**CAPE Sandbox Nedir?**

Siber güvenlikte, kötü amaçlı yazılımları analiz etmek için sandbox adı verilen izole ve kontrollü test ortamları kullanılır.  
CAPE Sandbox, bu amaçla geliştirilen, özellikle zararlı yazılımları (malware) detaylı olarak analiz eden açık kaynaklı bir analiz platformudur.

CAPE kelimesi:  
*Config and Payload Extraction* anlamına gelir.  
Yani:  
Yalnızca kötü amaçlı yazılımı çalıştırmakla kalmaz, aynı zamanda payload (zararlı yük) dosyasını da açığa çıkarır ve yapılandırma (config) bilgilerini analiz eder.

**CAPE Ne İşe Yarar?**

CAPE Sandbox, kötü amaçlı yazılım çalıştırıldığında ne yaptığını detaylıca analiz eder.  
Bir zararlı yazılım .exe, .dll, .doc, .js veya .bat uzantılı olabilir.  
CAPE bu dosyayı sanal bir sistemde çalıştırır ve aşağıdaki gibi aktiviteleri izler:

Dosya sistemine yaptığı değişiklikler  
Kayıt defteri (registry) erişimleri  
Ağ bağlantıları  
API çağrıları (sistemle nasıl konuştuğu)  
Bellek içeriği  
Şifreleme, kod gizleme ve injection yöntemleri  
Konfigürasyon dosyaları ve şifreli payload'ların açılması

**CAPE Sandbox Nasıl Kurulur?**

Kurulum karmaşık gibi görünse de temel adımlar net bir şekilde takip edilirse sistem çalışır hale gelir.  
En yaygın yöntem: Ubuntu (Linux) üzerine kurulum ve web arayüzü kullanımıdır.

Hızlı Kurulum Adımları (Özet)

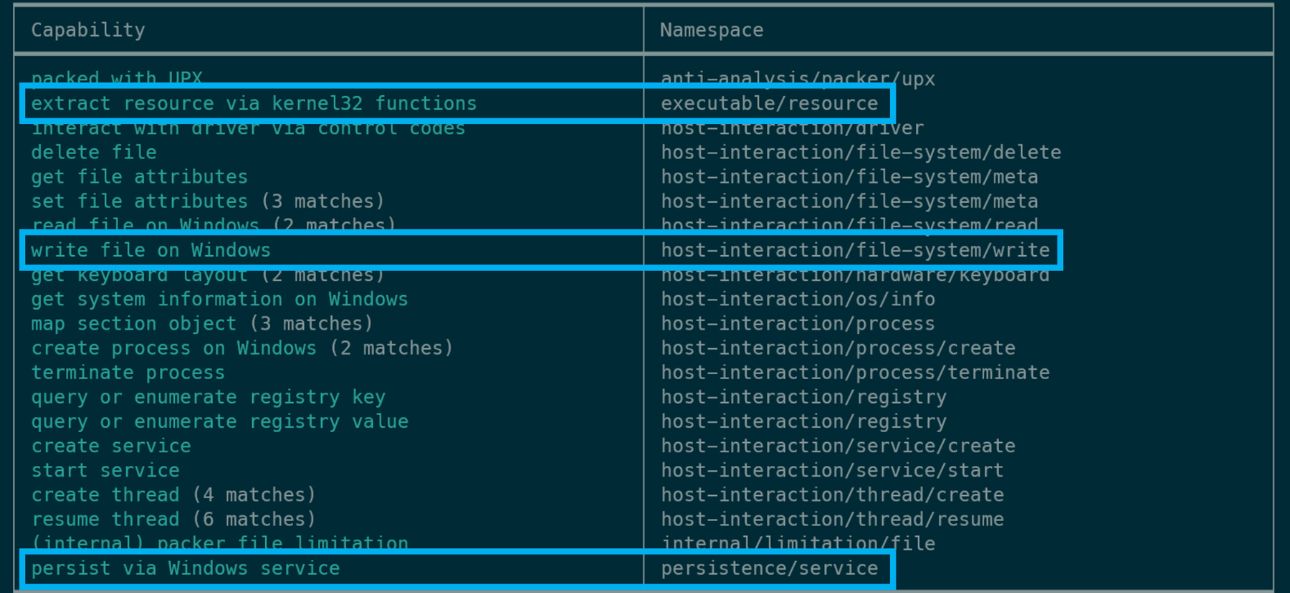
1. Ubuntu 20.04 veya benzeri bir Linux sistem kurulur.
2. Gerekli bağımlılıklar yüklenir (Python, MongoDB, Django, VirtualBox/VMware).
3. CAPE deposu GitHub’dan indirilir:

***git clone https://github.com/ctxis/CAPE.git***

***cd CAPE***

1. Kurulum scripti çalıştırılır: ***sudo ./install.sh***
2. Web arayüzüne erişmek için: [***http://localhost:8000***](http://localhost:8000)

Alternatif: CAPE’yi kurmak istemezseniz, analizleri **Any.Run** gibi hazır sandbox servisleriyle de yapabilirsiniz.



**CAPE Sandbox ile Neler Yapılabilir?**

| **Özellik** | **Açıklama** |
| --- | --- |
| **Malware Analizi** | **Zararlı yazılım çalıştırılıp sistem üzerindeki tüm etkisi analiz edilir** |
| **Ağ Trafiği İncelemesi** | **Wireshark benzeri pcap dosyası çıkışı alınabilir** |
| **Payload Çözümleme** | **Şifreli veya gizlenmiş dosya içeriği açığa çıkarılır** |
| **Config Extraction** | **Zararlı yazılımın yapılandırma bilgileri analiz edilir** |
| **API İzleme** | **Yazılımın hangi sistem işlevlerini kullandığı takip edilir** |
| **Otomatik Raporlama** | **HTML veya JSON formatında analiz raporu oluşturulur** |