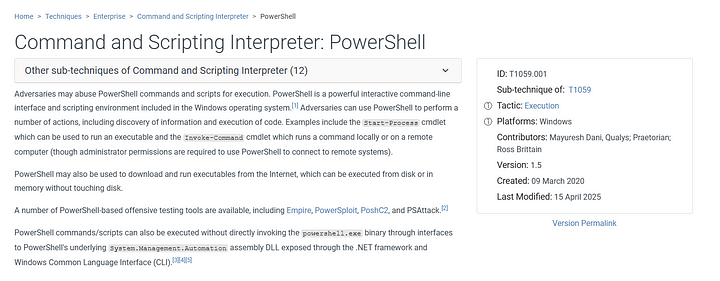
### **PowerShell Threat Emulation & Detection using MITRE ATT&CK T1059.001**

#### **T1059**

T1059 is a broader technique where Adversaries use command line interpreters to execute commands, scripts or binaries on a system. This technique is part of the Execution tactic of MITRE ATT&CK framework.

#### **T1059.001**

T1059.001 is a sub-technique of the broader Command and Scripting Interpreter technique. This sub-technique is related to PowerShell. PowerShell is a built in powerful command-line interface and scripting language on Windows.



#### **Atomic Test T1059.001**

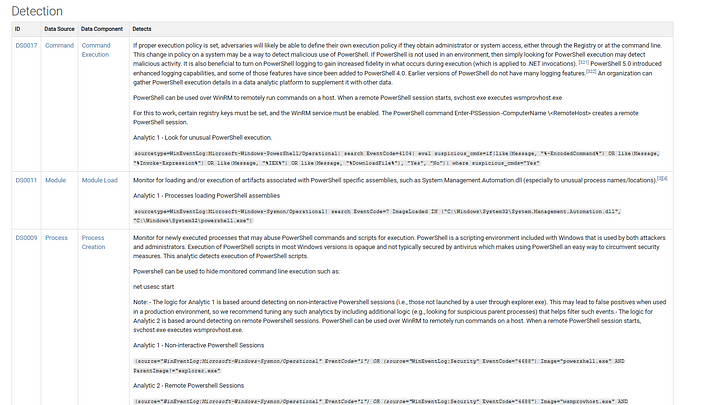
The Atomic test has a series of 22 tests that would implement the same techniques and commands that a Adversary would use. These tests provide a comprehensive test to detect any security weaknesses or to improve the detection. This test can be found under the GitHub repository — <https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1059.001/T1059.001.md>

**How to Detect:**

Look for the following red flags

* **Encoded commands**: -EncodedCommand is often used to hide malicious PowerShell commands.
* **IEX (Invoke-Expression)**: Executes a string as a command — often used with downloaded payloads.
* **Invoke-WebRequest / DownloadString**: Used to download malware or scripts.

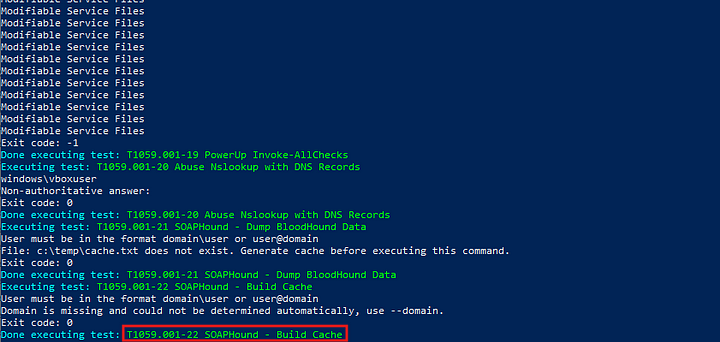
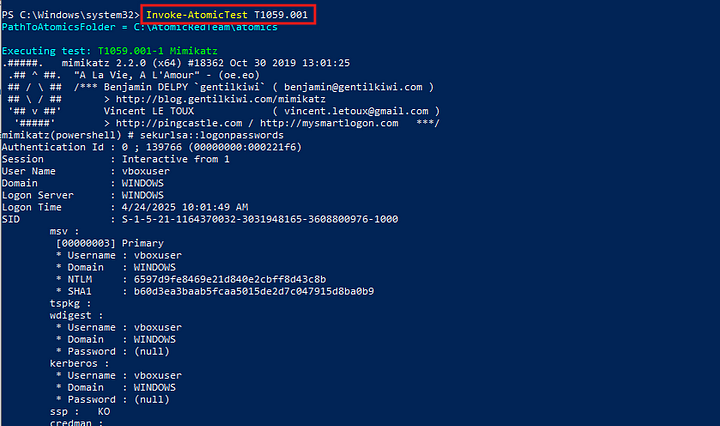
More on detecting these kind of attacks can be seen on the [MITRE's](https://attack.mitre.org/techniques/T1059/001/) page.



**Starting the test:**

We can start the test with the following command. Note that Invoke Atomic must be installed for this to work. More about how to install it [here](https://github.com/redcanaryco/invoke-atomicredteam/wiki/Installing-Invoke-AtomicRedTeam).

Invoke-AtomicTest T1059.001



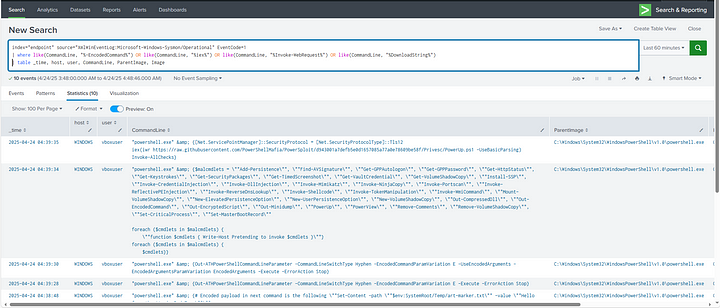
#### **Detection in Splunk**

Once the execution is complete, we can head over to Splunk and search for the suspicious activity. Based on the above mentioned red flags, we can craft a search filter as follows

index="endpoint" source="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" EventCode=1

| where like(CommandLine, "%-EncodedCommand%") OR like(CommandLine, "%iex%") OR like(CommandLine, "%Invoke-WebRequest%") OR like(CommandLine, "%DownloadString%")

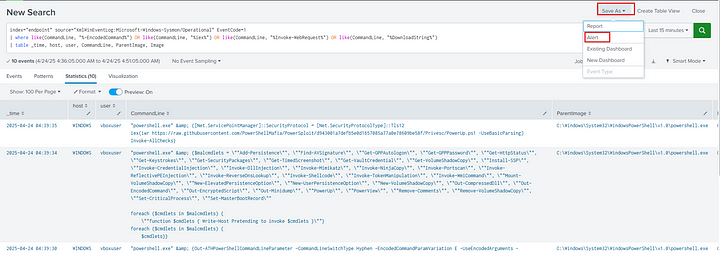
| table \_time, host, user, CommandLine, ParentImage, Image



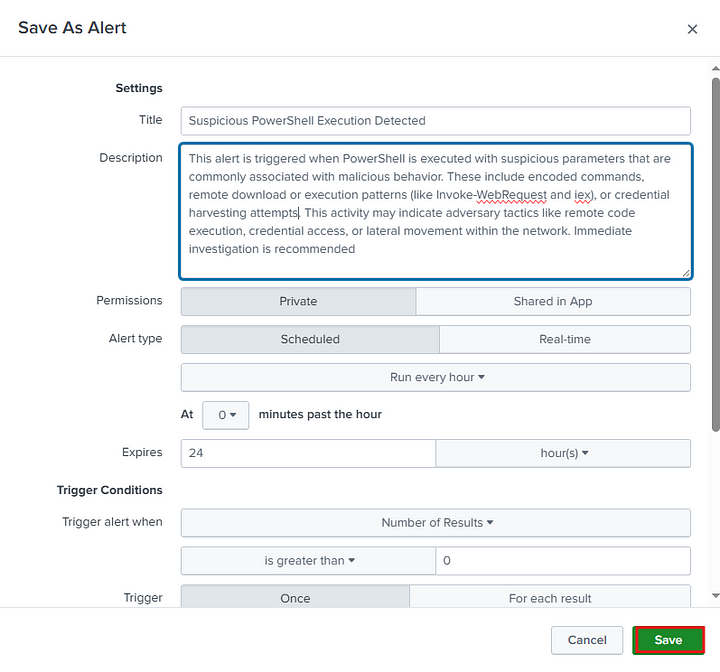
The above filter will search the Windows event logs generated by Sysmon, specifically for the process creation events where the suspicious commands were used.

We can create an alert in Splunk to keep monitoring for the suspicious activity and alert us when the search triggers any logs.

In the search, go to save as and click on alert.



Then choose the appropriate options on the next Dialog box and click on save. Now our Alert is created and will trigger when any suspicious activity is detected.



Cleanup

After successful execution and detection, we can cleanup with the following commands.

Remove-Item $env:Temp\\*BloodHound.zip -Force

Remove-Item $env:Temp\\*BloodHound.zip -Force

Remove-Item -path C:\Windows\Temp\art-marker.txt -Force -ErrorAction Ignore

Remove-Item HKCU:\Software\Classes\AtomicRedTeam -Force -ErrorAction Ignore

Remove-Item #{ads\_file} -Force -ErrorAction Ignore

This exercise helps simulate real-world PowerShell-based threats and demonstrates how to detect them using Sysmon and Splunk. By automating detection with alerts, you can proactively identify potential malicious behavior and respond more efficiently.