Detecting MITRE T1059 PowerShell Execution Using Wazuh

Objective:

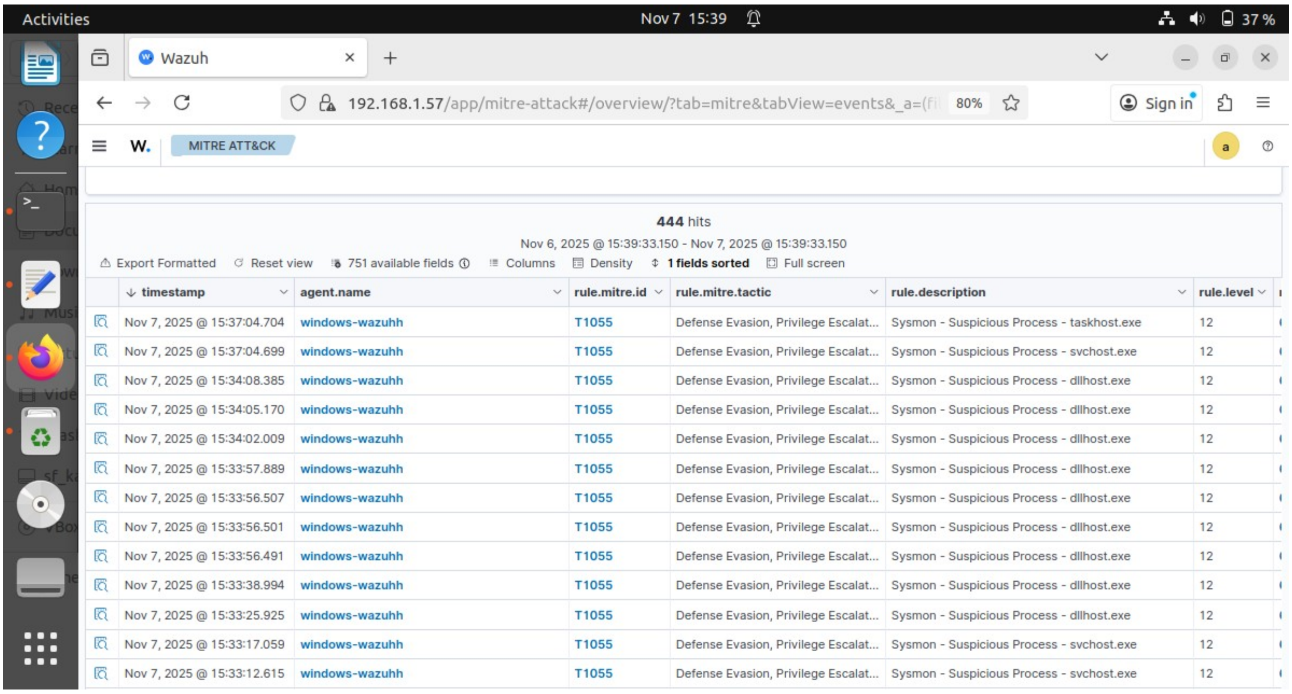
To detect and alert on adversarial use of PowerShell commands and scripts for malicious execution, focusing on the MITRE ATT&CK Technique T1059.001, using Wazuh.

Goals:

This focuses on detecting the abuse of Invoke-command for running commands locally or on remote systems by attackers, a common tactic within MITRE T1059.001

Before Trigger alert :

Before triggering the alert, check that the timestamp on the Wazuh manager is 15:37.



Activities
Nov 7 15:39
37 %
Wazuh
192.168.1.57/app/mitre-attack#/overview/?tab=mitre&tabView=events&_a=(fi
80%
Sign in
W.
MITRE ATT&CK
a

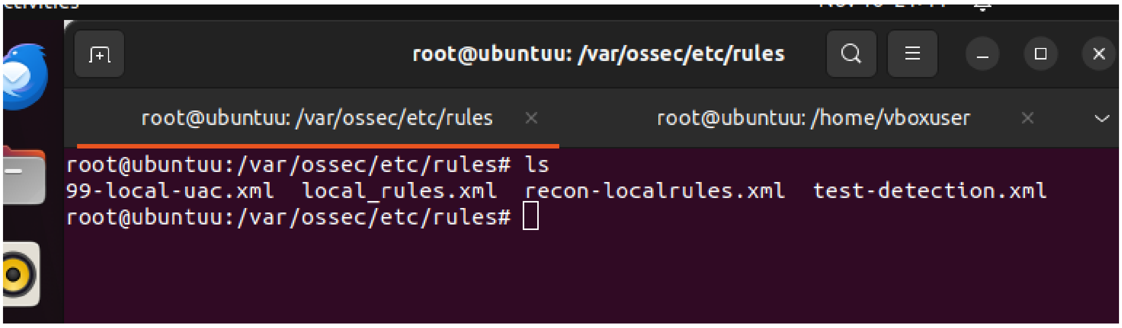
444 hits

Nov 6, 2025 @ 15:39:33.150 - Nov 7, 2025 @ 15:39:33.150

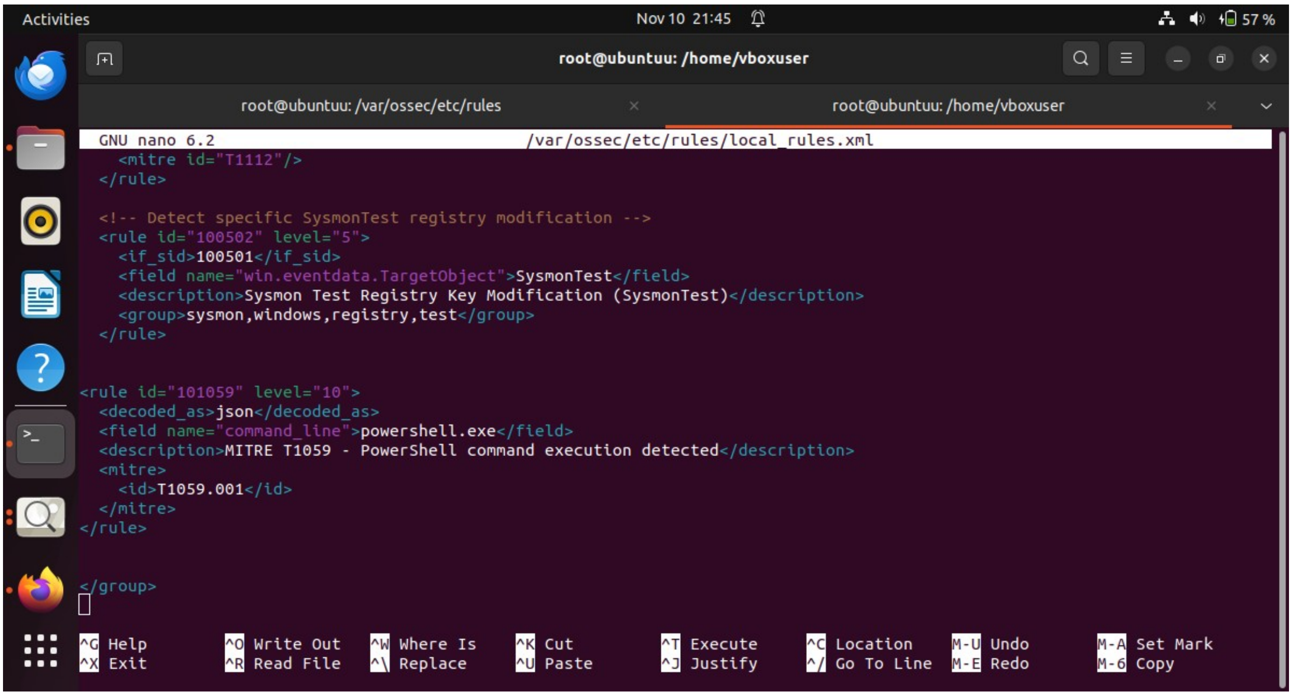
timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level
Nov 7, 2025 @ 15:37:04.704	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - taskhost.exe	12
Nov 7, 2025 @ 15:37:04.699	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - svchost.exe	12
Nov 7, 2025 @ 15:34:08.385	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:34:05.170	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:34:02.009	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:33:57.889	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:33:56.507	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:33:56.501	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:33:56.491	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:33:38.994	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:33:25.925	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - dllhost.exe	12
Nov 7, 2025 @ 15:33:17.059	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - svchost.exe	12
Nov 7, 2025 @ 15:33:12.615	windows-wazuhh	T1055	Defense Evasion, Privilege Escalat...	Sysmon - Suspicious Process - svchost.exe	12

Steps to Reproduce:

1. Create a local rule on the Wazuh manager based on the MITRE Tactic ID **T1059.001**.


root@ubuntuu: /var/ossec/etc/rules
root@ubuntuu: /var/ossec/etc/rules
root@ubuntuu: /home/vboxuser

```
root@ubuntu:/var/ossec/etc/rules# ls
99-local-uac.xml  local_rules.xml  recon-localrules.xml  test-detection.xml
root@ubuntu:/var/ossec/etc/rules#
```



```
    <mitre id="T1112"/>
  </rule>

  <!-- Detect specific SysmonTest registry modification -->
  <rule id="100502" level="5">
    <if_sid>100501</if_sid>
    <field name="win.eventdata.TargetObject">SysmonTest</field>
    <description>Sysmon Test Registry Key Modification (SysmonTest)</description>
    <group>sysmon,windows,registry,test</group>
  </rule>

<rule id="101059" level="10">
  <decoded_as>json</decoded_as>
  <field name="command_line">powershell.exe</field>
  <description>MITRE T1059 - PowerShell command execution detected</description>
  <mitre>
    <id>T1059.001</id>
  </mitre>
</rule>


</group>
```

```
<rule id="101059" level="10">
  <decoded_as>json</decoded_as>
  <field name="command_line">powershell.exe</field>
  <description>MITRE T1059 - PowerShell command execution detected</description>
  <mitre>
    <id>T1059.001</id>
  </mitre>
</rule>
```

Add the above ,local rule on the **$nano /var/ossec/etc/rules/localrule.xml**

Then restart wazuh manager :

```
$ sudo systemctl restart wazuh-manager
```

2) Generate PowerShell Encoded Command for Testing on the windows:

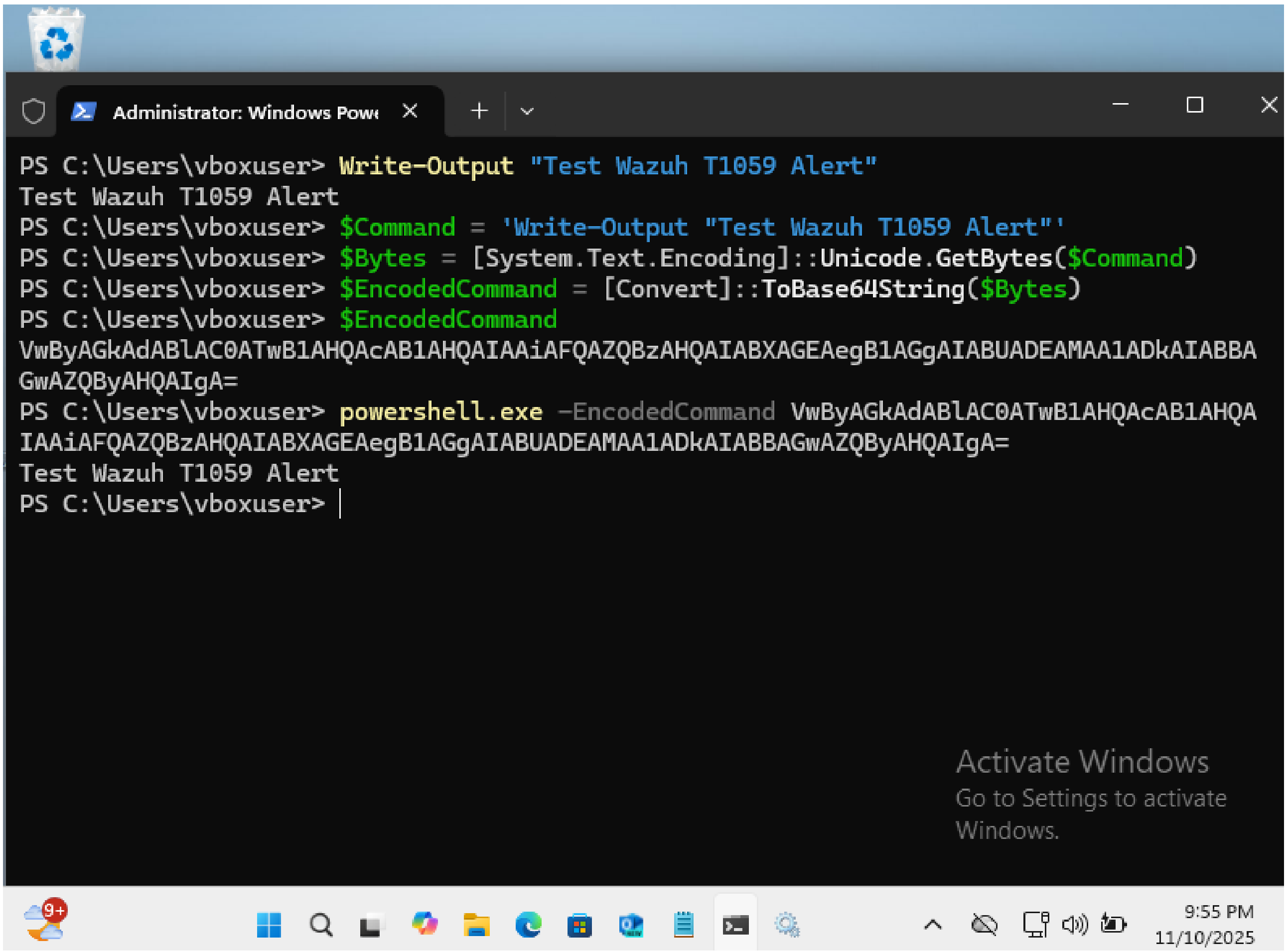
Open Powershell :

```
 > Write-Output "Test Wazuh T1059 Alert"
> $Command = 'Write-Output "Test Wazuh T1059 Alert"'
$Bytes = [System.Text.Encoding]::Unicode.GetBytes($Command)
$EncodedCommand = [Convert]::ToBase64String($Bytes)
$EncodedCommand
VwByAGkAdABlAC0ATwB1AHQAcAB1AHQAIAAiAFQAZQBzAHQAIABXA
GEAegB1AGgAIABUADEAMAA1ADkAIABBAGwAZQByAHQAIgA=
```

Next Add in this powershell command :

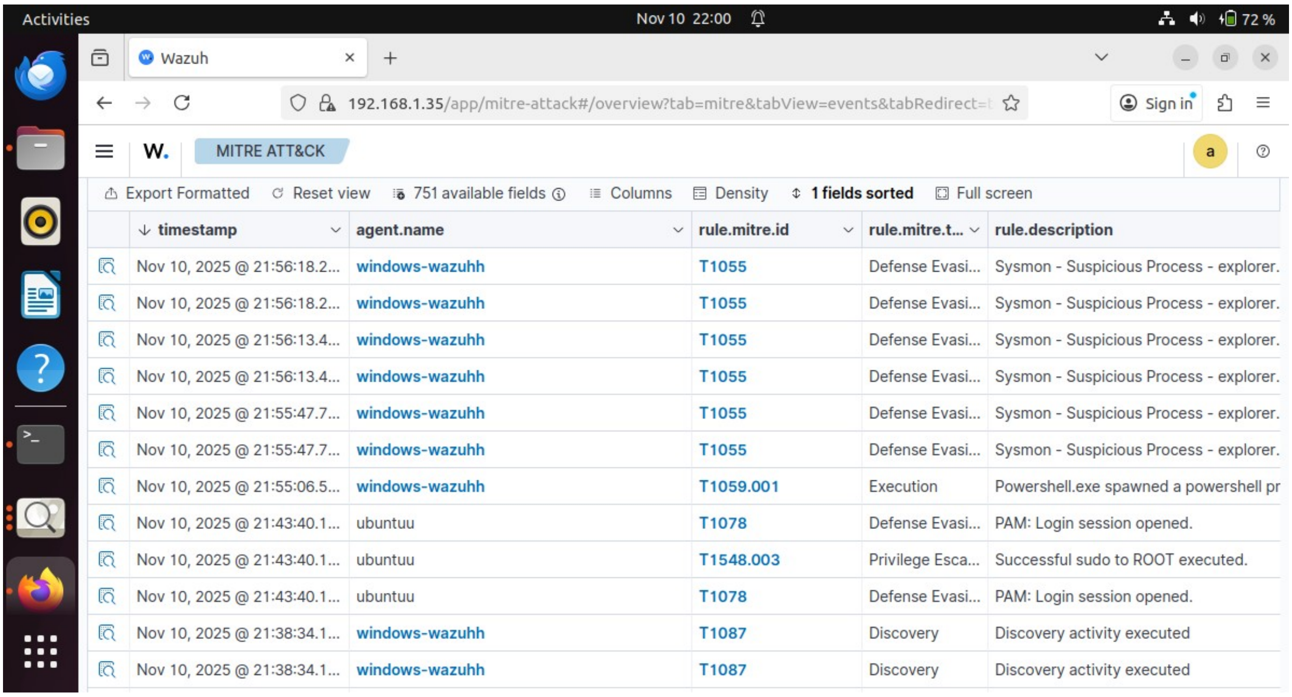
```
>  powershell.exe -EncodedCommand
VwByAGkAdABlAC0ATwB1AHQAcAB1AHQAIAAiAFQAZQBzAHQAIABXA
GEAegB1AGgAIABUADEAMAA1ADkAIABBAGwAZQByAHQAIgA=
```

Now I did the attack on the windows powershell , check the timestamp on below image : Time is 9:55 on the windows agent machine.


Administrator: Windows Powe
Activate Windows
Go to Settings to activate Windows.
9:55 PM
11/10/2025

```
PS C:\Users\vboxuser> Write-Output "Test Wazuh T1059 Alert"
Test Wazuh T1059 Alert
PS C:\Users\vboxuser> $Command = 'Write-Output "Test Wazuh T1059 Alert"'
PS C:\Users\vboxuser> $Bytes = [System.Text.Encoding]::Unicode.GetBytes($Command)
PS C:\Users\vboxuser> $EncodedCommand = [Convert]::ToBase64String($Bytes)
PS C:\Users\vboxuser> $EncodedCommand
VwByAGkAdABlAC0ATwB1AHQAcAB1AHQAIAAiAFQAZQBzAHQAIABXAGEAegB1AGgAIABUADEAMAA1ADkAIABBA
GwAZQByAHQAIgA=
PS C:\Users\vboxuser> powershell.exe -EncodedCommand VwByAGkAdABlAC0ATwB1AHQAcAB1AHQA
IAAiAFQAZQBzAHQAIABXAGEAegB1AGgAIABUADEAMAA1ADkAIABBAGwAZQByAHQAIgA=
Test Wazuh T1059 Alert
PS C:\Users\vboxuser> |
```

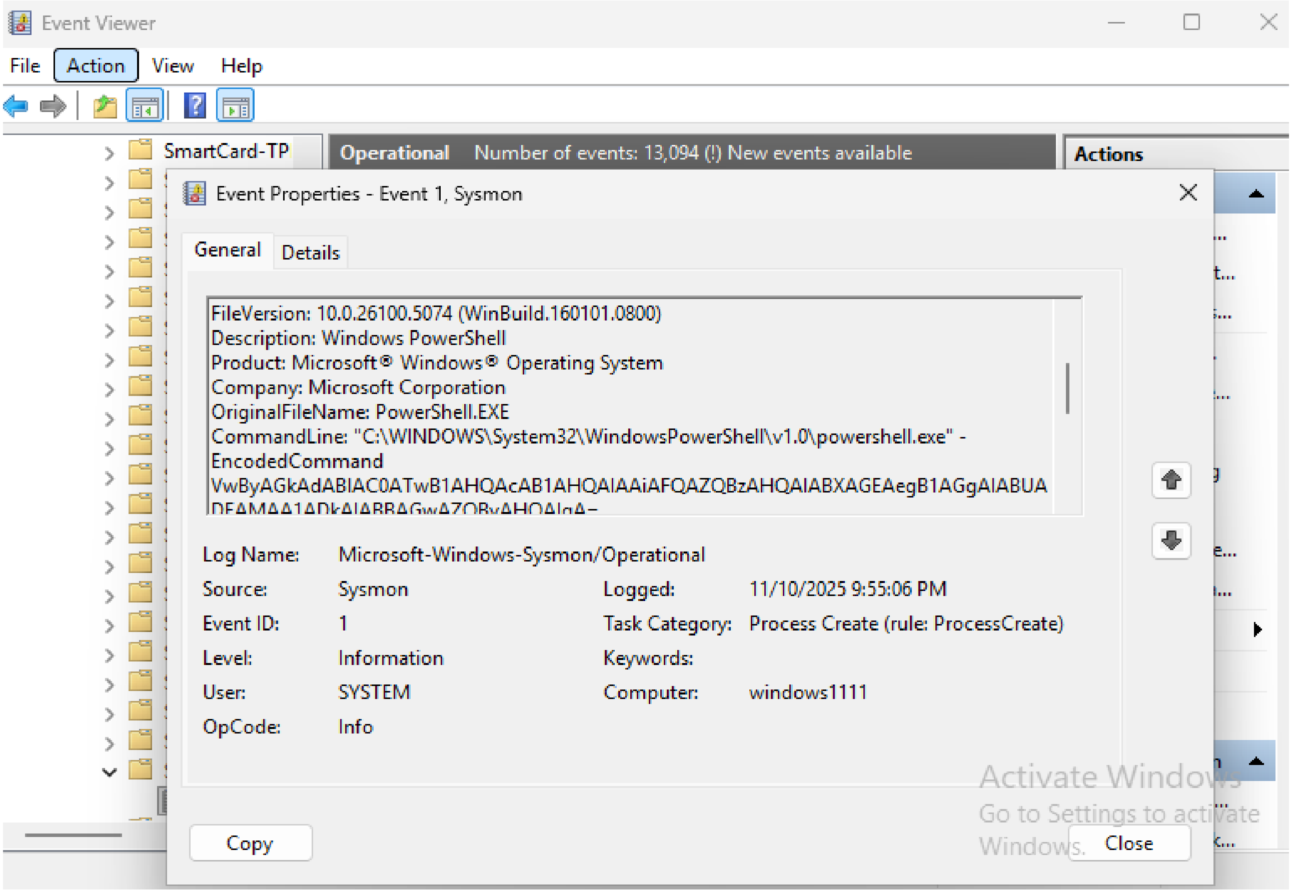
Check the wazuh manager on the console :



timestamp	agent.name	rule.mitre.id	rule.mitre.t...	rule.description
Nov 10, 2025 @ 21:56:18.2...	windows-wazuhh	T1055	Defense Evasi...	Sysmon - Suspicious Process - explorer.
Nov 10, 2025 @ 21:56:18.2...	windows-wazuhh	T1055	Defense Evasi...	Sysmon - Suspicious Process - explorer.
Nov 10, 2025 @ 21:56:13.4...	windows-wazuhh	T1055	Defense Evasi...	Sysmon - Suspicious Process - explorer.
Nov 10, 2025 @ 21:56:13.4...	windows-wazuhh	T1055	Defense Evasi...	Sysmon - Suspicious Process - explorer.
Nov 10, 2025 @ 21:55:47.7...	windows-wazuhh	T1055	Defense Evasi...	Sysmon - Suspicious Process - explorer.
Nov 10, 2025 @ 21:55:47.7...	windows-wazuhh	T1055	Defense Evasi...	Sysmon - Suspicious Process - explorer.
Nov 10, 2025 @ 21:55:06.5...	windows-wazuhh	T1059.001	Execution	Powershell.exe spawned a powershell pr
Nov 10, 2025 @ 21:43:40.1...	ubuntuu	T1078	Defense Evasi...	PAM: Login session opened.
Nov 10, 2025 @ 21:43:40.1...	ubuntuu	T1548.003	Privilege Esca...	Successful sudo to ROOT executed.
Nov 10, 2025 @ 21:43:40.1...	ubuntuu	T1078	Defense Evasi...	PAM: Login session opened.
Nov 10, 2025 @ 21:38:34.1...	windows-wazuhh	T1087	Discovery	Discovery activity executed
Nov 10, 2025 @ 21:38:34.1...	windows-wazuhh	T1087	Discovery	Discovery activity executed

In this image , just check the alert tactics T1059 its triggered on 21:55.

Sysmon event viewer :



Operational Number of events: 13,094 (!) New events available

Event Properties - Event 1, Sysmon

General Details

```
FileVersion: 10.0.26100.5074 (WinBuild.160101.0800)
Description: Windows PowerShell
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: PowerShell.EXE
CommandLine: "C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -
EncodedCommand
VwByAGkAdABlAC0ATwB1AHQAcAB1AHQAIAAiAFQAZQBzAHQAIABXAGEAegB1AGgAIABUA
DEAMAA1ADkAIABBAGwAZQByAHQAIgA=
```

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 11/10/2025 9:55:06 PM

Event ID: 1 Task Category: Process Create (rule: ProcessCreate)

Level: Information Keywords:

User: SYSTEM Computer: windows1111

OpCode: Info

Copy Close

Result :

The T1059.001 detection result shows that Wazuh successfully identified the execution of a PowerShell command using an encoded Base64 script. This confirms that your monitoring setup captures and alerts on adversarial use of PowerShell for execution, a common attacker technique.

- PowerShell was launched with a Base64 encoded command.
- The event was captured via Sysmon process creation logs.
- Wazuh triggered a high-level alert correlating to MITRE technique T1059.001.
- This detection helps identify script-based execution attacks leveraging PowerShell, which attackers use for code execution, discovery, and remote operations.