Wazuh, **açık kaynaklı bir güvenlik izleme platformudur**. Gerçek zamanlı tehdit tespiti, bütünlük denetimi, güvenlik analizi ve uyumluluk raporlaması gibi konularda yardımcı olur. Genellikle SOC (Security Operations Center) yapılarında tercih edilir.

Wazuh, temel olarak 3 bileşenden oluşur:

1. **Wazuh Agent**: İzlemek istediğin sistemlerde kurulur.
2. **Wazuh Server**: Tüm agent’lardan gelen verileri toplar, analiz eder.
3. **Wazuh Dashboard (Kibana ile)**: Grafiksel arayüz sunar, log’ları görselleştirir.

**Wazuh Özellikleri**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🛡️ Gerçek Zamanlı Tehdit Tespiti | Şüpheli etkinlikleri anlık olarak tespit eder. |
| 🔐 Dosya Bütünlüğü Denetimi | Dosya sistemindeki değişiklikleri izler (FIM). |
| 🔍 Log Analizi | Sistem, ağ ve uygulama log’larını analiz eder. |
| 📜 Uyum Takibi | PCI-DSS, GDPR, HIPAA gibi regülasyonlara uygunluğu izler. |
| 📈 SIEM Entegrasyonu | ELK (Elasticsearch, Logstash, Kibana) veya Splunk gibi sistemlerle uyumlu. |
| 🕵️‍♂️ Rootkit Tespiti | Kernel-level zararlı aktiviteleri algılayabilir. |

**Wazuh Nerelerde Kullanılır?**

* **Kurumsal ağlar**: Merkezi log toplama ve analiz için.
* **Bulut ortamları**: AWS, Azure, GCP entegrasyonu sayesinde bulut altyapılarında güvenlik izleme.
* **SOC'larda**: SIEM platformu olarak kullanılır.
* **Pentest / Red Team ortamlarında**: Gerçek saldırı senaryolarında tespit sistemi olarak test edilebilir.
* **Uygulama güvenliği**: Web ve veri tabanı log’larının incelenmesinde.

Kali Linux Üzerine Wazuh Kurulumu

**Adım 1: Kali Sistemini Güncelle**

Kali Linux sistemini güncel tutmak için aşağıdaki komutu çalıştır.

***sudo apt update && sudo apt upgrade -y***

ekran görüntüsü, metin, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 2: Wazuh Agent Kurulum Dosyalarını Ekle ve Kur**

Wazuh agent’i kurmak için GPG anahtarını ekle, depo ekle ve paketi kur.

***curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/share/keyrings/wazuh.gpg  
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list  
sudo apt update  
sudo apt install wazuh-agent -y***

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 3: Agent Yapılandırmasını Düzenle**

Agent’in Wazuh server’a bağlanması için config dosyasını düzenle.

***sudo nano /var/ossec/etc/ossec.conf***

ekran görüntüsü, metin, yazı tipi, siyah içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 4: Agent Servisini Başlat**

Wazuh agent servisini sistemde aktif hale getir ve başlat.

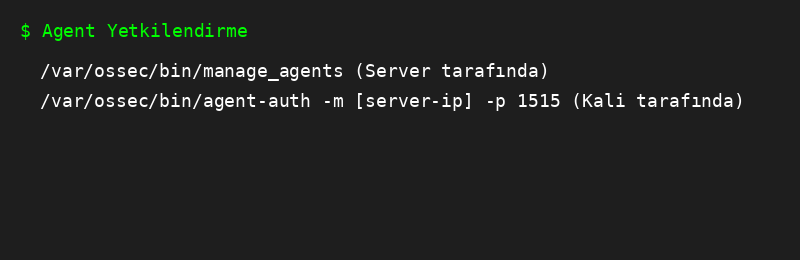
***sudo systemctl daemon-reexec  
sudo systemctl enable wazuh-agent  
sudo systemctl start wazuh-agent***

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Adım 5: Agent Yetkilendirme ve Server’a Bağlama**

Server tarafında agent tanımla, Kali üzerinde server’a bağlan.

***/var/ossec/bin/manage\_agents # (Server tarafında)  
/var/ossec/bin/agent-auth -m [server-ip] -p 1515 # (Kali tarafında)***