

# **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.

Activities

Nov 11 14:49 64%

Wazuh

MITRE ATT&CK

timestamp per 30 minutes

**560 hits**

Nov 10, 2025 @ 14:49:04.826 - Nov 11, 2025 @ 14:49:04.826

Export Formatted Reset view 770 available fields Columns Density 1 fields sorted Full screen

timestamp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description
Nov 11, 2025 @ 14:44:02.7...	windows-wazuhh	T1546	Privilege Escalation, Pe...	Sysmon - Event 1: Process creation
Nov 11, 2025 @ 14:44:01.7...	windows-wazuhh	T1546	Privilege Escalation, Pe...	Sysmon - Event 1: Process creation
Nov 11, 2025 @ 14:41:00.5...	windows-wazuhh	T1087 T1059.003	Discovery, Execution	Suspicious Windows cmd shell exec
Nov 11, 2025 @ 14:41:00.5...	windows-wazuhh	T1546	Privilege Escalation, Pe...	Sysmon - Event 1: Process creation
Nov 11, 2025 @ 14:41:00.5...	windows-wazuhh	T1546	Privilege Escalation, Pe...	Sysmon - Event 1: Process creation
Nov 11, 2025 @ 14:41:00.5...	windows-wazuhh	T1546	Privilege Escalation, Pe...	Sysmon - Event 1: Process creation
Nov 11, 2025 @ 14:40:44.1...	windows-wazuhh	T1546	Privilege Escalation, Pe...	Sysmon - Event 1: Process creation
Nov 11, 2025 @ 14:40:44.0...	windows-wazuhh	T1546	Privilege Escalation, Pe...	Sysmon - Event 1: Process creation

## 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 $</description>
    <win.eventdata.description>
      <mitre>
        <id>T1546</id>
      </mitre>
    </win.eventdata.description>
  </rule>
</group>
```

The screenshot shows a terminal window with the title bar "root@ubuntuu: /var/ossec/etc/rules". The window contains the content of the file "local\_rules.xml" which is being edited with the nano text editor. The XML code includes sections for MITRE rules and a group for Windows Sysmon events.

```
GNU nano 6.2          local_rules.xml
<mitre>
  <id>T1070.004</id>
  <id>T1485</id>
</mitre>
</rule>
</group>

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

At the bottom of the terminal window, there is a menu bar with various keyboard shortcuts:

- ^G Help
- ^O Write Out
- ^W Where Is
- ^K Cut
- ^T Execute
- ^C Location
- ^X Exit
- ^R Read File
- ^| Replace
- ^U Paste
- ^J Justify
- ^/ Go To Line

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

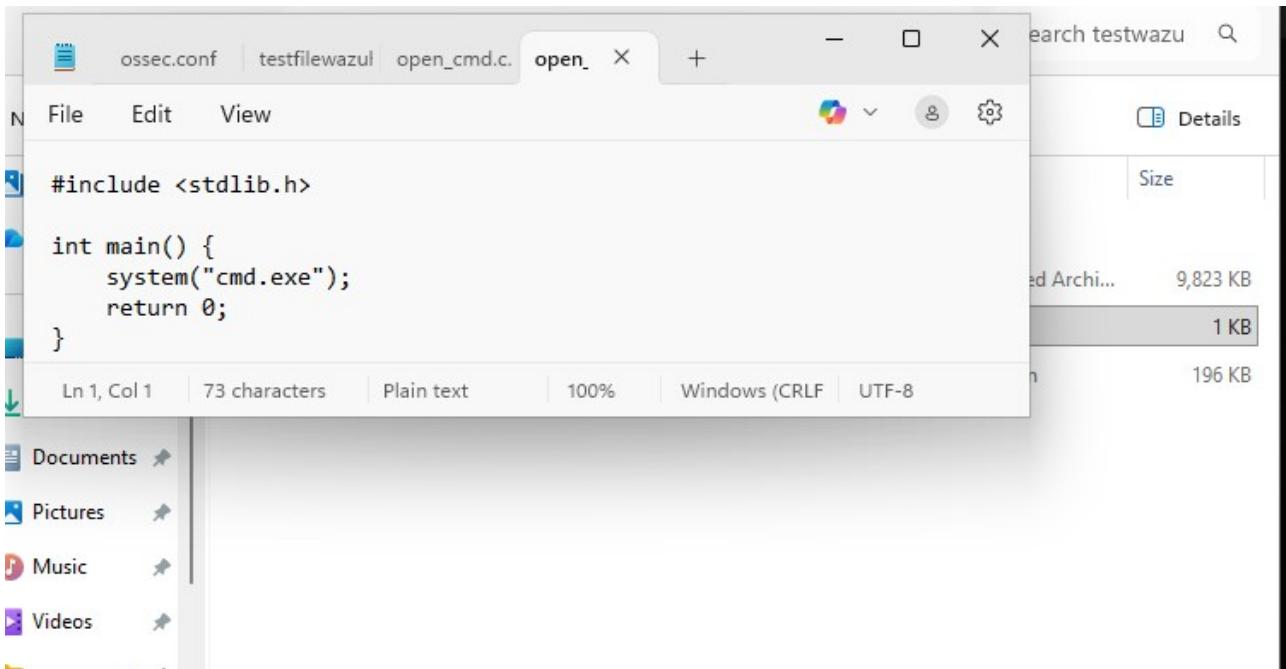
## 2) Create a c file on the windows agent :

**file name : open\_cmd.c**

```
#include <stdlib.h>
```

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

}



```
#include <stdlib.h>

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

The screenshot shows a file editor window with the file "open\_cmd.c" selected. The code in the editor is:

```
#include <stdlib.h>

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

The status bar at the bottom indicates 73 characters, 100% zoom, Windows (CRLF), and UTF-8 encoding.

Then compile the open\_cmd.c file .

```
>gcc open_cmd.c -o open_cmd.exe
```

```
Administrator: Command Pro + ▾
```

```
1/11/2025 02:59 PM <DIR> .
1/11/2025 02:15 PM <DIR> ..
1/11/2025 02:22 PM <DIR> mingw-w64-v11.0.0
1/11/2025 02:20 PM 10,058,657 mingw-w64-v11.0.0.tar.bz2
1/11/2025 02:16 PM 79 open_cmd.c
2 File(s) 10,058,736 bytes
3 Dir(s) 45,167,439,872 bytes free

\Users\vboxuser\Documents\testwazuh>gcc open_cmd.c -o open_cmd.exe

\Users\vboxuser\Documents\testwazuh>dir
Volume in drive C has no label.
Volume Serial Number is CCDC-6AC1

Directory of C:\Users\vboxuser\Documents\testwazuh

1/11/2025 03:00 PM <DIR> .
1/11/2025 02:15 PM <DIR> ..
1/11/2025 02:22 PM <DIR> mingw-w64-v11.0.0
1/11/2025 02:20 PM 10,058,657 mingw-w64-v11.0.0.tar.bz2
1/11/2025 02:16 PM 79 open_cmd.c
1/11/2025 03:00 PM 200,619 open_cmd.exe
3 File(s) 10,259,355 bytes
3 Dir(s) 45,167,300,608 bytes free

\Users\vboxuser\Documents\testwazuh>
```

Activate Windows  
Go to Settings to activate Windows.



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.

Activities Nov 11 15:21 36%

Wazuh - 192.168.1.51/app/mitre-attack#/overview/?tab=mitre&tabView=events&\_a=(fi) 80% Sign in

W. MITRE ATT&CK timestamp per 30 minutes

**562 hits**  
Nov 10, 2025 @ 15:21:21.441 - Nov 11, 2025 @ 15:21:21.442

Export Formatted Reset view 770 available fields Columns Density 1 fields sorted Full screen

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

## Win sysmon event :

Event Viewer

Action View Help

Event Properties - Event 1, Sysmon

General Details

ProcessGuid: {0f781464-033f-6913-c107-000000002800}  
 ProcessId: 11492  
 Image: C:\Windows\System32\cmd.exe  
 FileVersion: 10.0.26100.7019 (WinBuild.160101.0800)  
 Description: Windows Command Processor  
 Product: Microsoft® Windows® Operating System  
 Company: Microsoft Corporation  
 OriginalFileName: Cmd.Exe  
 CommandLine: cmd.exe

Log Name: Microsoft-Windows-Sysmon/Operational  
 Source: Sysmon Logged: 11/11/2025 3:04:55 PM  
 Event ID: 1 Task Category: Process Create (rule: ProcessCreate)  
 Level: Information Keywords:  
 User: SYSTEM Computer: windows1111  
 OpCode: Info

Copy Close

## **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.