🔍 Detecting Suspicious Tools on Windows Endpoints with Wazuh

📌 Objective

Demonstrate how **Wazuh** can detect the execution of suspicious tools (like `ncat.exe`, `mimikatz.exe`, or `psexec.exe`) on a Windows endpoint using **process monitoring**.

🛠️ Setup

- **Wazuh Manager**: Running in VMware
- **Wazuh Agent**: Windows 10
- **Monitored Command**: `tasklist.exe` (lists running processes).
- **Detection Method**: Wazuh rules to trigger alerts when suspicious binaries appear in the process list.

⚙️ Configuration

1. **Configure Wazuh Agent (Windows)**

On the Windows agent, edit `ossec.conf` to collect process list output:

Wazuh agent configuration file **(**`ossec.conf`**)**is located in:

```
C:\Program Files\ossec-agent\ossec.conf
#To collect the process list (tasklist.exe), you would edit `ossec.conf` and add inside the <ossec_config> block:
<localfile>
 <log_format>command</log_format>
 <command>C:\Windows\System32\tasklist.exe</command>
 <frequency>60</frequency>
</localfile>
```

Steps:

1. Open Notepad (as Administrator).
2. Navigate to the path above and open `ossec.conf`.
3. Add the `<localfile>...</localfile>` section inside `<ossec_config>...</ossec_config>`.
4. Save the file.
5. Restart the Wazuh agent service from **Services.msc** or by running in CMD (as Administrator)

2. Configure Wazuh Manager (Rules)

On the Wazuh Manager, edit `local_rules.xml`:

Go to **/var/ossec/etc/rules/local_rules.xml**

Command : **sudo nano ssec/etc/rules/local_rules.xml**

Add -

```
<group name="ossec,">
 <rule id="100010" level="10">
   <decoded_as>ossec</decoded_as>
   <description>Suspicious tool detected in process list</description>
   <match>ncat.exe|mimikatz.exe|psexec.exe|nc.exe</match>
   <group>process_monitor,</group>
 </rule>
</group>
```

✅ This rule raises an **alert with severity level 10** when any of these tool names appear in the process list.

🧪 Simulation

Step 1: Execute a Suspicious Tool

On the Windows agent, simulate an attacker starting a netcat listener:

```
ncat.exe -lvp 4444
```

Step 2: Process Collection

Within 60 seconds, the agent runs `tasklist.exe` and sends output like:

```
ossec: output: 'C:\Windows\System32\tasklist.exe':
ncat.exe                     11196 Console                    1      7,348 K
```

Step 3: Alert Triggered in Wazuh

The manager matches `ncat.exe` with the custom rule and generates an alert:

- **Timestamp**: Aug 26, 2025 @ 19:45:40.353
- **Agent**: Windows 10
- **Process**: ncat.exe
- **Action**: Suspicious process execution
- **Rule ID**: 100010
- **Level**: 10
- **Description**: Suspicious tool detected in process list

📊 Observation

- Wazuh successfully flagged `ncat.exe` as a suspicious process.
- The rule can be extended to detect **other red-team tools** (Mimikatz, PsExec, Cobalt Strike, etc.).
- Alerts appeared in the **Wazuh Dashboard**, making them available for triage and investigation.

🕵️ Detection Use Case

MITRE ATT&CK Techniques:

- **T1059**—Command and Scripting Interpreter
- **T1105**—Ingress Tool Transfer
- **T1057**—Process Discovery

Use Case: Detect unauthorized or suspicious tools running on endpoints.