANCED REMOTING CONFIGURATION

- USES CUSTOM ENDPOINT CONFIGURATIONS
- ENABLE MULTI-HOP REMOTING
- MUTUAL AUTHENTICATION
- MUTUAL AUTHENTICATION VIA SSL
- TRUSTEDHOSTS



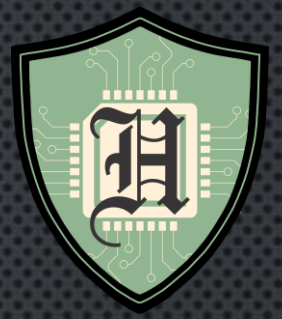
REFERENCES

- https://docs.microsoft.com/en-us/powershell/scripting/learn/windows-powershell-glossary?view=powershell-5.1
- https://docs.microsoft.com/en-us/dotnet/framework/additional-apis/index
- https://docs.microsoft.com/en-us/powershell/scripting/samples/creating-a-custom-input-box?view=powershell-5.1



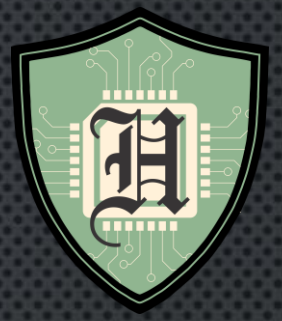
REFERENCES (CONT.)

- https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_commonparameters?view=powershell-6
- https://devblogs.microsoft.com/scripting/using-scheduled-tasks-and-scheduled-jobs-in-powershell/
- https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_language_modes?view=powershell-5.1



POWERSHELL V5 SECURITY REFERENCES

- https://blogs.msdn.microsoft.com/daviddasneves/2017/05/25/powershell-security-at-enterprise-customers/
- https://www.blackhillsinfosec.com/powershell-logging-blue-team/
- https://www.stigviewer.com/stig/windows_10/2017-02-21/finding/V-68819
- https://www.stigviewer.com/stig/windows_server_20122012_r2_member_server/2018-10-30/finding/V-80475



QUESTIONS

- Upcoming Talks/Training
  - PowerShell Crash course
    - BSidesCharm - (April 30)
    - ISSA Central Maryland (June 04)
  - Defensive PowerShell
    - ISSA Central Maryland (June 18)
- LinkedIn
  - in/james-Honeycutt
- Twitter
  - @P0w3rChi3f
- Website
  - JamesHoneycutt.net