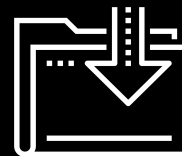




PowerShell Scripting

Cybersecurity

Windows Administration and Hardening Day 2



Class Objectives

By the end of today's class, you will be able to:



Run cmdlets to execute PowerShell calls.



Combine shell-scripting concepts such as cmdlets, parameters, piping, conditions, and importing files with data structures.



Use PowerShell to remote to Windows Server to send files.



Use a single script to prepare logs from a Windows 10 machine to be sent to Windows Server.



**While many
IT professionals prefer
Mac OS and Linux,
Windows is still the
leader for desktop operating
systems.**

Let's Review

Last class, we learned how to use CMD to execute many Windows sysadmin tasks.



How to audit processes with Task Manager.



Using CMD to create files.



Creating a report with `wmic` in the command line.



Auditing unwanted startup applications and services.



Enumerating local users, groups, and current local password policies.



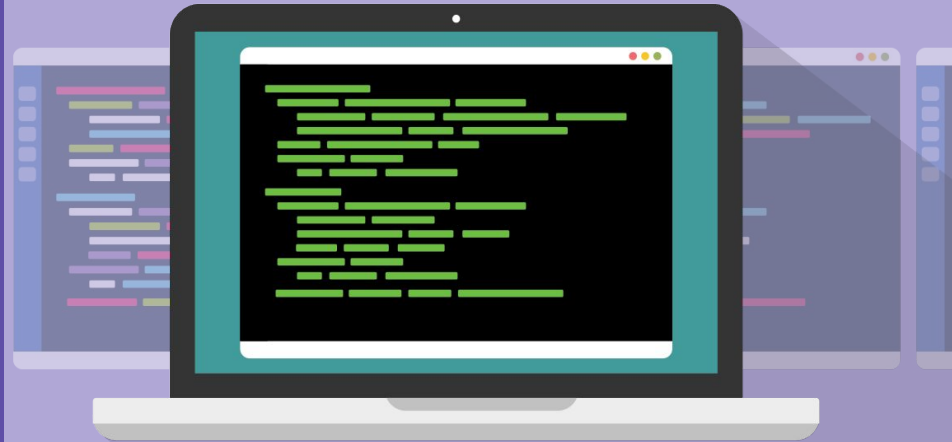
Creating new regular and administrative users and setting local password policies.



Scheduling tasks using Task Scheduler.

While CMD is short, simple and easy to learn, it isn't designed for complex operations and procedures.

On the other hand, PowerShell was designed as a powerful language used to execute, automate, and customize the most demanding and difficult tasks.



So, What is PowerShell?

PowerShell is a powerful scripting language that lets us locally and remotely manage Microsoft's line of products.

➡ Since Microsoft enterprise products are the most widely used by organizations, it is critical that system administrators and security professionals know PowerShell.

➡ PowerShell can be used to lock down and harden enterprise networks, leveraged by offensive security professionals, and exploited by malicious actors.



PowerShell vs. CMD

CMD's functionality is limited.

CMD output is only available in simple text format.

- For unsupported file formats, we need to edit the output with meticulous character replacing.

CMD command flags can be ambiguous, confusing, and specific to each command:

- Examples of different `/s` flags:
 - `shutdown /s` shuts down a computer.
 - `freekdisk /s` specifies the name of an IP or remote computer to check disk space.
- Examples of different `/d` flags.
 - `shutdown /d` specifies a reason for shut down.
 - `freedisk /d` specifies which disk drive to check.

PowerShell vs. CMD

PowerShell provides clearly defined, universal parameters for commands.



Based on the language used in the following commands, what do you think they do?

```
Stop-Computer -Confirm
```

```
Stop-Computer -Force
```


PowerShell vs. CMD

PowerShell provides clearly defined, universal parameters for commands.



Based on the language used in the following commands, what do you think they do?

Stop-Computer -Confirm

Shuts down the machine with a confirmation prompt verifying that you want to shut it down.

Stop-Computer -Force

Immediately shuts down the machine.

PowerShell vs. CMD


To find the file sizes of all files in C:\Windows, we can use a complex batch file consisting of the following:

```
@echo off
set size=0
for /r %%x in (System\*) do set /a size+=%%~zx
echo %size% Bytes
```

PowerShell can do this with a simple pipe (|):

```
dir C:\Windows\System -Recurse | Measure-Object -Sum Length
```

- `dir C:\Windows\System -Recurse`: Grabs all the current directory and subdirectory contents.
- `Measure-Object -Sum Length`: The output is piped into this command, which measures files.

 **Objects** are a very important PowerShell concept. We'll look at them next.

What Are Objects?

“Object” is Microsoft’s name for every component in a system that PowerShell recognizes and interacts with.

If we run `ls C:\Windows`:

- All the files and directories in C:\Windows are processed by PowerShell. Each is an object, with its own properties.
- `C:\Documents\Recipes\Guacamole.doc`
 - `Guacamole.doc` is the `file.name` property of the file (object).

What Are Objects?

Understanding everything as objects with properties allows us to use more specific commands to target the results we want.

For example: We can use a pipe to retrieve only objects containing the word “system”:

```
ls C:\Windows | Where-Object {$_.name -like "*system*"}
```

- Lists contents of C:\Windows in which the .name property contains “system.”
- `$_`: Indicates the previous object, referring to C:\Windows.

We'll cover syntax in more depth later.

More PowerShell Benefits



We can confirm we're using the right commands with PowerShell's extensive internal documentation system.



PowerShell supports some Unix commands, like `ls` and `cat`.



Despite being a Microsoft product, PowerShell is open source and available on GitHub. By contrast, there's no source code available for CMD, and writing tools are limited to batch scripts.

PowerShell Commands:

CMDlet	Function	Equivalent Command
Set-Location	Changes to specified directory	cd
Get-ChildItem	Returns current directory contents	ls, dir
New-Item	Makes new directory	mkdir
Remove-Item	Deletes file or directory	rm, rmdir
Get-Location	Retrieves path to current directory	pwd
Get-Content	Returns file content	cat, type
Copy-Item	Copies a file from one location to another	cp
Move-Item	Moves item from one location to another	mv
Write-Output	Prints output	echo
Get-Alias	Shows aliases from the current session	alias
Get-Help	Retrieves information about command	man
Get-Process	Retrieves processes running on machine	ps
Stop-Process	Stops specific process	kill
Get-Service	Retrieves list of services	service --status-all

Verbs-Nouns

Consider the following scenario:

- User **Alex** left the company.
- We want to remove their user account from the system, but we want to keep the reports they were working on.
- We need to move the reports files from their user Desktop directory to a directory outside of the user.
- Along the way, we'll show some other useful Powershell commands.

We'll use the following commands:

Set-Location, Move-Item, Get-ChildItem, New-Item, Remove-Item





Instructor Demonstration

Verbs-Nouns


Parameters

Now, we'll use parameters to customize the commands.

Instead of using **New-Item** to create another file, we can add parameters to the **New-Item** command and create a directory, with a specific name and location:

```
New-Item -Path "C:\\" -Name "Logs" -ItemType "Directory"
```

- **Path**: Parameter specifying the location of this new directory.
- **-Name**: Parameter specifying the directory's name.
- **-ItemType**: Parameter specifying the type of item we want to create.
If we don't specify **"Directory"**, it will default to a file.



Let's
take a look
at some more
parameters...



Instructor Demonstration

Parameters



Activity: Moving and Creating Directories

In this activity, you will work as a junior sysadmin tasked with vetting a process to create Windows Event logs.

First we need to create the appropriate directories to store our information. We'll run PowerShell commands to create, rename, and move items.

Suggested Time:
10 Minutes





Time's Up! Let's Review.

Activity Review: Moving and Creating Directories

To complete this activity, we needed to:

01

Move the **contracts** directory to **C:**.

02

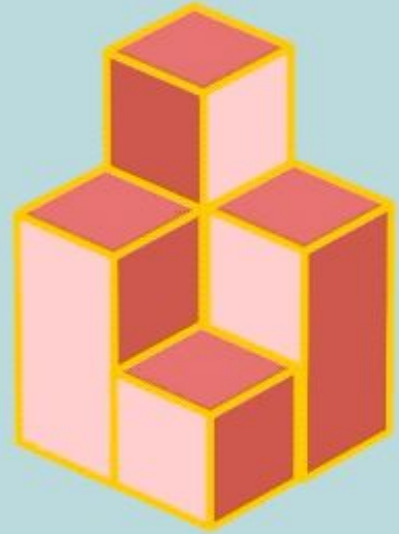
Create **Logs** and **Scripts** directories in **C:**.

03

Rename the **reports** directory as **Reports**.

Generating Windows Event Log Files with Parameters and Pipelines

Now, we will continue building on parameters by chaining commands with pipelines.



A woman with long dark hair, wearing a bright yellow long-sleeved shirt, is shown in profile from the chest up, focused on her work. She is sitting at a desk and typing on a laptop. The background is a blurred office environment with large windows and indoor plants. A semi-transparent white box with black text is overlaid on the right side of the image.

Pipeline Demo Setup

In the following demo, we're continuing our role as a junior sysadmin.

Our CIO asked us to retrieve multiple types of logs from our Windows 10 machine and save them as json files in our newly created C:\Logs directory. They will later be imported to a Splunk SIEM for analysis.

Use your cheat sheet to help follow along.



Instructor Demonstration

PowerShell Pipeline

Piping Logs to JavaScript Object Notation with ConvertTo-Json

Now that we've used parameters to get the logs we needed, we will output them into a file that can be later used by log analysis applications.

This is where pipelines come in.





Instructor Demonstration

Piping Logs to json



Activity: Generating Windows Event Log Files

In this activity, you will create and save log files to **C:/Logs**.

Suggested Time:
10 Minutes





Time's Up! Let's Review.

Activity Review: Generating Windows Event Log Files

To compete this activity, we needed to:

01

Execute cmdlets with a variety of parameters and parameter values.

02

Pipe cmdlets together to transform the PowerShell output.

03

Query event logs.

04

Select the most recent logs.

05

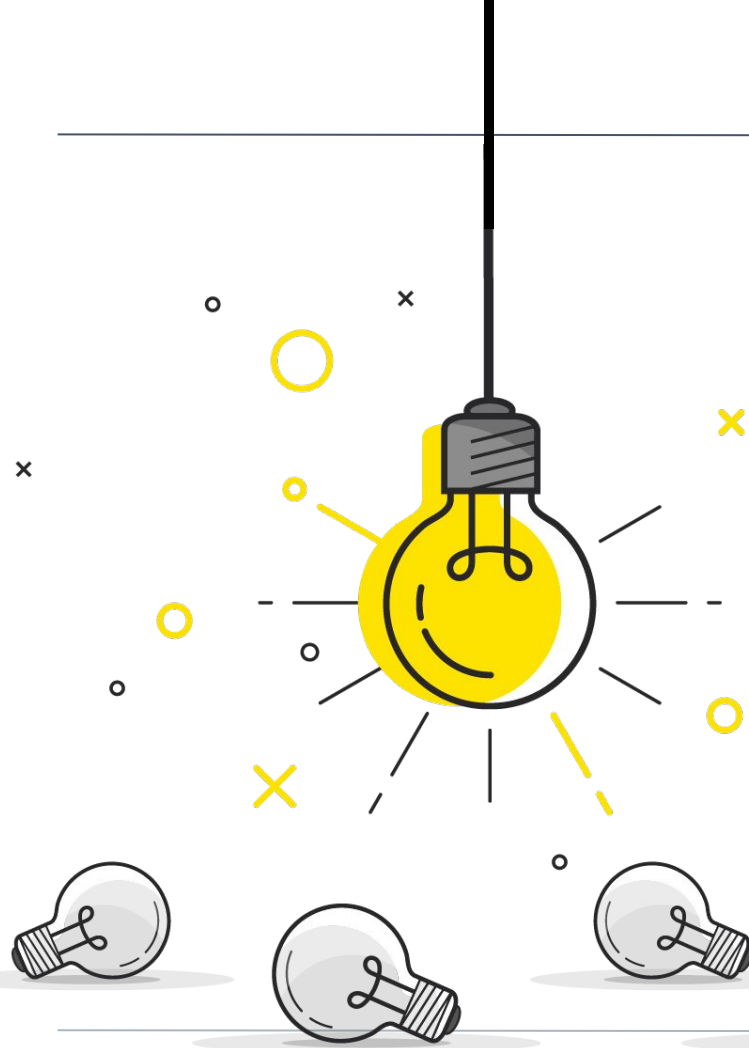
Output the logs to a **json** file.

Scripting with PowerShell

The Importance of Scripting (Again)

We've emphasized the importance and convenience of scripting in our past sysadmin units.

- Scripts allow sysadmins and security professionals to automate and execute basic to advanced procedures and operations.
- Scripts can be used for everything from setting basic firewall rules to standing up entire cloud virtual machine environments with networking, storage, and users.

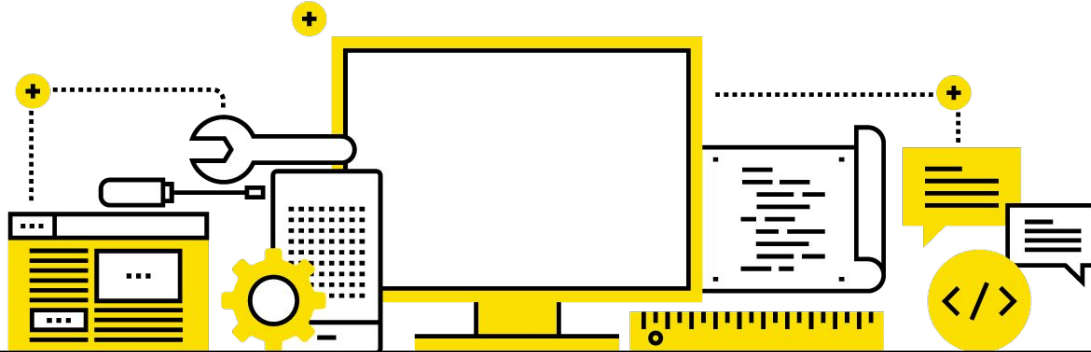


Scripting with PowerShell

Like Linux, PowerShell allows us to script many commands in sequence:

For example, suppose you need to set up Windows workstations for users in the accounting department. You could create a script do the following, in order:

- i. Pull sensitive accounting data and files from a file server to a specified directory.
- ii. Download **AppLocker**, a program for limiting and controlling access to files for certain users and groups.
- iii. Deploy application control policies for **AppLocker** to restrict user access to the directory so only people in the accounting group can access it.

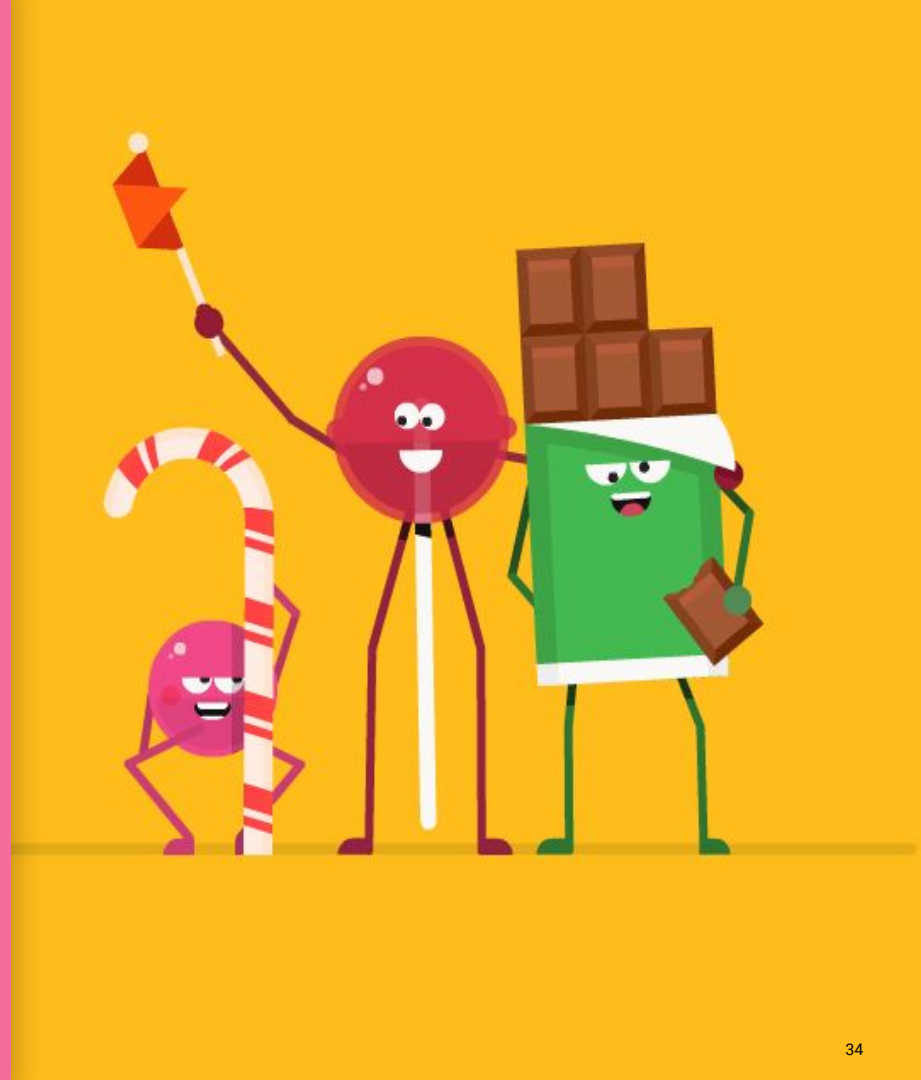


Scripting Demo Scenario

In this demonstration, we will create a script in VS Code to remove pre-installed *Candy Crush Friends Saga*.

Windows 10 has been notoriously known for implementing a lot of settings and preinstalled applications that have been considered bloat and potential larger attack vectors.

- Some of these settings include **telemetry tracking** and **advertising IDs** while some of the default installed applications include *Candy Crush*.
- We want to remove these applications to reduce the attack surface area for this workstation. Instead of trusting our users to not use these apps, we're going to remove the possibility.





Instructor Demonstration

Removing Candy Crush

We've just deleted a useless app from our machine. While we could remove the Windows Store apps one by one, it would be more time efficient to create a script that will loop through a **list** of the apps and uninstall them all at once.



CSV Files

More specifically, we can loop through **Comma-Separated Values** (CSV) files.

- CSV are plain text files that contain simply structured data (**fields**) separated by commas.
- The top line of a CSV file contains the **header** — the row that describes each field.

Sysadmins and security professionals will use CSV files containing lists of items they need to parse through.

- A system administrator may use a CSV file to maintain a list of employee email addresses and usernames.
- A penetration tester might have a list of IP addresses and corresponding domain and subdomain names to use in a test..

CSV File

```
appxpkg,name,description
"Microsoft.ZuneMusic","Zune","Microsoft's Zune Music Player"
"Microsoft.Music.Preview","Music Preview", "Microsoft's Music Preview"
"Microsoft.XboxGameCallableUI","Xbox Gaming GUI", "Microsoft's Xbox Overlay"
[CSV contents truncated]
```




appxpkg	name	description
Microsoft.ZuneMusic	Zune	Microsoft's Zune Music Player
Microsoft.Music.Preview	Music Preview	Microsoft's Music Preview
Microsoft.XboxIdentityProvider	Xbox ID Provider	Microsoft's Xbox Live Account Management

CSV File

To loop through these files' items, we have the `foreach` loop.

- The `foreach` loop in PowerShell is similar to the `for` loop in Linux, but it is mainly used for looping through files or read-only structured data that you need to loop through.

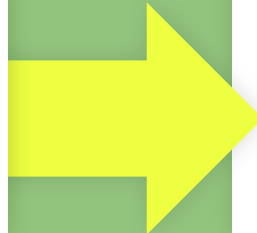


appxpkg	name	description
Microsoft.ZuneMusic	Zune	Microsoft's Zune Music Player
Microsoft.Music.Preview	Music Preview	Microsoft's Music Preview
Microsoft.XboxIdentityProvider	Xbox ID Provider	Microsoft's Xbox Live Account Management

`foreach` Loops and CSV Files

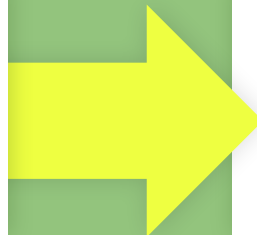
Sysadmins and security professionals will use CSV and `foreach` loops together:

A system administrator may use a CSV file to maintain a list of employee email addresses and usernames.



They can use a `foreach` loop to loop through each item and change the passwords.

A penetration tester might have a list of IP addresses and corresponding domain and subdomain names to use in a test.



They can use a `foreach` loop to try out each password with a known username.



Instructor Demonstration

PowerShell Script Importing a CSV File and Looping Through Field Attributes



Activity: Removing Windows Bloat with PowerShell Scripts

In this activity, you'll use PowerShell and a CSV file to create a script that removes unwanted applications.

Suggested Time:
15 Minutes





Time's Up! Let's Review.

Activity Review: Removing Windows Bloat with PowerShell Scripts

To compete this activity, we needed to:

01

Use the cmdlet **Import-Csv** to import a CSV file as an object into PowerShell.

02

Create a **foreach** condition that loops through each line, for the application name field, in the CSV file.

03

On every loop, execute a two-part cmdlet pipe that retrieves each application object by name, and sends it to the **Remove-AppxPackage -Verbose** cmdlet to uninstall it.

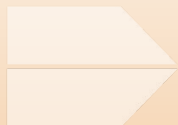
PowerShell Remoting

Throughout the day, we've been generating `json` log outputs in order to eventually send them to a Windows Server and then an SIEM.

We will achieve this through remoting, which allows a user to interact with, run commands on, and control programs running on a different, remote machine.

Remoting in a Larger Context

Remoting is a ubiquitous system administration and security skill.



A system administrator may remote into a user's machine to troubleshoot issues or install software.



An offensive security professional may use remoting to access a standard user's computer and escalate their privileges to accounts with more access within a network.

Remoting has important security implications.



Defensive security professionals and sysadmins will need to know how to harden this type of access.



Offensive security penetration testers will often try to exploit remoting to achieve lateral access to increasingly sensitive systems and accounts within an organization.

Remoting in Windows

We will be using the PowerShell session management cmdlets, `Enter-PSSession` and `New-PSSession`, over the WinRM protocol.

`Enter-PSSession` is a cmdlet that establishes an interactive PowerShell session with a single remote machine.

- Similar to using SSH to create interactive sessions on Linux machines.
- Commands used with `Enter-PSSession` will run on the remote computer.
- Interactive sessions are like “one-off” commands. Once you execute the command, the session is ended.

Remoting in Windows

We will be using the PowerShell session management cmdlets, `Enter-PSSession` and `New-PSSession`, over the WinRM protocol.

`New-PSSessions` is a cmdlet that establishes a persistent session that can be left running.

- Unlike an interactive session, a remote session stays running.
- It can be terminated using `Remove-PSSession`.

Remoting in Windows

We will be using the PowerShell session management cmdlets, `Enter-PSSession` and `New-PSSession`, over the WinRM protocol.

WinRM (Windows Remote Management) is a remoting protocol.

- It allows for remote access to a Windows system, similar to SSH.
- By default it is set to transfer over HTTP on port 5985, but can be set up with either a trusted host system or SSL certificates to enable HTTPS on port 5986.

(Don't worry too much about ports and protocols right now. We'll cover these *extensively* in the coming Network units.)

Remoting Demo Scenario

The CIO of our company wants to be able to pull Windows 10 logs off workstations and transport them to a central Windows Server. They want to transport logs using working scripts that can be used on any Windows 10 machine.

For the upcoming demo, we will:

- Enable WinRM remoting.
- Add the Windows Server as a trusted host.
- Use an interactive remote session to set up a logs folder on the Windows Server machine.
- Set up a script that initiates a session and transfers a log file.





Instructor Demonstration

Windows Remoting



Activity: PowerShell Remoting

In this activity, you will construct a script to send the **Get-WinEvent** security log **.json** files to the Windows Server.

Suggested Time:
15 Minutes





Time's Up! Let's Review.

Activity Review: PowerShell Remoting

To compete this activity, we needed to:

01

Enable PowerShell remoting to trusted hosts. In this case, the Windows Server IP address.

02

Use **Enter-PSSession** to remotely access the Windows Server and set up a **C:\Logs** directory.

03

Create a script that does the following:

- Sets up a variable to set up the **New-PSSession** cmdlet with **-ComputerName** and **-Credential** parameters.
- Adds a **Copy-Item** cmdlet to copy the **RecentSecurityLogs.json** file made in the previous activity to the **C:\Logs** directory on the remote host, with the following parameters: **-Destination** and **-ToSession**.
- Uses **Remove-PSSession \$Session** at the end of the script to end our remote session (since these are persistent sessions).

In the final activity of the day, **we will combine all the topics covered, and write a single script** that creates ingestible logs and remotely transfers files through PowerShell.





The Full Script

In the next activity, you will compile all the skills learned today to create a script that does the following:

- Creates the logs as json files.
- Establishes a PowerShell session.
- Transfers each log over to a target machine.

Important Note:

- Unlike previous activities, we are not using a CSV file. Rather, we will be working with the individual contents of a directory.
- You will need to run the script a directory above the log files that you are transferring over.



Activity: The Full Script

For this activity, we will make a script that creates logs, establishes a PowerShell session, and transfers each log over to a target machine.

Suggested Time:
15 Minutes





Time's Up! Let's Review.

Activity Review: The Full Script

This activity required us to complete a common operation for sysadmins and security professionals. We are also a step closer to automating and utilizing re-executable scripts.

In order for this script to function, it needed to do the following:

01

Create the event logs for each type of log, with a maximum of 50 events, in a `json` file.

02

Establish a session with a `$Session` variable.

03

Use a `$log` variable to store each item in our `Logs` directory.

04

Use a `foreach` loop that, for each item in our `Logs` directory, uses `Copy-Item` to send the file `$log` over our remote PowerShell session.

05

Use an `echo` line to show us, in PowerShell's console output, each file name that is sent over.

06

Use `Remove-PSSession $Session` at the end of our script to end the session.

Any Questions?