PowerShell

Before we start

- Run powershell_ise.exe (Does your screen look like mine)
- Or run get-host
- Download PowerShell version 5
- * Optional - Download and install Microsoft PowerBI

Course Summary

- Basics
- Piping Commands
- Objects
- Variables
- Arrays
- Foreach and If
- Functions
- Modules
- APIs
- Cybershield tips / conclusion
- PowerShell Challenge

Introductions

#NAME

#JOB

#LOCATION

#POWERSHELL EXPERIENCE, SCRIPTING EXPERIENCE

PowerShell

Kung Fu for Windows

What is PowerShell?

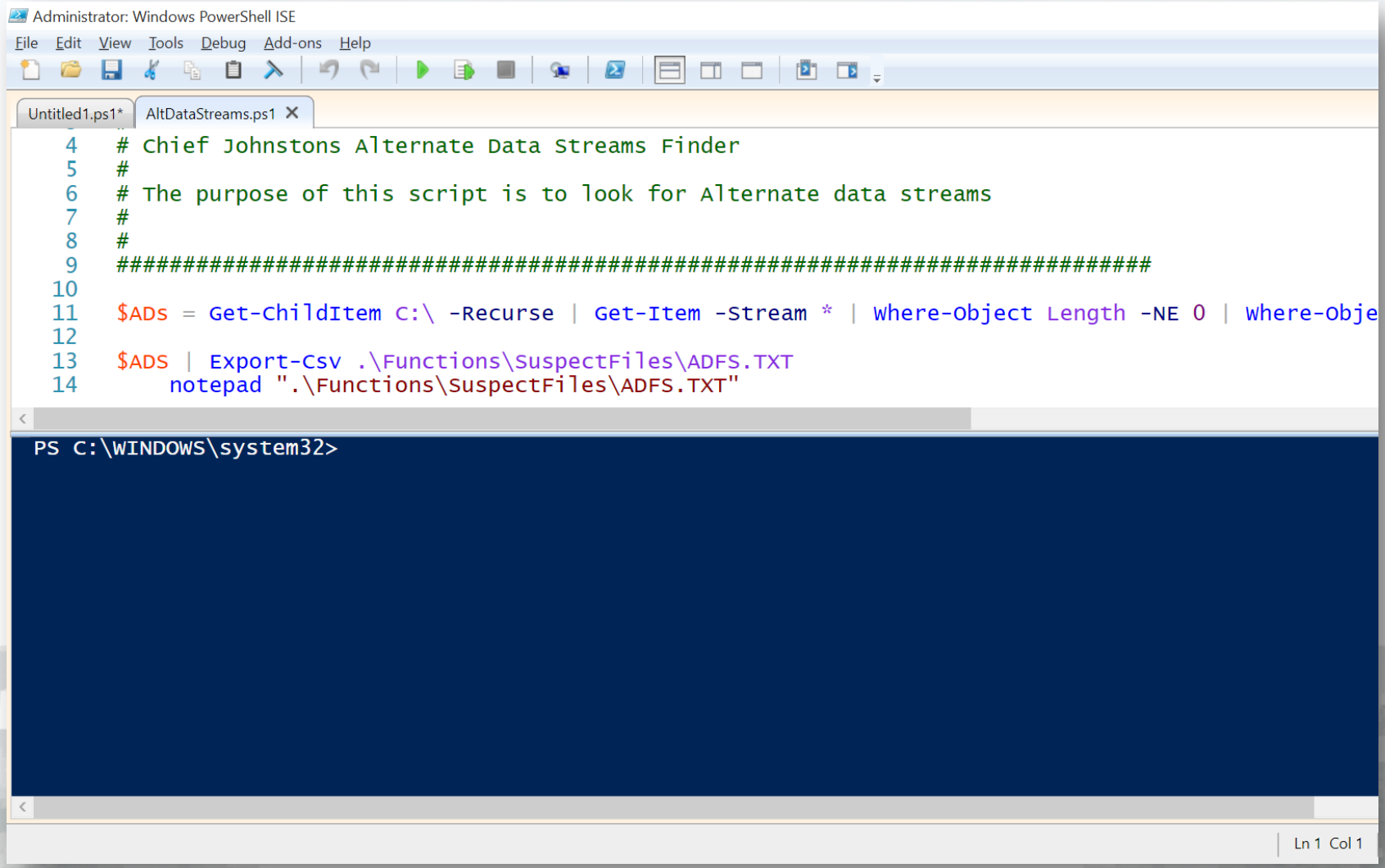
- MICROSOFT DEFINITION OF POWERSHELL
  - Windows PowerShell® is a task-based command-line shell and **scripting language** designed especially for **system administration.** Built on the **.NET Framework**, Windows PowerShell helps IT professionals and power users control and automate the administration of the Windows operating system and applications that run on Windows.

PowerShell

Administrator: Windows PowerShell

```
PS C:\WINDOWS\system32> ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 3:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c9ea:a2dd:501a:59dd%11
   IPv4 Address. . . . . . . . . . . : 192.168.121.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8984:90ac:c92a:2e0d%10
   IPv4 Address. . . . . . . . . . . : 192.168.3.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::d899:8449:18e5:1f6b%9
```

Power ISE

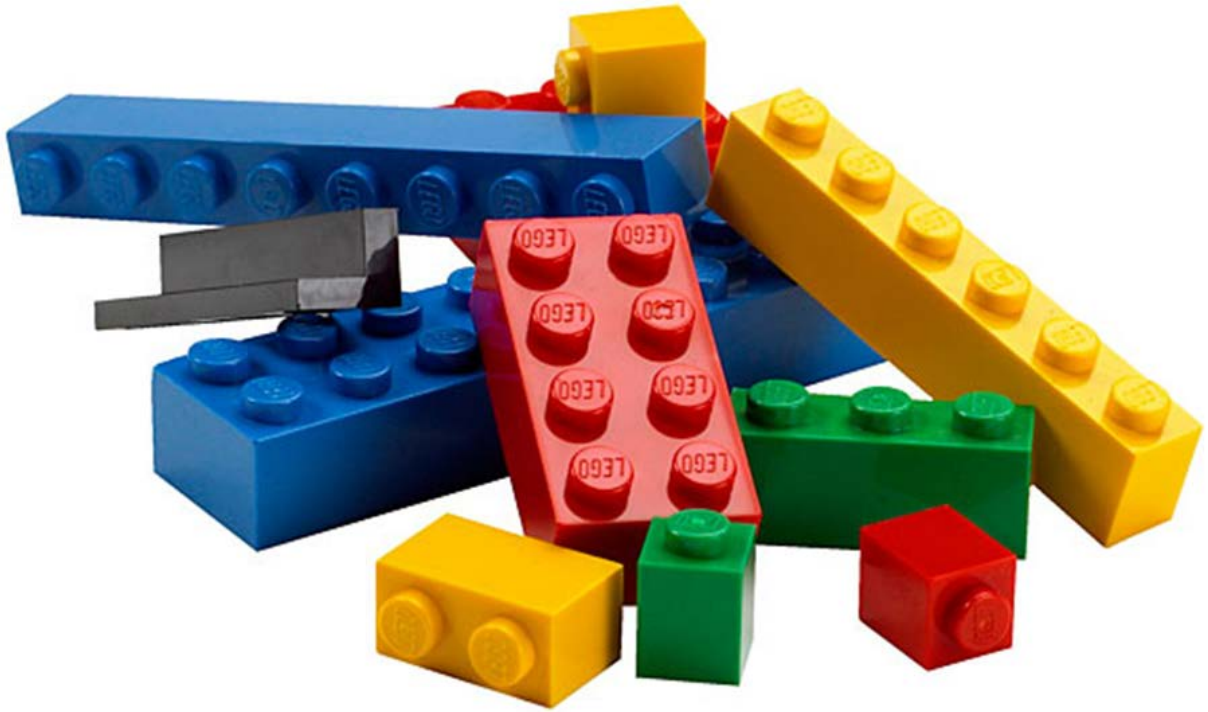

Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1*
AltDataStreams.ps1
4 # Chief Johnstons Alternate Data Streams Finder
5 #
6 # The purpose of this script is to look for Alternate data streams
7 #
8 #
9 ##
10
11 $ADs = Get-ChildItem C:\ -Recurse | Get-Item -Stream * | Where-Object Length -NE 0 | Where-Obje
12
13 $ADS | Export-Csv .\Functions\SuspectFiles\ADFS.TXT
14 notepad ".\Functions\SuspectFiles\ADFS.TXT"
PS C:\WINDOWS\system32>
Ln 1 Col 1

The CMD line problem?

dir, copy

The PowerShell Way

COLORADO ARMY NATIONAL GUARD
INFORMATION MANAGEMENT



Think like PowerShell

VERB-NOUN

GET-ITEM
SET-ITEM
IMPORT-CSV

PE1 – Basic Commands

```
Get-ChildItem .\ -Recurse
get-item -Path
HKLM:\SOFTWARE\Microsoft\Windows\Curr
entVersion\Run

Get-ItemProperty -Path
C:\Windows\System32\cmd.exe
Get-Service
Get-Process
get-nettcpconnections
show-command
```

Power of the Pipe

- COMMAND | COMMAND | COMMAND
- Get, Where, Select, Set
- Import, get, set, export
- Import, foreach

PE2 – Piping commands

```
Get-ChildItem C:\Windows\System32\cmd.exe |
Get-FileHash -Algorithm SHA256

Get-process | where-object ID –eq 4 |
select-object Name

Get-childitem c:\ -recurse | where-object
extension –eq .exe

Get-service | export-csv –path
c:\services.csv
```

How would you get a list of software installed? and then export it to a CSV?

Objects

- What is an object
- Properties of an object (Get-Member)
- Select-Object
- Where-Object

PE3 – Filtering Objects

- Get a list of files in your system that are larger than 25MB, select only the File Name and Path
- **Try it first before opening the PE3 file**
- hint… Get-childitem, get-member, where-object, select-object

Variables

- What are variables
- Setting and storing a variable
- What type of variable
- Import-variables from other data sources

Types of variables

```
$test = “123”

$test = 123

[int]$test = “123”

[xml]$test = get-content
d:\pathtoxmlfile
```

PE4 Setting a variable


```
$process = Get-Process
```

```
$env:USERNAME
```

How would you get all Messages in the security event log that contain your username, and then set it to a variable?

Arrays and Hash Tables

- A PowerShell array holds a list of data items. Items are similar objects that can be referenced in an index.

- A hash table, also known as a dictionary or associative array, is a compact data structure that stores one or more key\/value pairs

PE5 Working with an Array


```
$dictionary = import-csv
.\Class\PE5\Dictionary.txt

$dictionary.count
$dictionary[0]
$dictionary[27849]
$dictionary[0..99]
```

Can you reference the last item in your array?

What is the longest word in the dictionary?
Who can say that word?

FOREACH Conditions

- When you have an array of objects that you want to take an action on each object

```
foreach ( $i in $array ) {
execute-command on $i
}
```

PE6 – FOREACH EXAMPLE

GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity

```
$importIP = import-csv .\Class\PE6\JAR-16-20296A.csv

foreach ( $i in $importIP ) {
$i | where-object type -EQ "FQDN" | export-csv .\Class\PE6\FQDN.csv -Append -NoTypeInformation
$i | where-object type -eq "IPV4ADDR" | export-csv .\Class\PE6\IPADDRESS.csv -Append -NoTypeInformation
$i | where-object type -EQ "MD5" | Export-Csv .\Class\PE6\HASH.csv -Append -NoTypeInformation
}
```

IF condition

- If statement will execute an action on an object if it meets the condition

```
if ( $i -eq 5 ) { echo do something
} else { echo do nothing }
```

PE7 – IF COMMAND

How would you extract IP addresses from the Grizzly Step Report?

```
$importIP = import-csv .\Class\PE7\JAR-16-20296A.csv

 foreach ( $i in $importIP ) {
if ( $i.Type -eq "IPV4ADDR" ) {
($i.INDICATOR_VALUE -replace "\[",'') -replace '\]' | Add-Content .\Class\PE7\IPv4.csv }
}
```

Functions & Cmdlets

- What are functions-
- What are Cmdlets
- Importing a function
- REVIEW FUNCTIONS BEFORE YOU RUN THEM!

PE8 – Base64 Decoder

Base64 decoder function

```
function decode-base64 {
### Example Command
# decode-base64 -base64 $string
# decode-base64 -base64 aGVsbG8=
param( [string]$base64 )
[System.Text.Encoding]::UTF8.GetString([Sys
tem.Convert]::FromBase64String("$base64"))
}
```

Modules and CMDLets

- What is a Module
- What can you do with a module
- Get-module
- Import-module

PE9 – Virus Total Module

```
Import-Module .\Class\PE9\VirusTotal.psm1

$MYAPIKEY = “NotARealKey"
$hash = Get-Hash -file
C:\Windows\System32\cmd.exe -hashType MD5
Get-VTReport -VTApiKey $MYAPIKEY -hash
$hash
```

Could you develop your own PowerShell virus scanner using this module?

API

- API – Advanced Programming Interface
- We can use APIs and PowerShell to play with other devices such as, Nessus, Palo Alto, ARIN, IP-API, Cisco ICE, ELK, and many more
- Invoke-restmethod
- All you need is an API key and generally a way to sort through XML data

PE10 – ARIN API

- Open up PE10 and let's take a look at the code
- This is to give you an example of how to use PowerShell to tap into a Web-API

PE11 – Visualize the data

- Open up PowerBI, under the GetData menu, select CSV and then select the file you just generated from PE10.

- Now select the map visualization and start select the fields you want to use to map information

Need to Know!

- Lowest Common Denominator
- Execution Policy
- Executes with errors
- Windows Remote Management

Good Scripting Practices

- Versioning
- WHO/WHAT/WHEN/WHERE/WHY
- Detailed Notes
- TEST, TEST, TEST, TEST, TEST!

Cyber Shield Tips

- Process Hacker >>>
- Check registry startup items
- Check processes running
- Check ScheduledTask
- Look for brand new executables
- Baseline AD groups
- Search through event logs
- Get-nettcpconnections

Great Resources

- Free MS PowerShell Training

https://mva.microsoft.com/en-us/training-courses/getting-started-with-powershell-3-0-jump-start-8276?l=r54IrOWy_2304984382

- Hey, Scripting Guy

https://blogs.technet.microsoft.com/heyscriptingguy/

PowerShell Challenge

- We learn best when challenged. Underneath the class folder is a PowerShell Challenge Folder.
- Each level contains a code. Collect each code from every level and then decode the BASE64 encoded command to reveal the final challenge
- Winner gets a prize

Questions