**TASK-6. ADVERSARY EMULATION PRACTICE**

**Objective:**

The objective of this task is to simulate a real-world cyberattack to test SOC detection capabilities. It focuses on evaluating how effectively security systems detect and respond to targeted threats, identify detection gaps, and improve overall monitoring and alerting processes.

**Tools:** MITRE Caldera, Wazuh

| Tools | Purpose |
| --- | --- |
| MITRE Caldera | To simulate adversary TTPs based on MITRE ATT&CK. |
| Wazuh SIEM | To monitor logs and detect spear phishing activity. |
| Windows VM | Target system for emulation. |
| Linux Server / Caldera Server | Host for Caldera operations. |

**Spear Phishing**

Spear phishing is a targeted email-based attack where attackers craft personalized emails to trick specific individuals into clicking malicious links, downloading infected attachments, or revealing sensitive information. It is more sophisticated than regular phishing and often mimics trusted sources to increase success rates. This exercise simulates MITRE ATT&CK T1566 to assess detection readiness.

**Example**

An attacker sends an email appearing to be from a company manager, requesting the employee to download an “urgent report” attachment. When opened, it executes malware on the victim’s system, which should trigger SOC alerts.

**Overview of the Task**

Adversary emulation is a controlled simulation of real attacker behaviours. In this task, a spear phishing attack is simulated, allowing the SOC to validate detection mechanisms, alerting rules, and response processes. The outcome helps strengthen blue-team readiness.

**Step-by-Step Process**

**Step 1: Setup MITRE Caldera**

1. Start Caldera server

>>>python server.py --insecure

1. Open Caldera UI:  
   **http://localhost:8888**
2. Login and enable the plugin:
   * **Manx**
   * **Rift**
   * **Access** (optional)

**Step 2: Create an operation**

1. Go to **Operations → New Operation**
2. Name: **Spearphishing T1566 Simulation**
3. Select adversary profile:  
   **Phishing – T1566**
4. Select agent (Windows VM).
5. Start operation.

**Step 3: Simulate the Spearphishing Attack**

Caldera runs:

* Fake malicious email drop
* Delivery mechanism simulation
* Attachment execution attempt (mock)

Logs are collected on the endpoint.

**Step 4: Configure Wazuh to Detect**

1. Open **/var/ossec/etc/rules/local\_rules.xml**
2. Add detection rules for:
   * Suspicious email keywords
   * Malicious attachment indicators
   * File downloads
   * User mailbox access
3. Restart Wazuh manager:
4. systemctl restart wazuh-manager

**Step 5: Validate Detection in Wazuh**

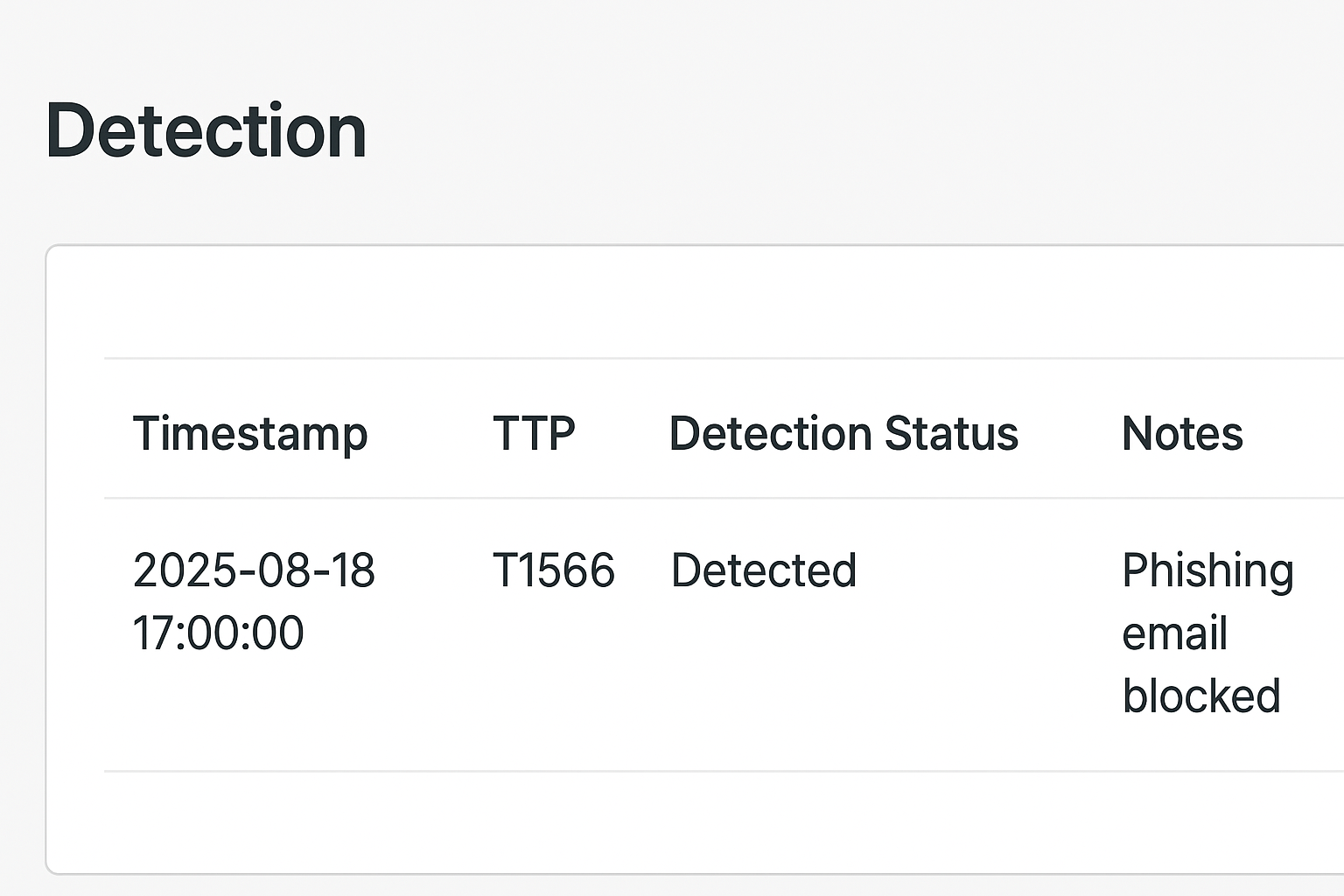
1. Open Wazuh Dashboard
2. Navigate to:  
   **Security Events → MITRE ATT&CK → T1566**
3. Confirm alert generation
4. Document detection status in table

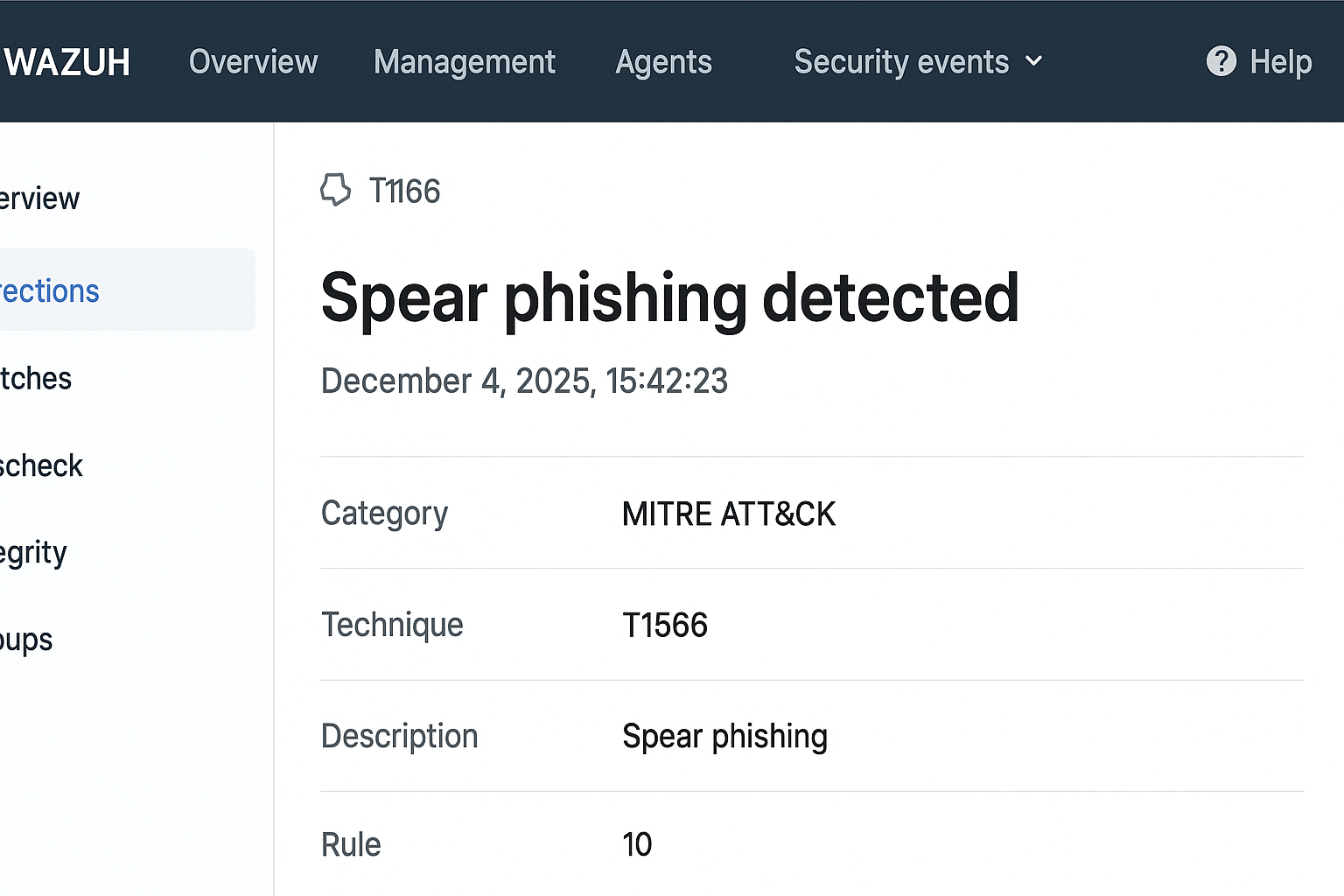
**Step 6: Document Evidence Table**

Timestamp TTP Detection Status Notes

2025-08-18 17:00:00 T1566 Detected Phishing email blocked







**Challenges Overcome**

* Difficulty integrating Caldera agents with Windows endpoint.
* Wazuh rules not triggering initially — required tuning custom rules.
* Time synchronization issues between systems affecting timestamps.
* Identifying correct MITRE ATT&CK mapping in Wazuh dashboard.
* Ensuring Caldera operations successfully executed without agent drop-off.

**Learning Outcomes**

* Practical hands‑on execution of adversary emulation using MITRE ATT&CK.
* Understanding spearphishing TTPs used by real threat actors.
* Ability to configure Wazuh for custom SIEM detection.
* Enhanced SOC analysis of alerts and event correlation.
* Improved understanding of red‑team vs blue‑team workflows.

**Emulation Report**

The adversary emulation exercise simulated a spear phishing attack using MITRE Caldera implementing T1566. A phishing payload was delivered to the target host, triggering Wazuh’s email security monitoring rules. The alert was successfully detected and logged with accurate timestamps, demonstrating effective baseline detection capability. However, several detection gaps were identified. While the initial phishing email was blocked, no alert was generated for the user’s interaction attempts, such as link clicks or attachment access. Additionally, lateral movement post-phishing was not monitored due to missing correlation rules. Improving behavioral analytics and enhancing rule coverage is recommended.