Adversary Emulation Practice

1. Objective

This report contains the details of the task including Emulation simulation, and Emulation Report. The goal of this task is to:

- Learn imitation of real attacker behavior and reporting of emulation.

2. Introduction

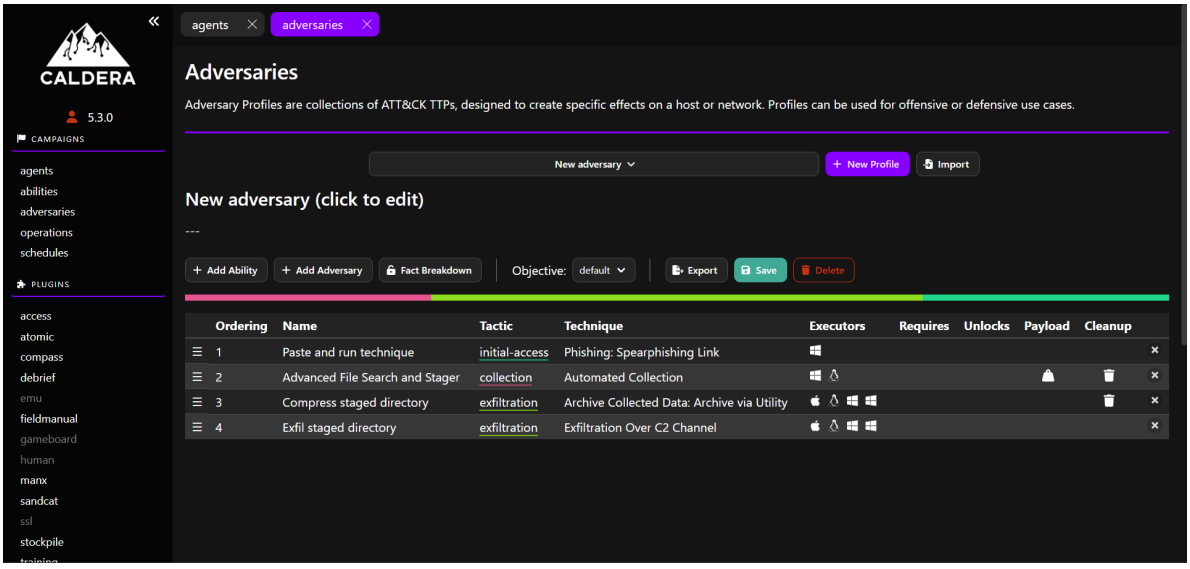
Adversary emulation is a process of imitating real attacker behavior for testing how effectively The defense mechanism of the organization is working. After emulation simulation reporting the emulation to detect the vulnerabilities if found during simulation. This is a better approach for detecting different issues and resolving them before the real threat actor exploit them.

3. Tools

- Wazuh setup using official Wazuh documentation . https://documentation.wazuh.com/current/quickstart.html
- MITRE Caldera https://caldera.readthedocs.io/en/latest/Installing-Caldera.html

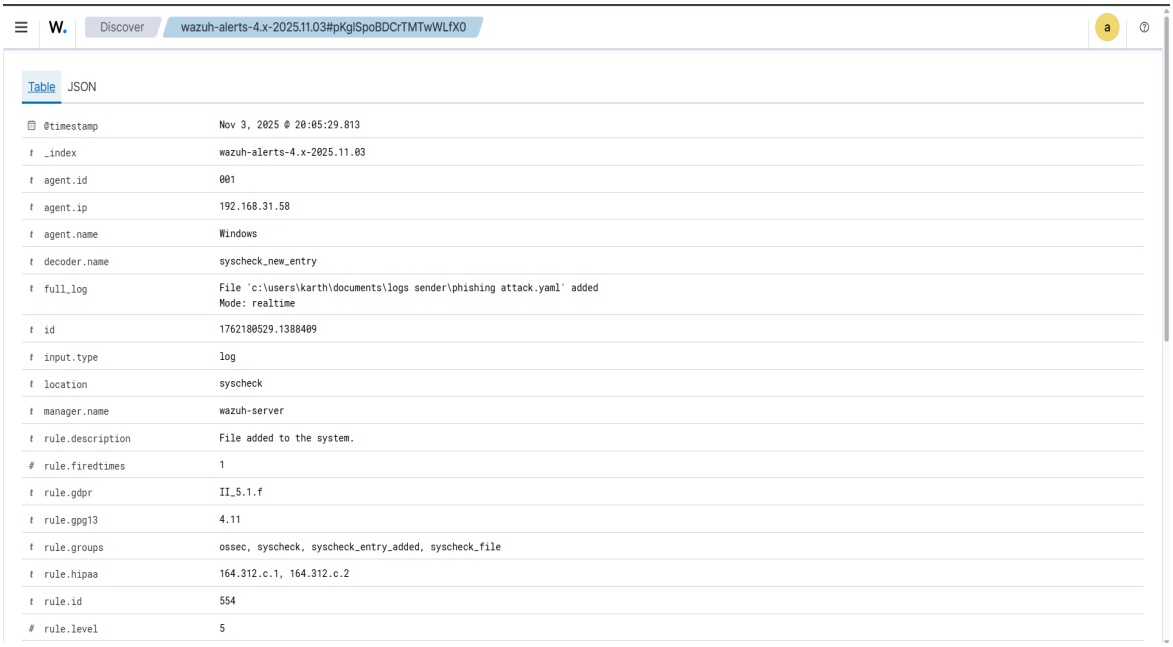
4. Emulation Simulation

Emulation simulation using Caldera which is an emulation simulation tool for simulating a spearphishing attack (T1566). I Configured Wazuh to detect that attack.



4.1 Configuring Wazuh to Detect

I configured Wazuh to detect the simulated attack using Caldera on the Virtual Machine



4.1 Triage Simulation Metadata

The below table contains the metadata of the analysis of a mock alert. It includes Timestamp, TTP, Detection Status, and Notes.

Timestamp	TTP	Detection Status	Notes
2025-08-1817:00:00	T1566	Detected	Phishing email blocked

5. Emulation Report

Emulation report contains the details of the emulation simulation.

Adversary Emulation Report – Spearphishing (T1566)

A spearphishing attack was emulated using MITRE Caldera to evaluate SOC detection capabilities. The simulated phishing email attempted to deliver a malicious payload to the target system. Wazuh successfully detected the event and generated an alert indicating that the phishing attempt was blocked. However, the analysis identified areas for improvement: email

content scanning was limited, attachment behavior was not fully monitored, and lateral movement attempts following the initial compromise were not logged. Additional alert correlation and automated response actions are recommended to strengthen defenses. Overall, the test validated baseline detection but exposed notable gaps in deeper threat monitoring and post-infection visibility.