**Wazuh-Notes**

**Task 1 – Introduction**

* **Wazuh** is an **open-source Security Information and Event Management (SIEM)** platform.
* Features:
  + Log collection and analysis.
  + Intrusion detection.
  + Vulnerability assessment.
  + File integrity monitoring.
  + Compliance auditing.
* Works with **Wazuh Server**, **Wazuh Agents**, and **Elastic Stack/Kibana**.

**Task 2 – Required: Deploy Wazuh Server**

* The **Wazuh Server**:
  + Processes and analyzes data from agents.
  + Stores events in Elasticsearch.
  + Visualizes data in Kibana.
* Deployment options:
  + Manual installation.
  + Docker containers.
  + Cloud services (AWS, Azure, GCP).
* Ensure proper **network ports** are open (default agent-server port: 1514/1515).

**Task 3 – Wazuh Agents**

* Installed on monitored endpoints (Windows, Linux, macOS).
* Collect and forward:
  + System logs.
  + Security events.
  + Configurations.
* Key command to register an agent with the server:

bash

CopyEdit

/var/ossec/bin/agent-auth -m <server\_ip>

**Task 4 – Wazuh Vulnerability Assessment & Security Events**

* **Vulnerability Detection**:
  + Compares system packages/software against known CVE databases.
  + Generates alerts in Wazuh dashboard.
* Security events include:
  + Unauthorized access attempts.
  + Privilege escalation.
  + Exploit attempts.

**Task 5 – Wazuh Policy Auditing**

* Checks systems for compliance with:
  + PCI DSS.
  + HIPAA.
  + GDPR.
  + CIS Benchmarks.
* Policy results shown in Kibana.
* Helps maintain **security posture** and meet **regulatory requirements**.

**Task 6 – Monitoring Logons with Wazuh**

* Monitors **Windows Event IDs** (e.g., 4624 for successful logon, 4625 for failed logon).
* Detects:
  + Brute-force attacks.
  + Suspicious login times.
  + Unusual account usage.

**Task 7 – Collecting Windows Logs with Wazuh**

* Wazuh agent uses **Windows Event Channel**.
* Collects:
  + Security logs.
  + Application logs.
  + System logs.
* Configured in ossec.conf.

**Task 8 – Collecting Linux Logs with Wazuh**

* Reads logs from:
  + /var/log/auth.log
  + /var/log/syslog
  + /var/log/secure
* Detects:
  + SSH logins.
  + Sudo command executions.
  + Kernel warnings.

**Task 9 – Auditing Commands on Linux with Wazuh**

* Monitors commands run by users:
  + Captures user, timestamp, and command.
  + Helps detect **malicious activity** or **policy violations**.
* Uses **auditd** integration.

**Task 10 – Wazuh API**

* RESTful API for automation and integration.
* Example request:

bash

CopyEdit

curl -u wazuh:wazuh https://<server\_ip>:55000/agents

* Supports agent management, rule queries, and alert retrieval.

**Task 11 – Generating Reports with Wazuh**

* Create **PDF/CSV reports** in Kibana.
* Use for:
  + Security incident summaries.
  + Vulnerability scan results.
  + Compliance audit evidence.

**Task 12 – Loading Sample Data**

* Test Wazuh setup with **sample log data**.
* Helps verify:
  + Parsing rules.
  + Dashboard visualizations.
  + Alert triggers.

✅ **Summary:**  
Wazuh is a **comprehensive, open-source SIEM** that enables real-time log analysis, threat detection, vulnerability scanning, and compliance monitoring across diverse environments.

