Indicator Removal on Host (MITRE ATT&CK Technique T1070):Detecting Defense Evasion via Artifact Deletion and Manipulation

Objective :

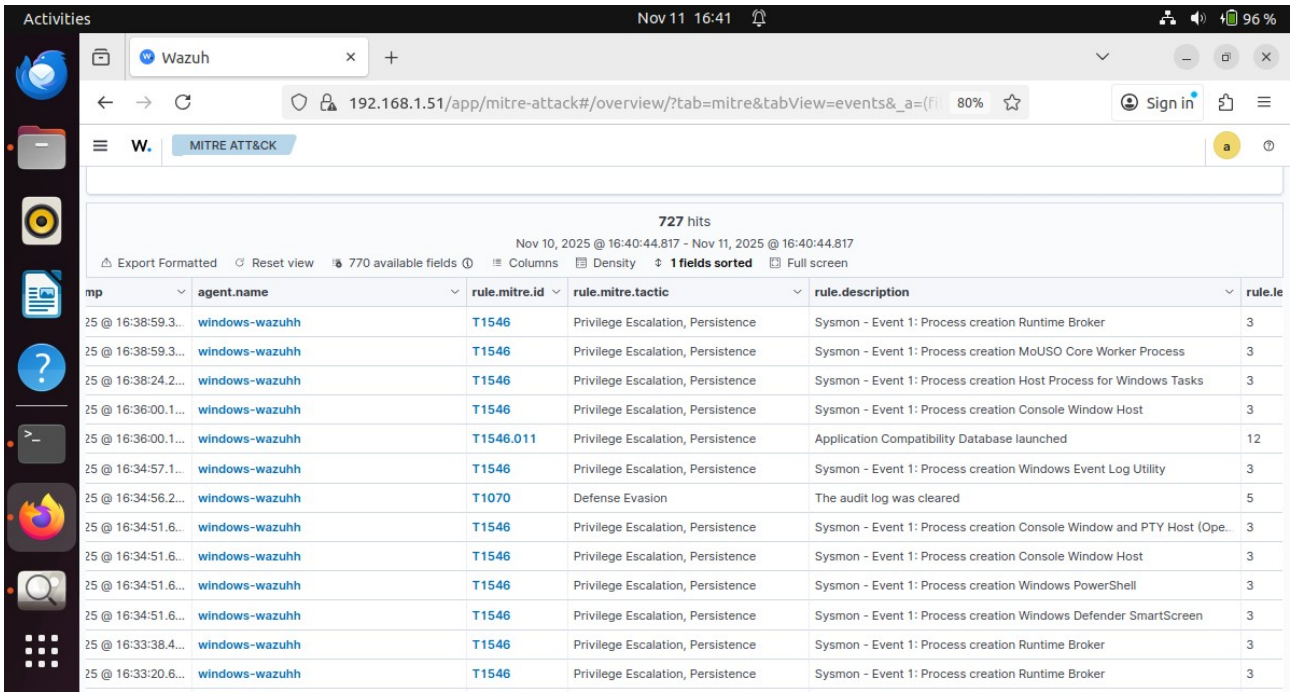
To detect and analyze adversary behaviors involving the deletion or modification of host-based indicators, such as logs, files, or registry keys, which are used to remove evidence of malicious activities and evade detection.

Goal:

The goal is to configure and validate detection rules using Wazuh and Sysmon that monitor process creation events indicative of indicator removal activities. This facilitates early identification of defense evasion attempts, enabling timely incident response and improving overall security posture.

Before Trigger alert in wazuh manager:

Check if the timestamp for this alert is 16:34.



mp	agent.name	rule.mitre.id	rule.mitre.tactic	rule.description	rule.le
25 @ 16:38:59.3...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Runtime Broker	3
25 @ 16:38:59.3...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation MoUSO Core Worker Process	3
25 @ 16:38:24.2...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Host Process for Windows Tasks	3
25 @ 16:36:00.1...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Console Window Host	3
25 @ 16:36:00.1...	windows-wazuhh	T1546.011	Privilege Escalation, Persistence	Application Compatibility Database launched	12
25 @ 16:34:57.1...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Windows Event Log Utility	3
25 @ 16:34:56.2...	windows-wazuhh	T1070	Defense Evasion	The audit log was cleared	5
25 @ 16:34:51.6...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Console Window and PTY Host (Ope...	3
25 @ 16:34:51.6...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Console Window Host	3
25 @ 16:34:51.6...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Windows PowerShell	3
25 @ 16:34:51.6...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Windows Defender SmartScreen	3
25 @ 16:33:38.4...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Runtime Broker	3
25 @ 16:33:20.6...	windows-wazuhh	T1546	Privilege Escalation, Persistence	Sysmon - Event 1: Process creation Runtime Broker	3

Steps to Reproduce :

1) Open this dir on wazuh manger , create a rule :

$ cd /var/ossec/etc/rules

$ nano local_rules.xml

Add the rule on the below code on local rules .xml

<rule id="100103" level="3">

<if_sid>100100</if_sid>

<field

name="win.eventdata.ruleName">^technique_id=T1070,technique_name=Indicator Removal on Host$</field>

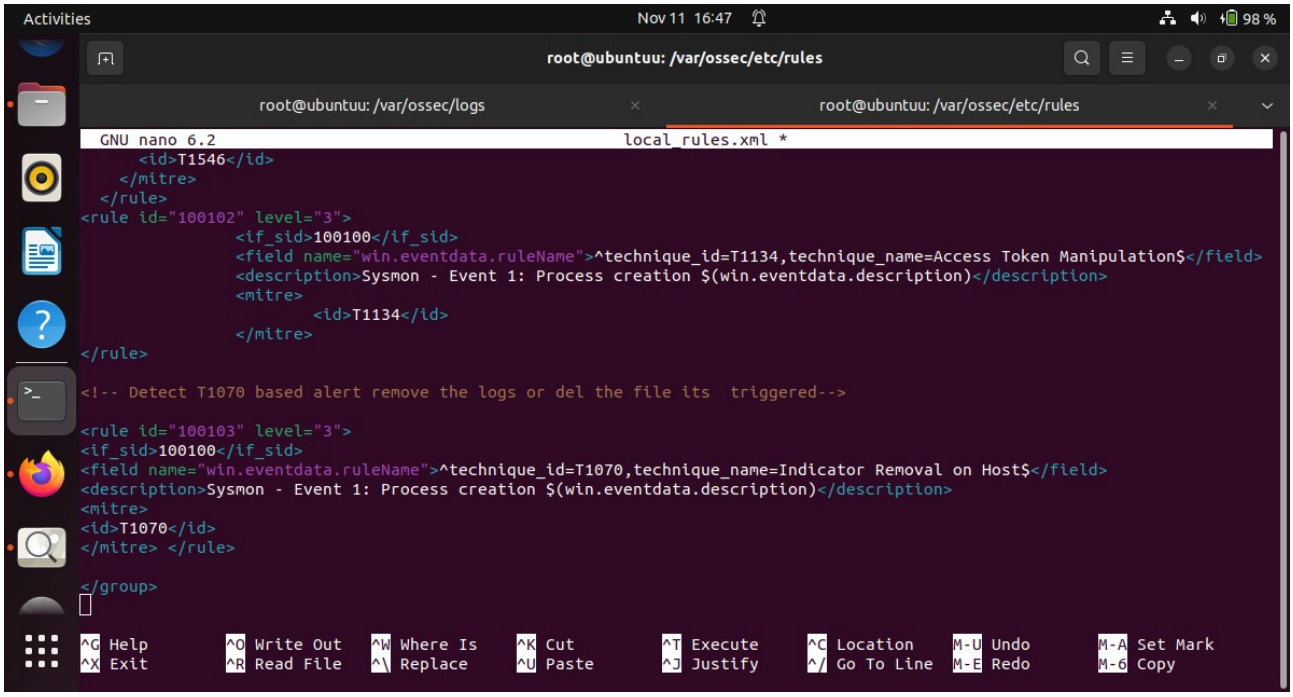
<description>Sysmon - Event 1: Process creation $

(win.eventdata.description)</description>

<mitre>

<id>T1070</id>

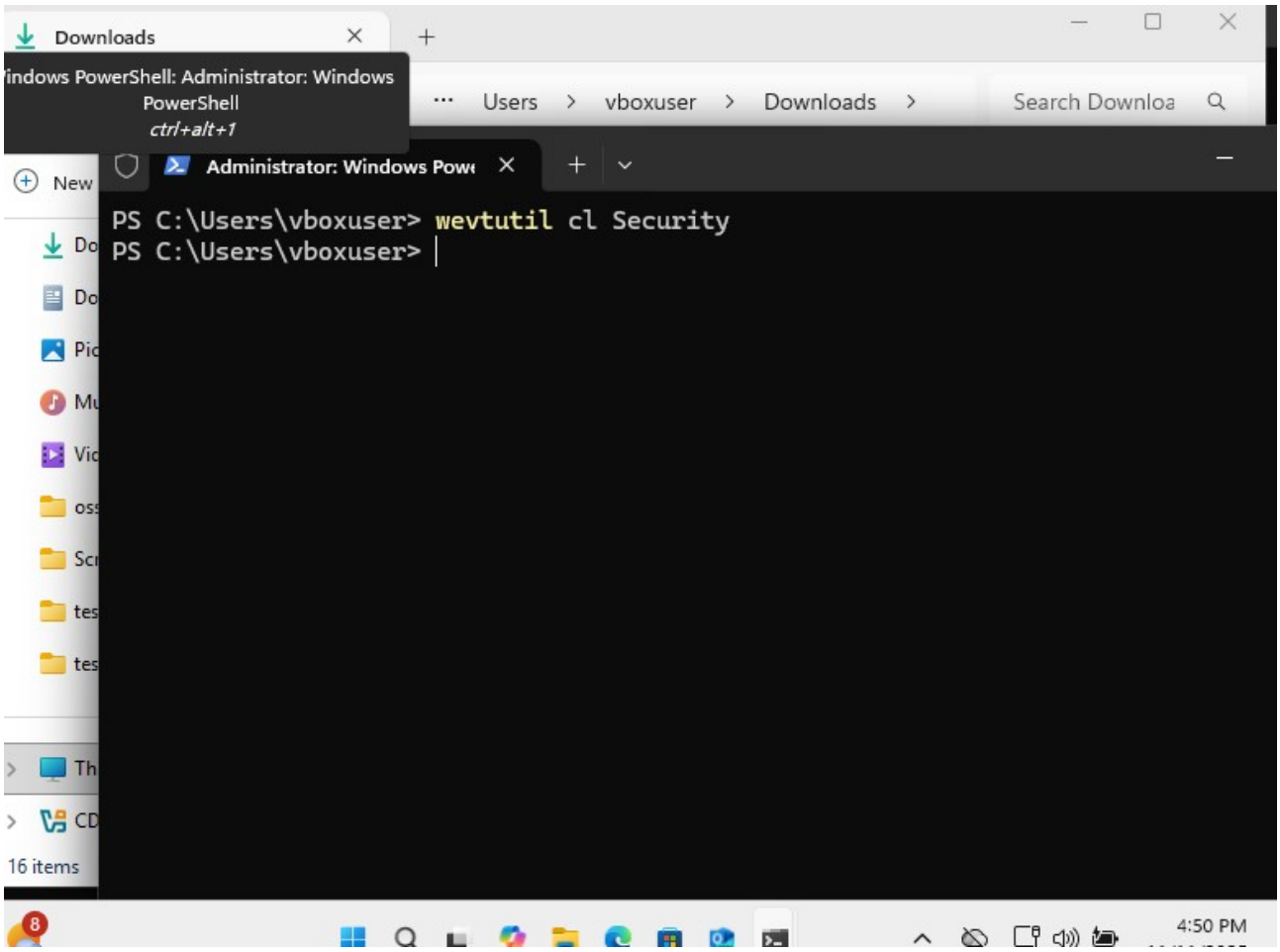
</mitre> </rule>



$ systemctl restart wazuh-manager

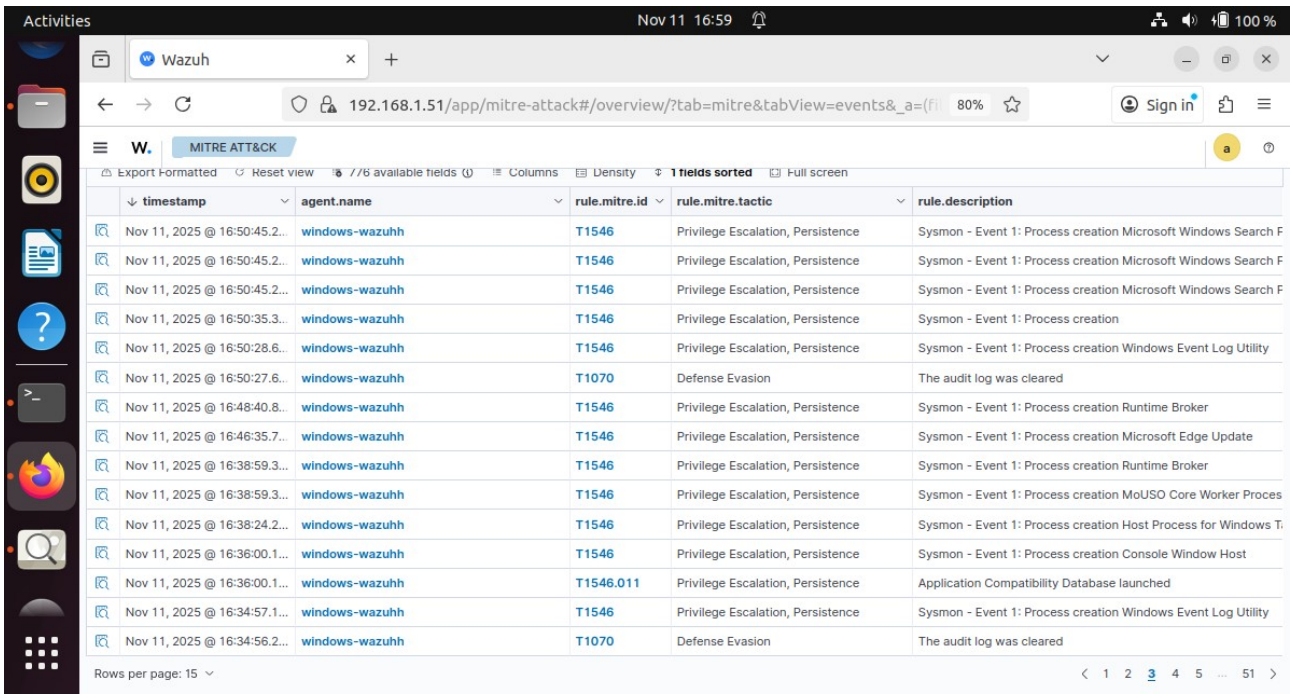
windows agent :

> wevtutil cl Security



Wazuh manager triggered alert :

Check the below image , alert was triggered the timestamp is 16:50 (Defense evation) The audit log was cleared.



Result :

During the testing, the audit log clearing activity was successfully detected and displayed on the Wazuh dashboard. The alert triggered by the custom rule monitoring Sysmon Event ID 1 captured the process creation event associated with the deletion or clearing of audit logs (Indicator Removal on Host – MITRE T1070).

The Wazuh dashboard showed details including the timestamp, the cleared audit log action, and relevant contextual information, confirming the effective detection of defense evasion techniques on the monitored Windows agent.