**CrowdSec**

**1. Nedir?**  
CrowdSec, kötü amaçlı aktiviteleri tespit etmek ve engellemek için kullanılan **açık kaynaklı bir güvenlik duvarı sistemidir**.  
Aynı zamanda topluluk tabanlıdır; yani birçok kullanıcı kötü niyetli IP’leri sisteme bildirir ve herkes bu bilgilere ulaşabilir.

Kısaca:  
 - "Saldırganları tespit et"  
 - "Engelle"  
 - "Toplulukla paylaş"



**2. Ne İşe Yarar?**

* Sunucunuza gelen kötü niyetli bağlantı denemelerini tespit eder.
* Örneğin: brute-force saldırıları, port taramaları, şüpheli davranışlar.
* Tespit ettiği IP adreslerini otomatik olarak **engeller**.
* Daha güzeli: Diğer kullanıcıların tespit ettiği saldırganları **sen de engelleyebilirsin.**

➡️ CrowdSec, fail2ban’a benzer ama çok daha gelişmiş ve modern bir sistemdir.  
Makine öğrenimiyle davranışları analiz edebilir.

**3. Neden Önemlidir?**

* Siber saldırılar günümüzde çok yaygın ve sürekli olarak sistemler taranıyor.
* Sadece kendi verini değil, **diğer kullanıcıların tespit ettiği tehditleri** de kullanarak savunmanı güçlendirmiş oluyorsun.
* Yani: **Ne kadar çok kullanıcı, o kadar güçlü koruma!**
* Özellikle SSH brute-force, RDP saldırıları, port taramaları gibi tehditlerde çok başarılıdır.

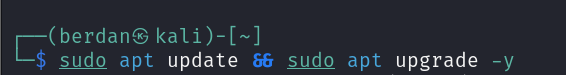
Ayrıca log dosyalarını analiz ederek davranışsal saldırı tespiti yapabilir.

**4. Nasıl Kurulur? (Linux Örneği)**

Kurulum oldukça kolaydır. Debian/Ubuntu sistemlerde aşağıdaki adımlarla yapılabilir:

**# 1. Sistem güncellemesi**

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



**# 2. CrowdSec kurulumu (resmi komut)**

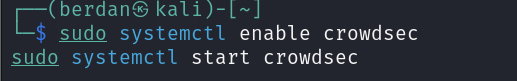
**curl -s https://install.crowdsec.net | sudo bash**

****

**# 3. Kurulumdan sonra servisi başlat**

**sudo systemctl enable crowdsec**

**sudo systemctl start crowdsec**

****

**# 4. Durum kontrolü**

**sudo systemctl status crowdsec**

****

🛠️ Ekstra olarak:

* **cscli** komutu ile IP engelleme listesi kontrol edilir.
* **crowdsec-firewall-bouncer** ile saldırganlar otomatik engellenir.

**5. Örnek Bir Anlatım:**  
Diyelim ki bir sunucuda SSH servisi açık. Saldırgan sürekli olarak farklı şifrelerle oturum açmayı deniyor.

**CrowdSec** logları tarar ve şunu fark eder:

"Bu IP, son 1 dakikada 20 kez yanlış şifre denedi!"

O zaman:  
✅ IP engellenir.  
✅ Bu IP topluluğa raporlanır.  
✅ Başka biri bu IP’yi görürse **önceden engelleyebilir.**

**# Engellenen IP'leri listele**

**sudo cscli decisions list**

**# Belirli bir IP'yi engelle**

**sudo cscli decisions add -i 192.168.1.100**

* Gerçek zamanlı koruma sağlar.
* Giderek büyüyen bir savunma ağına katılmış olursun.

**Uyarı:**  
CrowdSec yasal, açık kaynaklı ve savunma amaçlı bir araçtır. Ancak yanlış yapılandırılırsa, iyi niyetli IP'ler de engellenebilir. Dikkatli kullanılmalıdır.