Task # 03

Task Document: Malware Download and Incident Response Plan

Objective:

Download a freely available malware via a VM with an active pfSense firewall, observe detection and log activities, analyze logs and malware, and create an incident response plan.

Steps:

1. Setup and Download Malware

- Preparation:
  - Ensure pfSense firewall is configured and running.
  - Set up a VM for malware download.
- Download Malware:
  - Download a freely available malware sample from a reputable site (e.g., theZoo, VirusShare).

2. Detection and Observation

- pfSense Monitoring:
  - Check pfSense logs for detection of the malicious download.
  - Document any alerts or blocks.
- Wazuh Dashboard:
  - Observe Wazuh for alerts/log entries related to the malware.
  - Gather detailed log entries.

3. Log and Malware Analysis

- Log Details Collection:
  - Collect comprehensive logs from Wazuh.
  - Identify Indicators of Compromise (IOCs) and Indicators of Attack (IOAs).
- Analysis Report:
  - Create a report analyzing the logs and malware behavior.

4. Incident Response Plan

- Create Incident Response Plan:
  - Develop an incident response plan based on industry standards.
  - Include steps for detection, analysis, containment, eradication, and recovery.
- Share Incident Response Plan:
  - Compile the report and incident response plan.
  - Share the document for review and implementation.

Notes:

- **Follow industry standards for the incident response plan.**
- **Include IOCs, IOAs, and the URL of the malware source in the report.**