**Peirates:**

**Peirates Nedir?**

Peirates, Kubernetes ortamlarında güvenlik açıklarını tespit etmek, istismar etmek (exploitation) ve genel olarak Kubernetes küme güvenliğini değerlendirmek için kullanılan açık kaynaklı bir güvenlik test ve exploitation framework’üdür.

Kubernetes, konteyner orkestrasyonunda yaygın kullanılan bir platformdur ve güvenlik zafiyetleri ciddi riskler oluşturabilir. Peirates, pentester (sızma testi yapan) ve güvenlik uzmanlarının Kubernetes altyapısını test edip zayıf noktaları bulmasını kolaylaştırır.

**Özellikleri:**

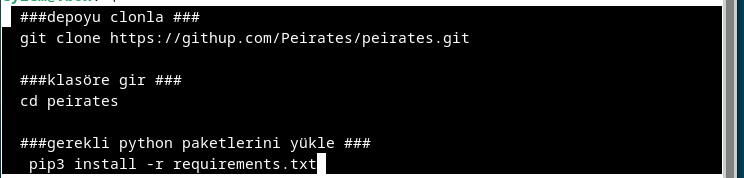
* **Kubernetes Saldırı Vektörlerini Test Edebilme:** Node’lar, pod’lar, servis hesapları (service accounts), RBAC (Role-Based Access Control) politikaları gibi birçok farklı bileşende güvenlik açıklarını tespit eder.
* **Exploit Modülleri:** Bulunan açıkları kullanarak örnek saldırılar yapabilir, böylece güvenlik risklerinin ciddiyetini değerlendirmeye yardımcı olur.
* **Kolay Kullanım:** CLI (Command Line Interface) üzerinden kolayca yönetilir.
* **Modüler ve Genişletilebilir:** Yeni test ve exploit modülleri eklenebilir.
* **Otomatik Tarama:** Kubernetes cluster üzerinde otomatik güvenlik taramaları yapabilir.
* **Detaylı Raporlama:** Güvenlik açığı raporları oluşturur.

**Kullanım Alanları**

* **Kubernetes Güvenlik Değerlendirmesi:** Sistem yöneticileri ve pentesterlar Kubernetes ortamının zayıf noktalarını keşfetmek için kullanır.
* **Sızma Testleri:** Güvenlik açığı olup olmadığını kontrol etmek için simüle edilmiş saldırılar yapar.
* **Güvenlik Eğitimleri:** Kubernetes güvenlik konularında eğitim ve farkındalık artırmak için pratik ortam sağlar.
* **Sürekli Güvenlik İzleme:** Otomatik testler ile zaman içinde güvenlik durumunun takibi yapılabilir.

**Kurulum Aşaması**

Peirates genellikle Linux ortamında veya Kali Linux gibi pentest odaklı dağıtımlarda kullanılır. Kurulum aşamaları genel olarak şu şekildedir:

1. **Gereksinimler:**
   * Python 3
   * Kubernetes cluster erişimi (kubectl config ayarları)
   * Git (kaynak kodu indirmek için)
2. **Kurulum Komutları: **
3. **Kubernetes Erişimi:**
   * kubectl komut satırı aracı kurulu ve Kubernetes cluster erişiminiz konfigüre edilmiş olmalı.
   * Peirates, bu ayarları kullanarak cluster'a bağlanır.
4. **Başlatma:**

****

**5. Dikkat Edilmesi Gerekenler**

* **Yasal İzin:** Peirates ile yapılacak güvenlik testleri mutlaka ilgili Kubernetes cluster yöneticisinin izniyle yapılmalıdır. İzinsiz testler yasal sorunlara yol açabilir.
* **Canlı Ortamda Kullanım:** Canlı (production) ortamda dikkatli olunmalıdır. Bazı exploitler sistemde kesintiye neden olabilir.
* **Kubernetes Sürümü:** Peirates’in uyumlu olduğu Kubernetes sürümleri takip edilmelidir.
* **Güvenlik:** Test sırasında ortaya çıkan veriler ve raporlar gizli tutulmalıdır.
* **Güncelleme:** Araç ve modüller düzenli güncellenmeli, yeni zafiyetlere karşı güncel tutulmalıdır.
* **Yetki Kontrolü:** Testler sırasında kullanılan servis hesapları ve izinler kontrol edilmelidir. Gereksiz yetkiler verilmemelidir.