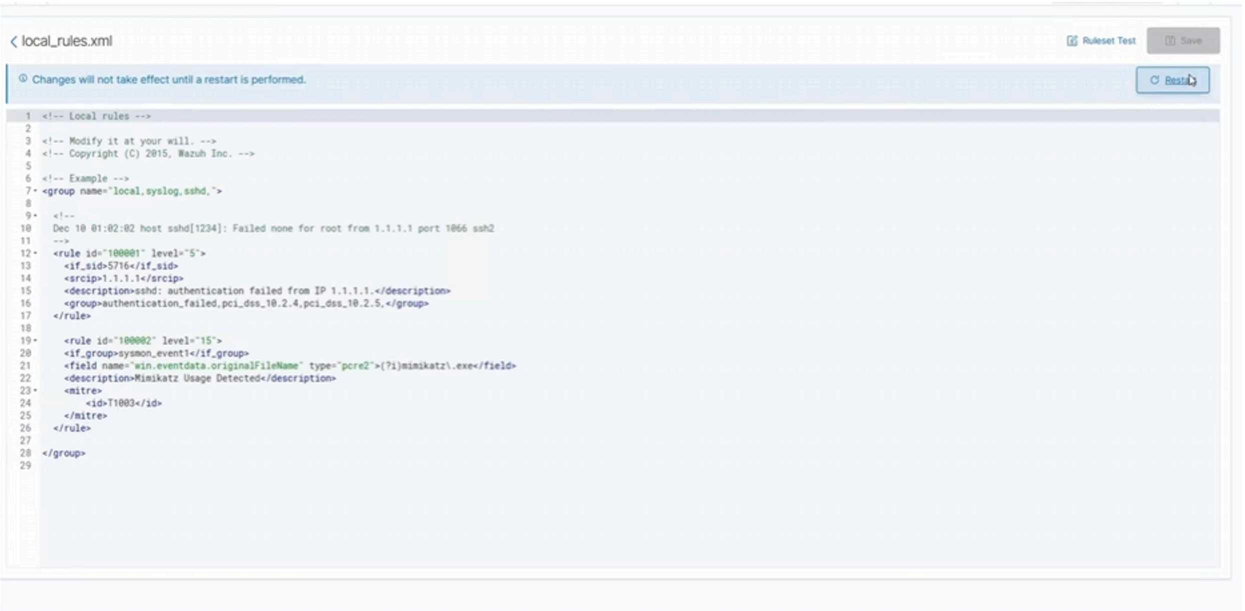
7. Mimikatz Custom Detection Rule (Detailed Explanation)

Goal

Create a detection rule in Wazuh that alerts the analyst when the credential-harvesting tool **Mimikatz** is executed on the Windows 11 endpoint.



< local_rules.xml

Changes will not take effect until a restart is performed.

```
<!-- Local rules -->

<!-- Modify it at your will. -->
<!-- Copyright (C) 2015, Wazuh Inc. -->

<!-- Example -->
<group name="local,syslog,sshd,">

  <!--
  Dec 10 01:02:02 host sshd[1234]: Failed none for root from 1.1.1.1 port 1066 ssh2
  -->
  <rule id="100001" level="5">
    <if_sid>5716</if_sid>
    <srcip>1.1.1.1</srcip>
    <description>sshd: authentication failed from IP 1.1.1.1.</description>
    <group>authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,</group>
  </rule>

    <rule id="100002" level="15">
    <if_group>sysmon_event1</if_group>
    <field name="win.eventdata.originalFileName" type="pcre2">(?i)mimikatz\.exe</field>
    <description>Mimikatz Usage Detected</description>
    <mitre>
        <id>T1003</id>
    </mitre>
  </rule>

</group>

```

(Detection Rule)

What is Mimikatz? (Add This to Documentation)

Mimikatz is a well-known **post-exploitation** tool used by penetration testers and adversaries to:

- Extract plaintext passwords from memory
- Dump hashed passwords (NTLM hashes)
- Steal Kerberos tickets (Pass-the-Ticket attacks)
- Perform Pass-the-Hash attacks

- Elevate privileges (Token manipulation)

Mimikatz is widely used by threat actors and is associated with multiple advanced persistent threat (APT) groups.
Because of its widespread abuse, detection of Mimikatz execution is essential in any SOC environment.

MITRE ATT&CK Technique:
Credential Dumping — **T1003**

Why Sysmon Detects It (Analyst Explanation)

Sysmon Event ID **1** logs *process creation*.
When Mimikatz runs, Sysmon logs:

- Process name
- Original file name
- Command line arguments
- Process ID
- Parent process
- Hashes (SHA1, SHA256, MD5)

Even if the attacker renames the binary, Sysmon often still records the **OriginalFileName** metadata from the PE header, which remains `mimikatz.exe`.

This makes the detection rule **highly reliable**.

Steps to Create the Detection Rule

1. Open the local Wazuh rules file

On the Wazuh Manager VM:

File location:
/var/ossec/etc/rules/local_rules.xml

Open with a text editor:

```
sudo nano /var/ossec/etc/rules/local_rules.xml
```

---

2. Add the custom Mimikatz detection rule

Paste-Ready Rule Description to Include in Google Docs:

- **Group:** windows, sysmon
- **Rule ID:** 1000002
- **Trigger:** Sysmon Event ID 1 (process creation)
- **Field Match:** originalFileName = mimikatz.exe
- **Description:** “Mimikatz usage detected”
- **MITRE Mapping:** Credential Access → T1003

Full Rule Logic (Text Only for Google Docs):

```
<rule id="1000002" level="10"> <if_sid>61602</if_sid> <field
name="sysmon.process.originalFileName">mimikatz.exe</field> <description>Mimikatz usage
detected</description> <mitre> <id>T1003</id> </mitre> </rule>
```

Explanation (include in Doc):
• **61602** is the Sysmon parent SID for Event ID 1 (Process Create).
• The rule looks for the **OriginalFileName** metadata inside the PE header.
• Even if the attacker renames the binary (e.g., `mimi.exe`), Sysmon often still reports the true original file name.
• Severity level **10** categorizes this as a critical credential-access alert.

---

3. Restart the Wazuh Manager

Restart Command (Google Doc friendly):

sudo systemctl restart wazuh-manager

This reloads the updated rule set.

---

4. Test the Rule (Execution in Windows VM)

Steps:

1. Disable Microsoft Defender (temporarily for lab use).
2. Download and extract Mimikatz.
3. Run from PowerShell:
   .\mimikatz.exe
4. Generate telemetry: Sysmon logs Event ID 1.
5. Wazuh receives and analyzes the event.
6. The custom rule fires and creates an alert.

---

5. Expected Result in Wazuh Dashboard

Open Wazuh → Alerts → Search:

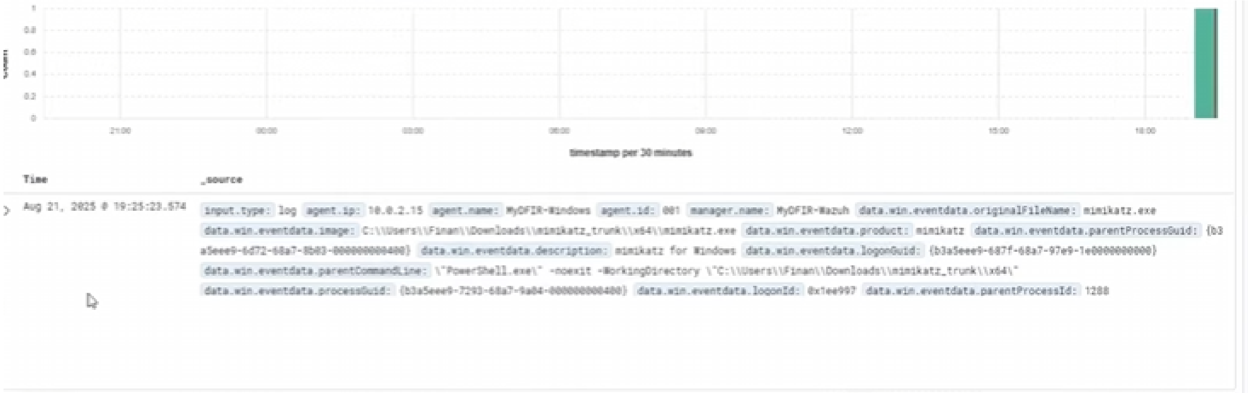
mimikatz
or
rule.id: 1000002

You should see:

Alert: “Mimikatz usage detected”
Severity: 10
Technique: MITRE T1003
Source Host: Windows 11 VM
Event Source: Sysmon Event ID 1 (Process Create)

The alert should display:

- Process path
- Parent process (often PowerShell)
- SHA256 hash
- User account executing the binary
- Timestamp



```
Time                       _source
Aug 21, 2025 @ 19:25:23.574  input.type: log agent.ip: 10.0.2.15 agent.name: MyDFIR-Windows agent.id: 001 manager.name: MyDFIR-Wazuh data.win.eventdata.originalFileName: mimikatz.exe
data.win.eventdata.image: C:\\Users\\Finan\\Downloads\\mimikatz_trunk\\x64\\mimikatz.exe data.win.eventdata.product: mimikatz data.win.eventdata.parentProcessGuid: {b3
a5eee9-6d72-68a7-8b03-000000000400} data.win.eventdata.description: mimikatz for Windows data.win.eventdata.logonGuid: {b3a5eee9-687f-68a7-97e9-1e0000000000}
data.win.eventdata.parentCommandLine: \"PowerShell.exe\" -noexit -WorkingDirectory \"C:\\Users\\Finan\\Downloads\\mimikatz_trunk\\x64\"
data.win.eventdata.processGuid: {b3a5eee9-7293-68a7-9a04-000000000400} data.win.eventdata.logonId: 0x1ee997 data.win.eventdata.parentProcessId: 1288
```

(generated rule)