Caldera - MITRE ATT&CK Simülasyon Aracı Eğitim Materyali

# 🔍 Caldera Nedir?

CALDERA, MITRE tarafından geliştirilen, siber güvenlik testleri ve Red Team simülasyonları yapmak için kullanılan açık kaynaklı bir saldırı simülasyon sistemidir.  
Özellikle MITRE ATT&CK matrisi üzerinden tehdit aktörlerinin taktik ve tekniklerini test etmek için kullanılır.

# 🔧 Özellikleri

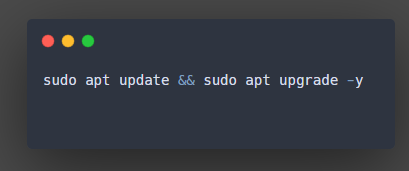
- MITRE ATT&CK teknikleriyle entegre çalışır.  
- Otonom ajanlar üzerinden saldırı simülasyonu yapar.  
- Web tabanlı arayüze sahiptir.  
- Linux, Windows, MacOS ajan desteği sunar.  
- Geliştirilebilir plugin mimarisi vardır.

# 📌 Kullanım Alanları

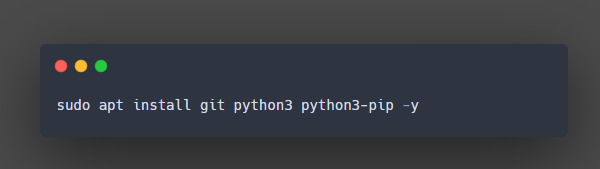
- Red Team - Blue Team eğitimleri  
- Güvenlik açığı testleri  
- Tehdit simülasyonu ve tespit mekanizmalarının kontrolü  
- SOC ekipleri için olay senaryoları oluşturma

# 💻 Kurulum Adımları (Linux - Kali Örneği)

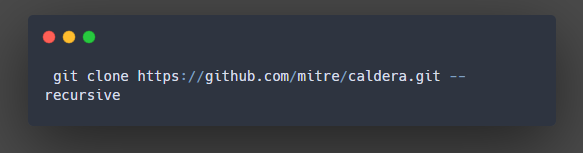
1. Sistem güncellemesi:



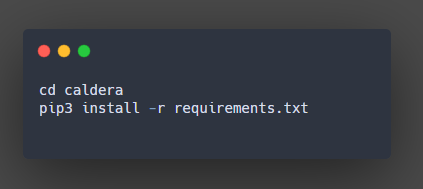
2. Gerekli bağımlılıkların kurulması:



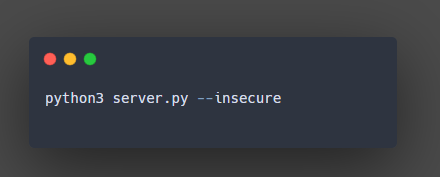
3. Caldera deposunu klonlayın:



4. Klasöre geçin ve modülleri yükleyin:



5. Aracı başlatın:



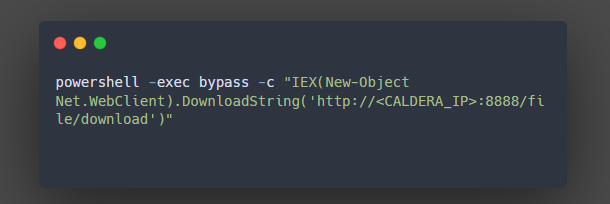
# 🌐 Web Arayüz ve Giriş

- Caldera arayüzüne web tarayıcınızdan erişin: http://localhost:8888  
- Varsayılan kullanıcı adı: red  
- Varsayılan şifre: admin

# 🛰️ Ajan (Agent) Ekleme ve Simülasyon Başlatma

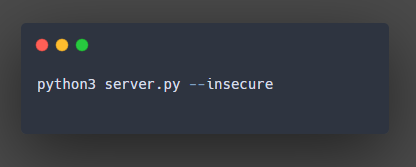
1. Bir hedef sisteme "Sandcat" ajanı gönderilir.  
2. Ajan başarılı şekilde bağlandığında web arayüzde görünür.  
3. "Operation" menüsünden yeni görev oluşturulur.  
4. Taktik ve teknikler seçilerek simülasyon başlatılır.

# 🖥️ Örnek Terminal Komutları ve Çıktılar

# Ajan çalıştırma örneği (Windows hedefte)  


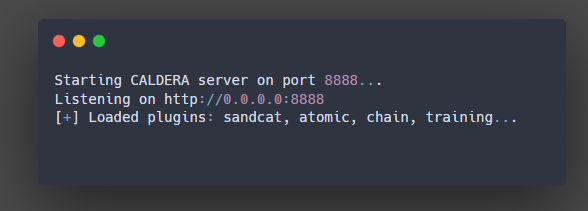
Bu komut hedef sisteme "sandcat" isimli ajanı indirip çalıştırır.  
<CALDERA\_IP> yerine Caldera kurulu sistemin IP adresi yazılır.

🟥 **Not:** Bu komut hedef sistemde çalıştırılır (örneğin Windows VM).



Caldera'yı başlatır, web arayüzü dinlemeye başlar. --insecure parametresi şifreleme olmadan çalıştırır.

# Caldera başlatıldığında gelen terminal çıktısı:

  
Bu çıktı, Caldera sunucusunun başarıyla başlatıldığını ve web arayüzünün hazır olduğunu gösterir.

🧠 Öğrenci İçin Notlar

- Caldera, gerçek saldırı vektörlerini taklit eder.  
- Hedef sistemde anti-virüs devre dışı değilse ajanlar engellenebilir.  
- Eğitim amaçlı ağ ortamlarında kullanılması önerilir.