

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

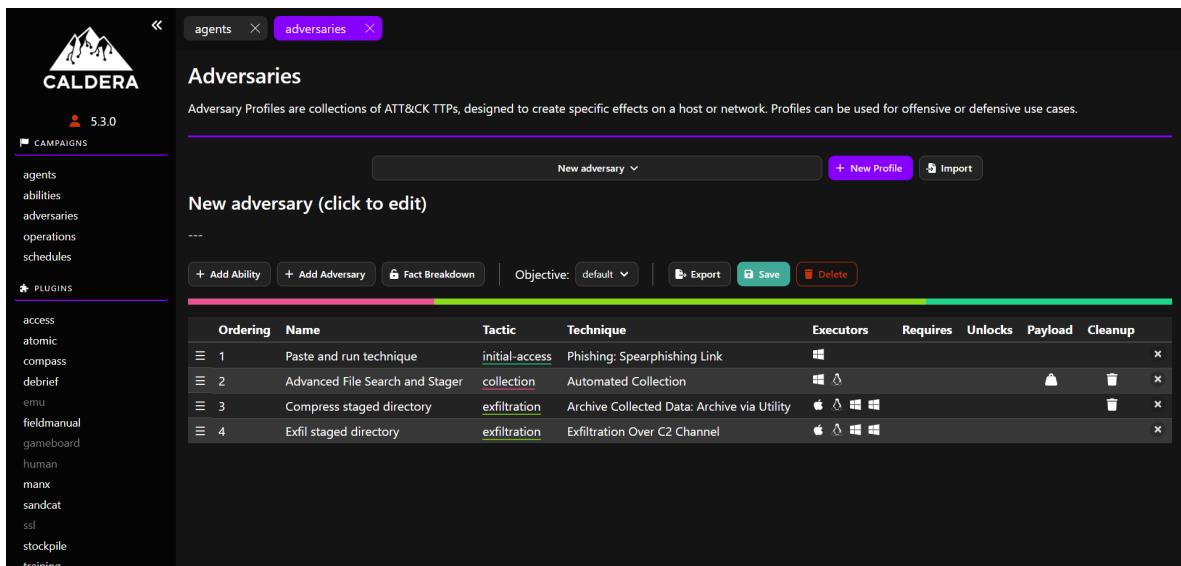
Adversary emulation is a process of imitating real attacker behavior for testing how effectively the defense mechanism of the organization is working. After emulation simulation reporting the emulation to detect the vulnerabilities if found during simulation. This is a better approach for detecting different 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.



Ordering	Name	Tactic	Technique	Executors	Requires	Unlocks	Payload	Cleanup
1	Paste and run technique	initial-access	Phishing: Spearphishing Link	Mac				X
2	Advanced File Search and Stager	collection	Automated Collection	Windows	Mac			X
3	Compress staged directory	exfiltration	Archive Collected Data: Archive via Utility	Mac	Windows	Mac		X
4	Exfil staged directory	exfiltration	Exfiltration Over C2 Channel	Mac	Windows	Mac		X

4.1 Configuring Wazuh to Detect

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

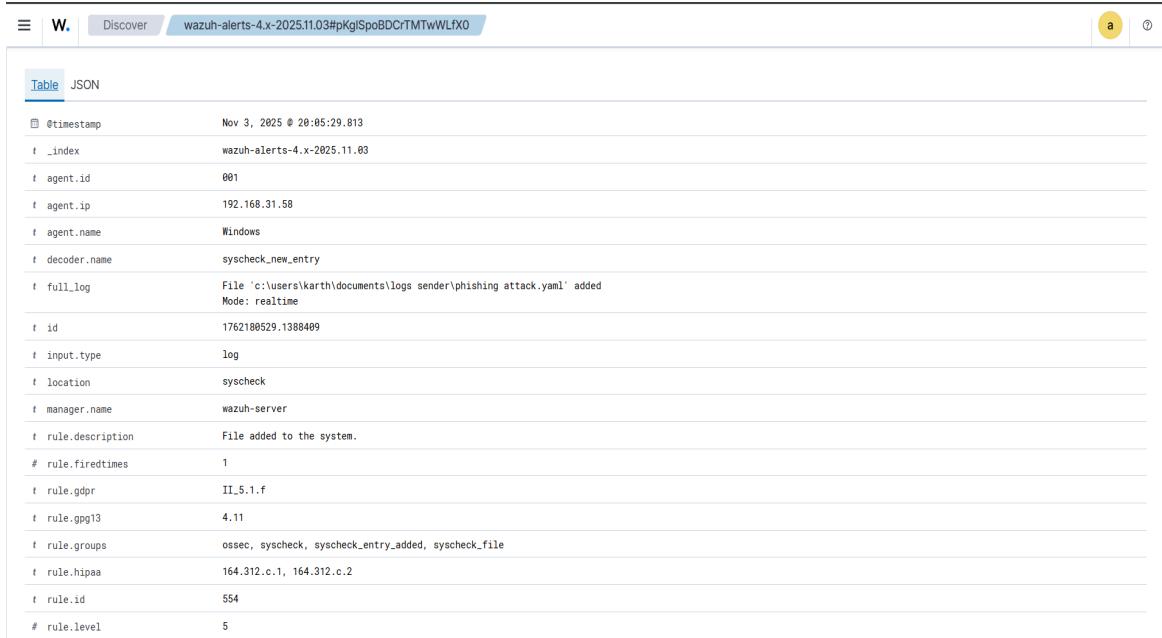


Table JSON	
□ @timestamp	Nov 3, 2025 @ 20:05:29.813
t _index	wazuh-alerts-4.x-2025.11.03
t agent.id	001
t agent.ip	192.168.31.58
t agent.name	Windows
t decoder.name	syscheck_new_entry
t full_log	File 'c:\users\karth\documents\logs\sender\phishing attack.yaml' added Mode: realtime
t id	1762100529.1388409
t input.type	log
t location	syscheck
t manager.name	wazuh-server
t rule.description	File added to the system.
# rule.firetimes	1
t rule.gdpr	II_5.1.f
t rule.gpg13	4.11
t rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_file
t rule.hipaa	164.312.c.1, 164.312.c.2
t rule.id	554
# rule.level	5

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
2025-08-18 17:00:00	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.