Detecting Event-Triggered Execution Attacks (MITRE T1546) Using Wazuh and Sysmon Process Creation Monitoring

Objective :

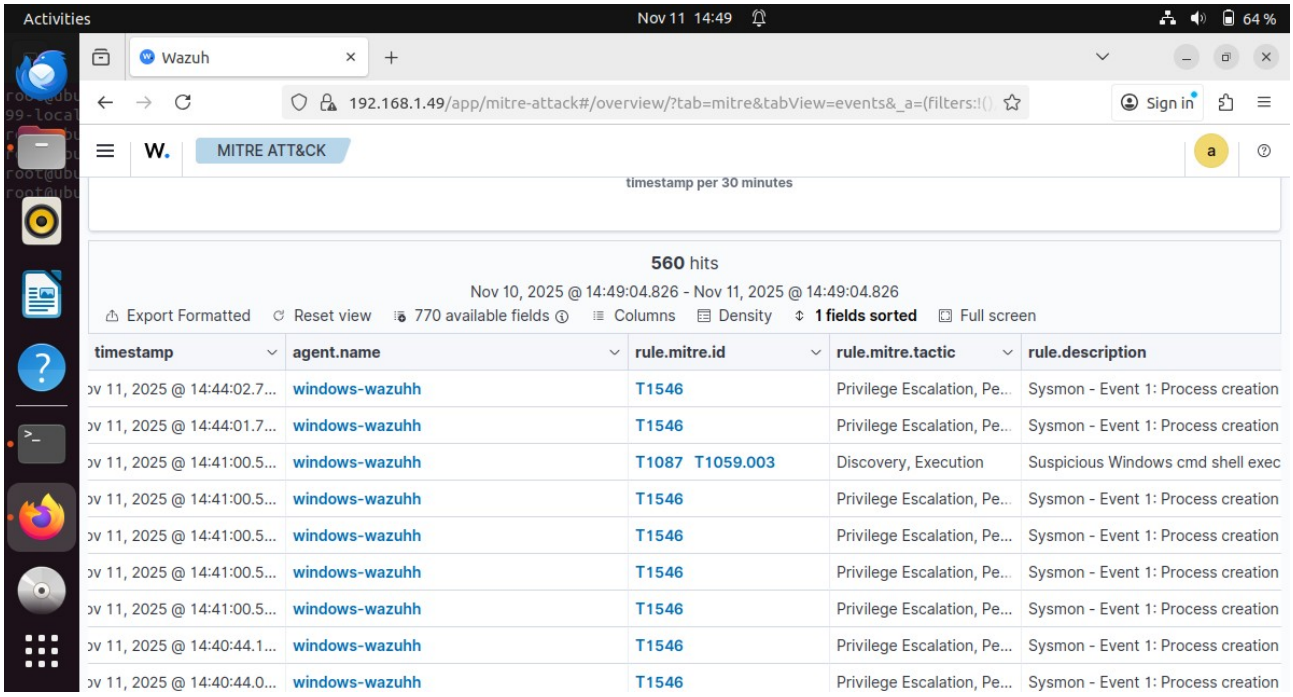
To configure and demonstrate a custom Wazuh detection rule that monitors Sysmon process creation events (Event ID 1) to identify adversarial event-triggered execution techniques (MITRE ATT&CK T1546). This enables early detection of attacker persistence methods leveraging process creation on Windows endpoints.

Goal:

The goal is to enhance security monitoring by integrating Sysmon logs with Wazuh, creating a targeted detection rule, and validating its effectiveness by generating real process creation events using a custom C program. This showcases the practical application of MITRE ATT&CK mappings for threat detection and response.

Before Triggering alert:

Now, check the Wazuh manager for the alert that occurred before the trigger, with the timestamp 14:44.



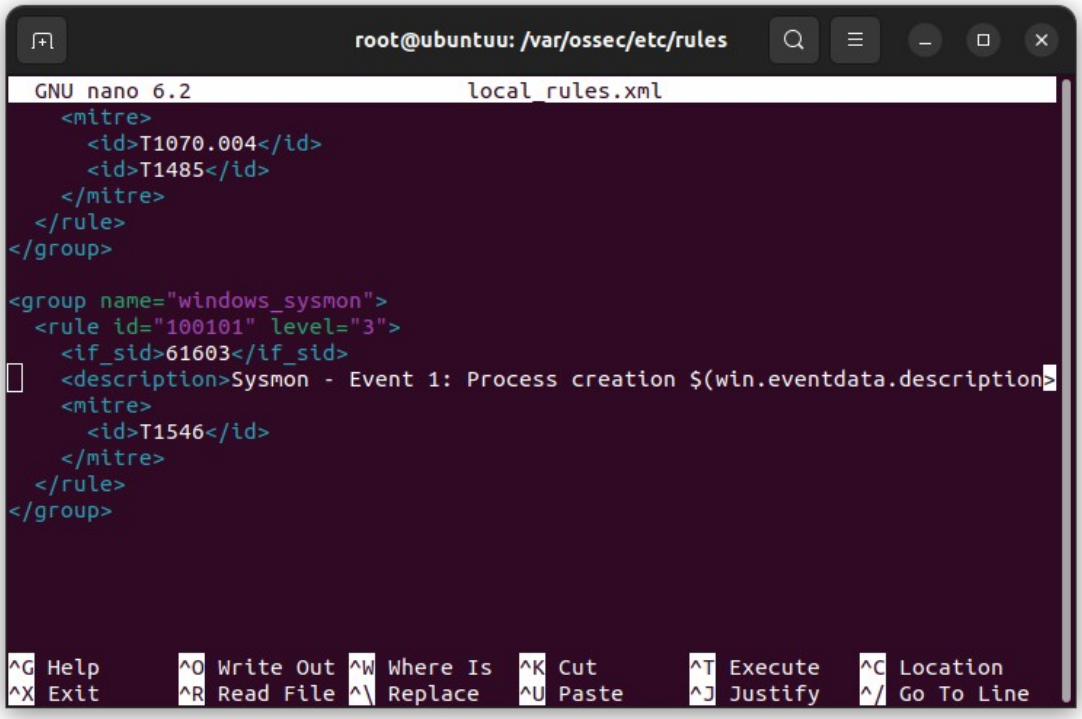
Steps to Reproduce :

Open this dir on manager --> cd /var/ossec/etc/rules/

$ nano local_rules.xml

Add this rule on the local rules :

```
<group name="windows_sysmon">
  <rule id="100101" level="3">
    <if_sid>61603</if_sid>
    <description>Sysmon - Event 1: Process creation $
(win.eventdata.description>
    <mitre>
      <id>T1546</id>
    </mitre>
  </rule>
</group>
```



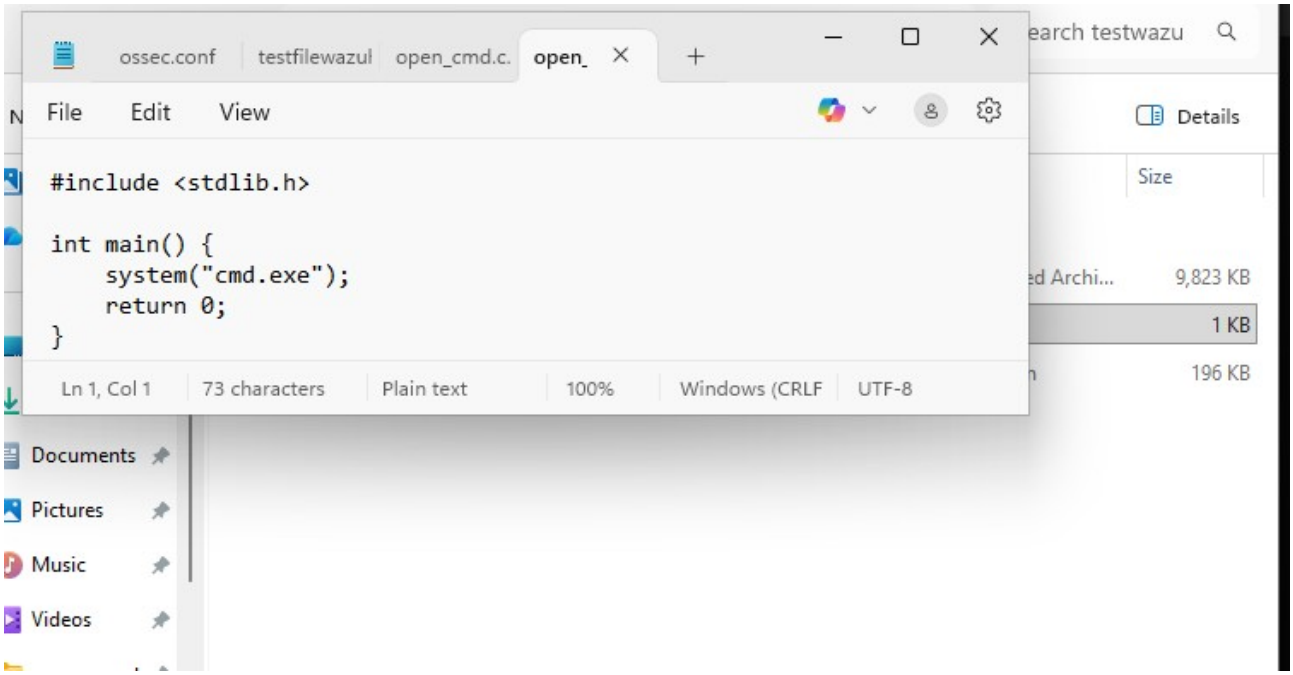
$ systemctl restart wazuh-manager

2) Create a c file on the windows agent :

file name : open_cmd.c

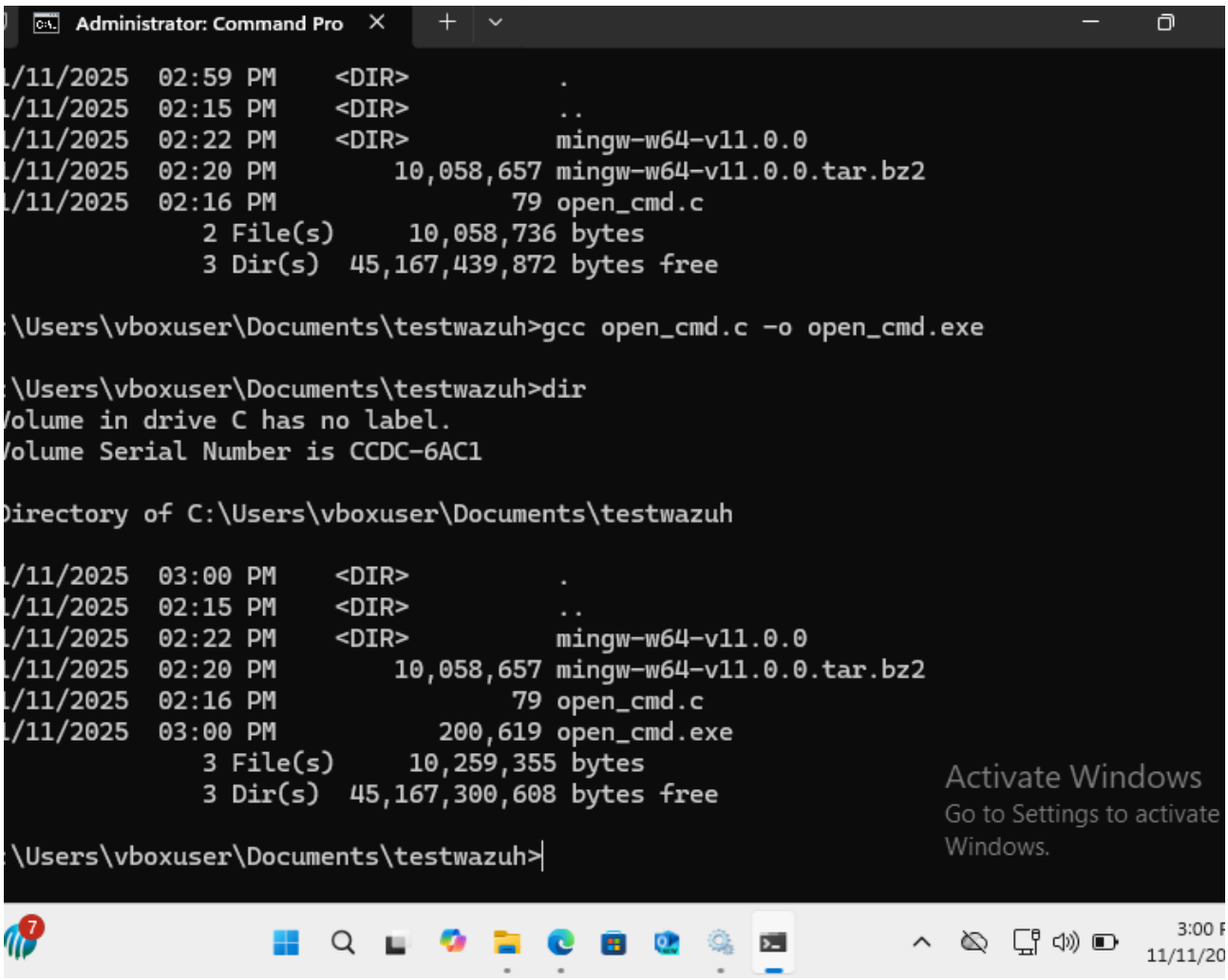
```
#include <stdlib.h>

int main() {
    system("cmd.exe");
    return 0;
```

}



Then compile the open_cmd.c file .

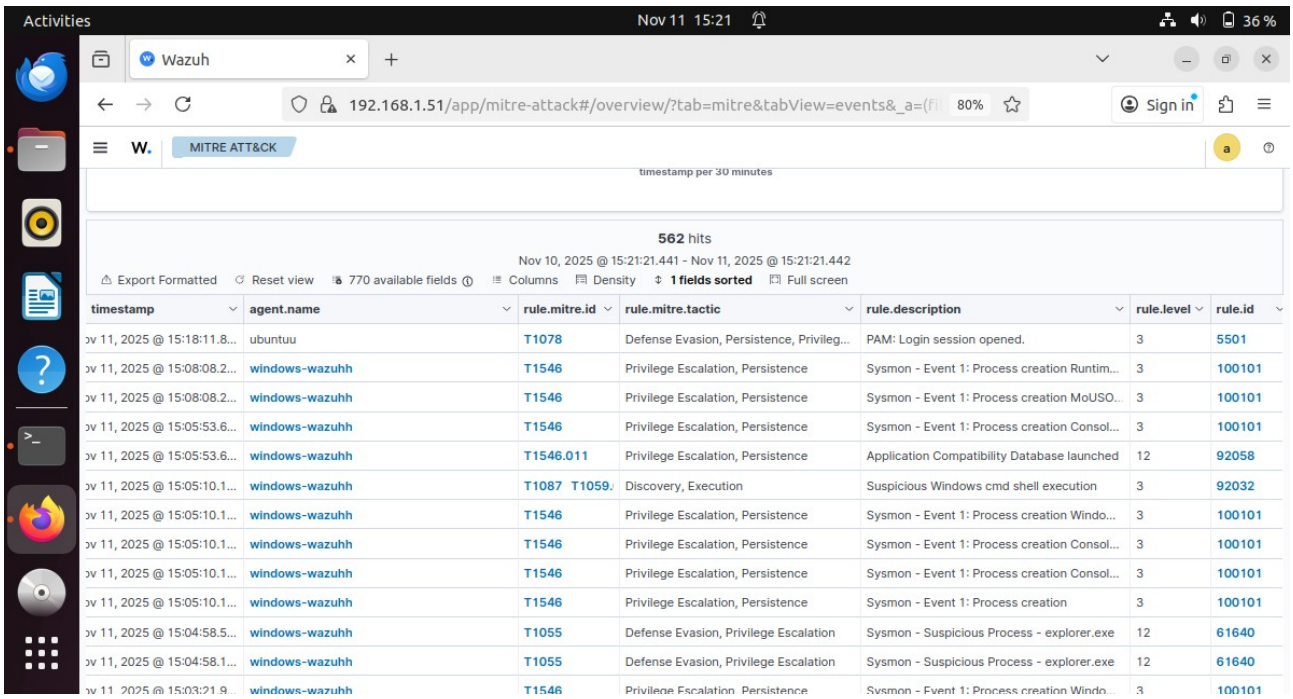
>gcc open_cmd.c -o open_cmd.exe



Now , I run the open_cmd .exe.

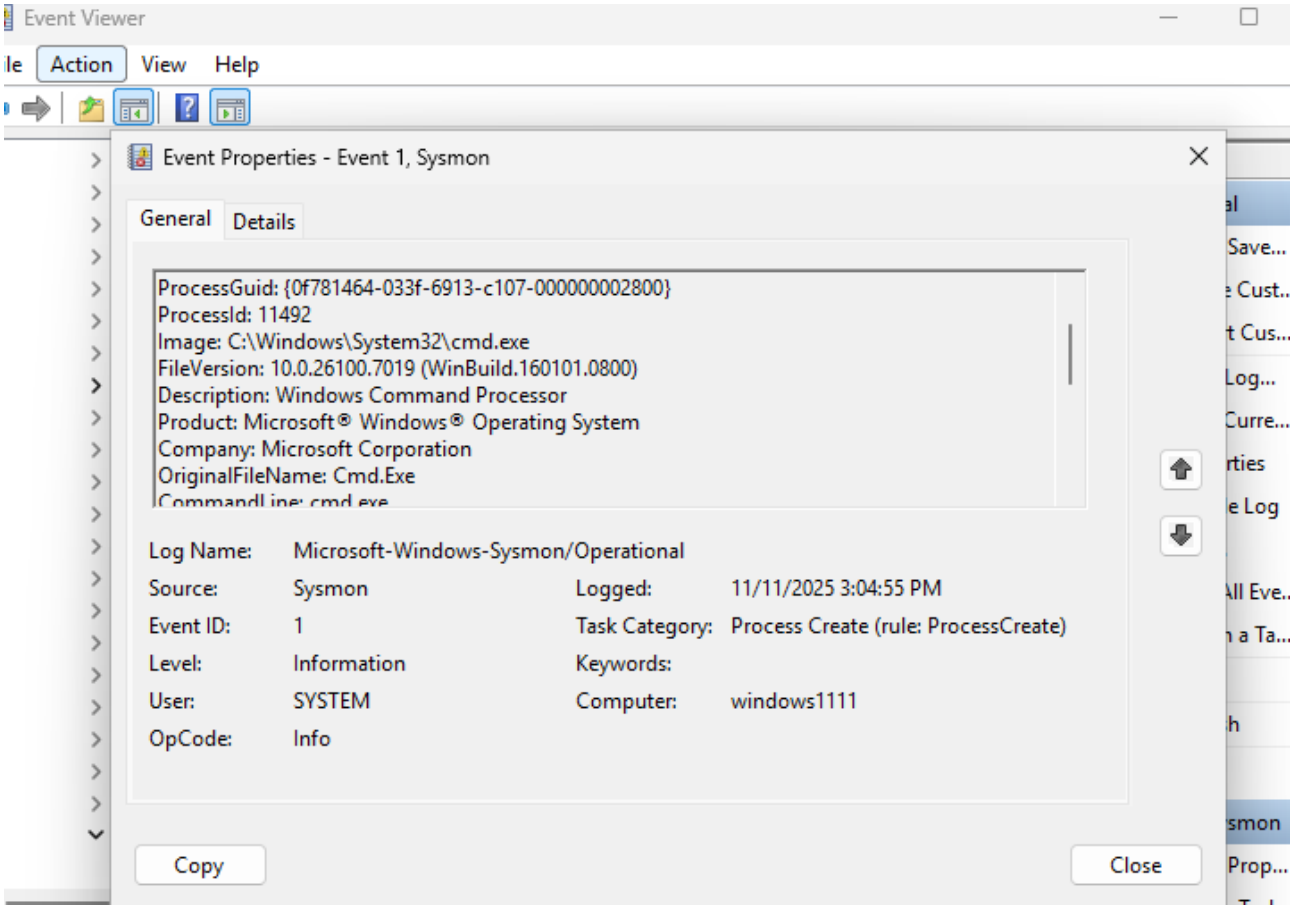
Wazuh manager alert triggered :

Check the alert T1546 in the image below; it is triggered by Sysmon Event 1 (process creation). Then check the timestamp—the alert was triggered at 15:08.



timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.level	rule.id
ov 11, 2025 @ 15:18:11.8...	ubuntuu	T1078	Defense Evasion, Persistence, Privileg...	PAM: Login session opened.	3	5501
ov 11, 2025 @ 15:08:08.2...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Runtim...	3	100101
ov 11, 2025 @ 15:08:08.2...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation MoUSO...	3	100101
ov 11, 2025 @ 15:05:53.6...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Consol...	3	100101
ov 11, 2025 @ 15:05:53.6...	windows-wazuhh	T1546.011	Privilege Escalation, Persistence	Application Compatibility Database launched	12	92058
ov 11, 2025 @ 15:05:10.1...	windows-wazuhh	T1087 T1059.	Discovery, Execution	Suspicious Windows cmd shell execution	3	92032
ov 11, 2025 @ 15:05:10.1...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Windo...	3	100101
ov 11, 2025 @ 15:05:10.1...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Consol...	3	100101
ov 11, 2025 @ 15:05:10.1...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Consol...	3	100101
ov 11, 2025 @ 15:05:10.1...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation	3	100101
ov 11, 2025 @ 15:04:58.5...	windows-wazuhh	T1055	Defense Evasion, Privilege Escalation	Sysmon - Suspicious Process - explorer.exe	12	61640
ov 11, 2025 @ 15:04:58.1...	windows-wazuhh	T1055	Defense Evasion, Privilege Escalation	Sysmon - Suspicious Process - explorer.exe	12	61640
ov 11, 2025 @ 15:03:21.9...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Windo...	3	100101

Win sysmon event :



Result :

The MITRE ATT&CK technique **T1546 (Event Triggered Execution)** was successfully triggered on the Wazuh dashboard based on the execution of a custom C program on the Windows agent. This program created a new process (Command Prompt) representing a process creation event that Sysmon logged.

The custom Wazuh rule monitored Sysmon Event ID 1 (Process Creation) and promptly detected the execution event, raising an alert that correlated the process creation with the MITRE ATT&CK framework technique T1546.