Wazuh

What is Wazuh?

- **Open-Source Security Platform:** Free and open-source solution for security monitoring, threat detection, incident response, and compliance.
- **Unified Capabilities:** Combines aspects of **XDR** (Extended Detection and Response) and **SIEM** (Security Information and Event Management).
- **Agent-Based:** Uses lightweight agents deployed on endpoints to collect data.

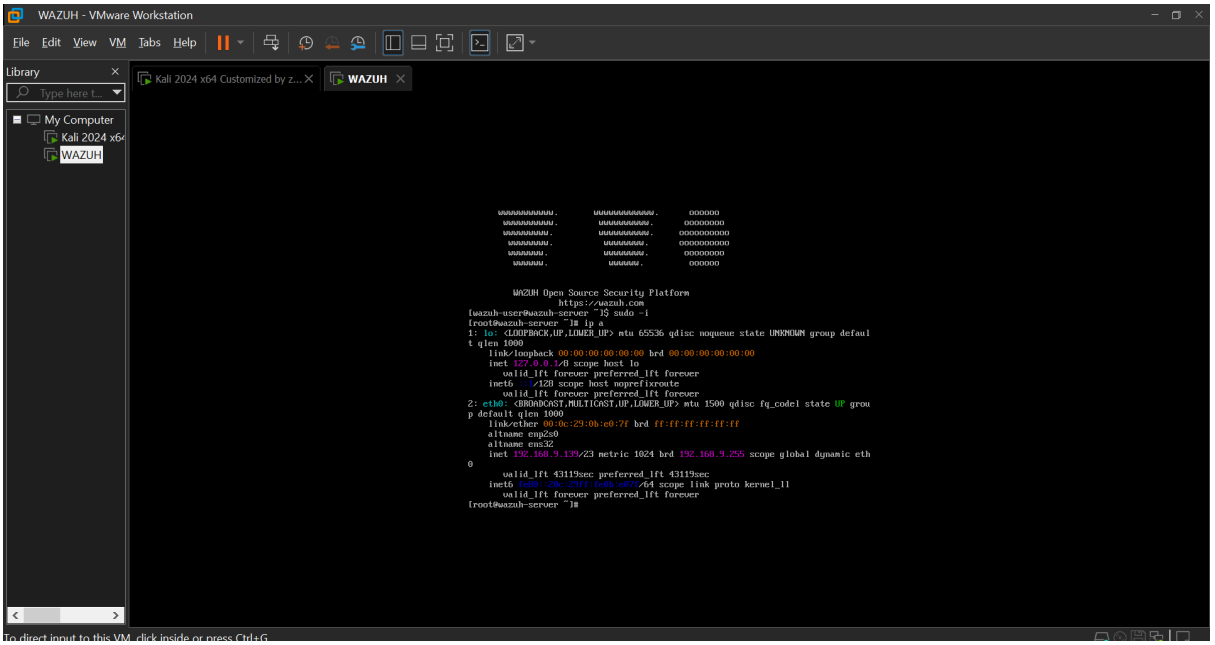
Core Capabilities / What it Does:

- **Endpoint Detection & Response (EDR):**
  - **File Integrity Monitoring (FIM):** Detects changes to critical files and configurations.
  - **Intrusion Detection (HIDS):** Identifies suspicious activities, rootkits, and unauthorized access on hosts.
  - **Vulnerability Detection:** Scans for known software vulnerabilities (CVEs) on endpoints.
  - **Security Configuration Assessment (SCA):** Checks for deviations from security baselines (e.g., CIS Benchmarks).
  - **Active Response:** Can automate actions to contain threats (e.g., block IP, kill process).
- **Log Management & SIEM:**
  - Collects, parses, and normalizes logs from virtually any source (OS, apps, network devices, cloud).
  - Performs real-time **event correlation** to identify attack patterns.
  - Generates **alerts** for suspicious activities.
- **Cloud Security:** Integrates with AWS, Azure, GCP for cloud infrastructure monitoring.
- **Compliance Monitoring:** Helps meet regulatory requirements like **SOC 2**, PCI DSS, GDPR, HIPAA by providing audit trails and continuous monitoring.

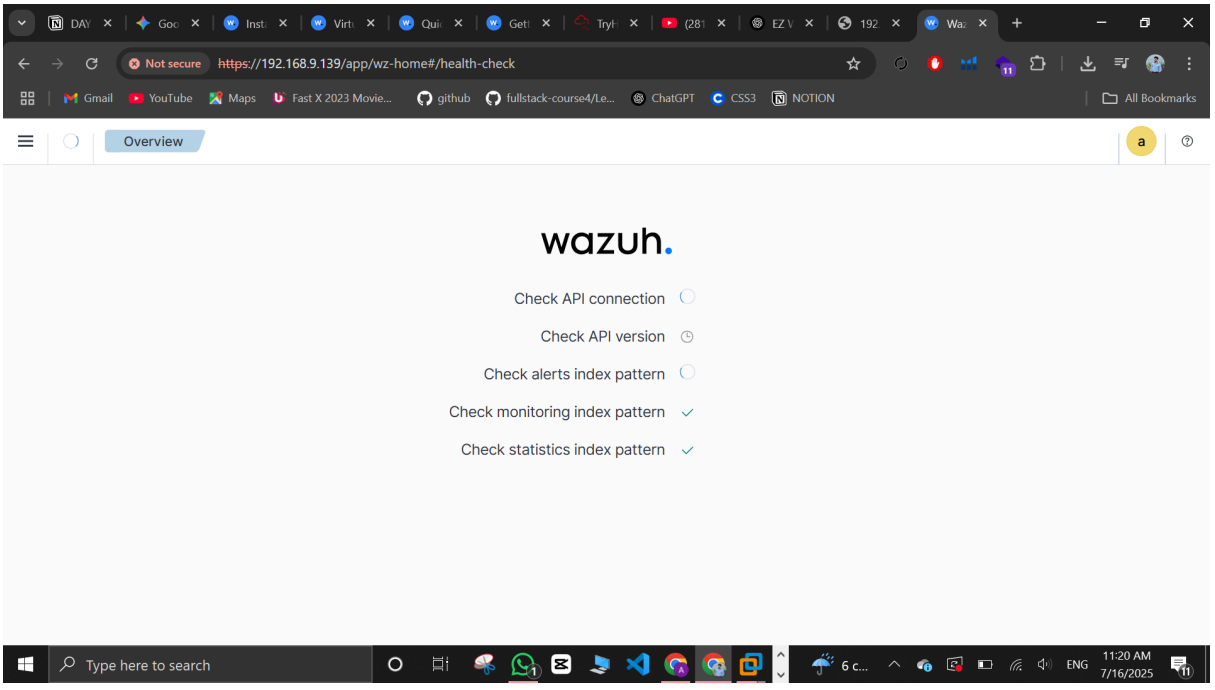
Key Components (How it Works):

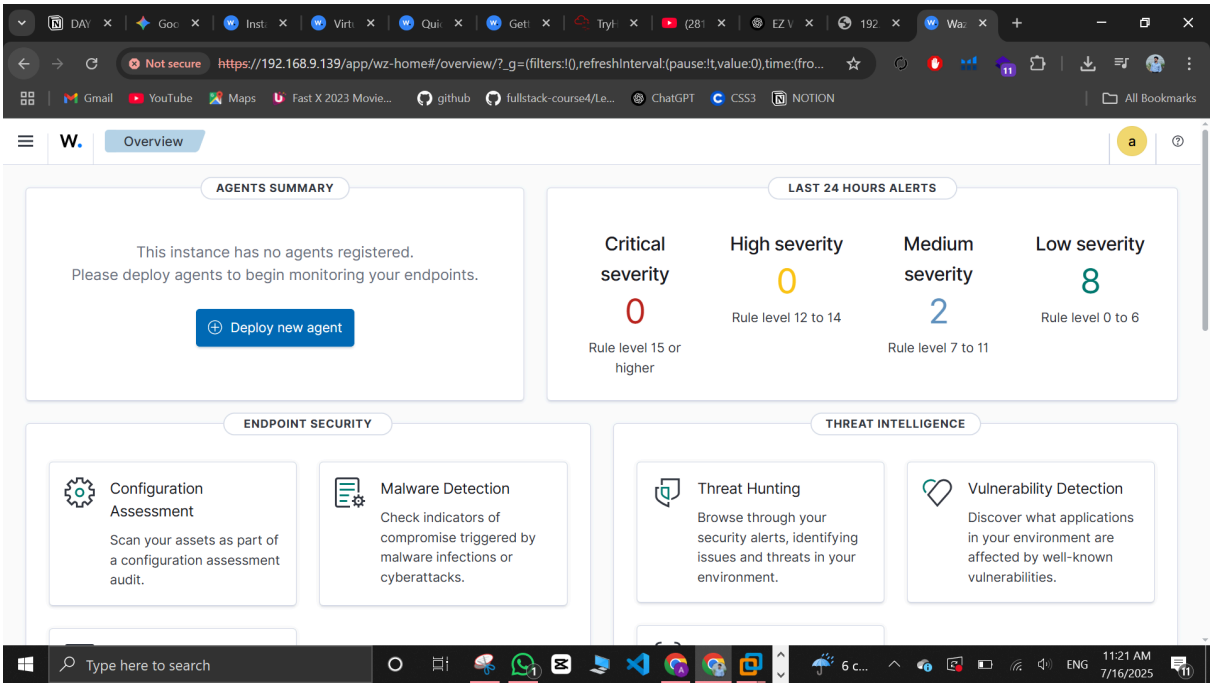
1. **Wazuh Agent:**
    - Lightweight software installed on monitored systems (servers, laptops, VMs, containers, cloud instances).
    - Collects data, performs FIM, HIDS, SCA, vulnerability scans.
    - Communicates securely with the Wazuh Manager.
2. **Wazuh Server (Manager):**
    - The central brain of Wazuh.
    - Processes, analyzes, and correlates data received from agents.
    - Applies detection rules and generates security alerts.
    - Can be deployed in a cluster for high availability and load balancing in larger environments.
3. **Wazuh Indexer:**
    - (Typically OpenSearch or Elasticsearch).
    - Stores and indexes all collected security events and alerts.
    - Enables fast and powerful searching and historical analysis of data.
    - Can be deployed in a cluster for scalability.
4. **Wazuh Dashboard:**
    - (Built on OpenSearch Dashboards/Kibana).
    - The web-based user interface for managing Wazuh.
    - Provides visualizations, dashboards, real-time alerts, and a search console for security data

installed wazuh server through and ova file that was imported in vmware



accessed the dashboad through web browser





deployed agent