Cuckoo Sandbox Hakkında Eğitim Materyali

# 1. Cuckoo Sandbox Nedir?

Cuckoo Sandbox, zararlı yazılımları güvenli bir ortamda analiz etmek için kullanılan açık kaynaklı bir otomatik kötü amaçlı yazılım analiz sistemidir. Sanal makineler kullanarak dosyaların, URL’lerin ve e-posta eklerinin davranışlarını izler.

# 2. Özellikleri

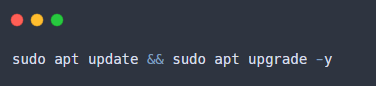
* - Windows, Linux, macOS ve Android ortamlarında analiz yapabilme.
* - Dosya, URL, e-posta eki ve bellek dökümü analizi.
* - Ayrıntılı rapor çıktıları (HTML, JSON vb.).
* - Ağ trafiğini, dosya değişikliklerini ve API çağrılarını izleme.
* - Modüler yapı sayesinde özelleştirme imkanı.

# 3. Nerelerde Kullanılır?

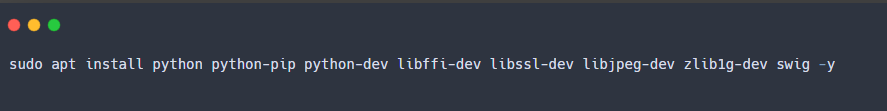
* - Siber olay müdahalesinde zararlı yazılım analizi.
* - Adli bilişim incelemelerinde.
* - Tehdit istihbaratı toplama süreçlerinde.
* - Eğitim ve araştırma amaçlı zararlı yazılım davranış analizi.

# 4. Kali Linux Üzerine Kurulum Adımları

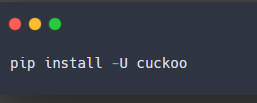
1. Paketleri güncelleyin:

******

2. Gerekli bağımlılıkları yükleyin:

******

3. Cuckoo Sandbox'ı yükleyin:

******

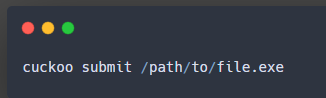
4. Cuckoo için sanal makine ayarlarını yapın (VirtualBox veya KVM).

5. Cuckoo Sandbox'ı başlatın:

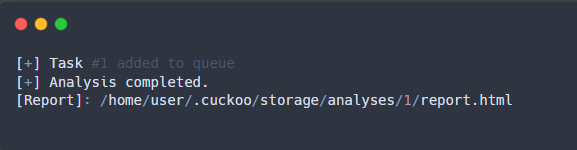
# 

# 5. Örnek Kullanım ve Çıktı

* Örnek: Bir dosyayı analiz etme:

******

* Örnek Çıktı (özet):



# Güvenlik Dipnotu

Cuckoo Sandbox yalnızca izole test ortamlarında kullanılmalıdır. Gerçek sistemlerde zararlı yazılım çalıştırmak ciddi güvenlik riskleri doğurur.