**VECTR Nedir?**

**VECTR** (Versatile Enterprise Cybersecurity Test Range), MITRE ATT&CK tabanlı bir saldırı simülasyonu ve mavi takım (blue team) test yönetimi platformudur. Güvenlik ekiplerinin savunma mekanizmalarını değerlendirmeleri, test etmeleri ve geliştirmeleri için kullanılır.

**VECTR Özellikleri**

* **MITRE ATT&CK Uyumluluğu:** Tüm simülasyonları MITRE ATT&CK framework’üne göre planlar.
* **Saldırı Simülasyonu:** Gerçek saldırı senaryolarını simüle ederek sistem tepkilerini ölçer.
* **Raporlama ve Kayıt Tutma:** Detaylı analiz, raporlama ve geçmiş testlerin kaydını tutma.
* **Web Arayüzü:** Kullanımı kolay bir web arayüzüyle birlikte gelir.
* **Takım İşbirliği:** Mavi (savunma) ve kırmızı (saldırı) takım iş birliği için tasarlanmıştır.
* **Açık Kaynak:** Ücretsizdir ve GitHub üzerinden erişilebilir.

**VECTR Kurulum Aşamaları**

**Gereksinimler:**

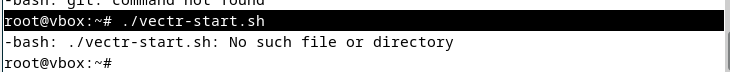
* Java 11+
* Docker (isteğe bağlı)
* MongoDB (VECTR kendi içinde entegre sunar)
* 4 GB+ RAM önerilir

1. **Docker ile Kolay Kurulum (Önerilen**): 

-Bu komutlar, VECTR’i docker üzerinden ayağa kaldırır. Web arayüzü genellikle http://localhost:8081 adresindedir.

### 2. Manuel Kurulum (Advanced)

Eğer Docker kullanmak istemiyorsan:

* [VECTR Releases](https://github.com/SecurityRiskAdvisors/VECTR/releases) sayfasından .zip dosyasını indir.
* Java 11 yüklü olmalı.
* Dosyayı çıkar ve terminalden çalıştır: 

-Tarayıcıdan: http://localhost:8081 adresine giderek arayüze ulaşabilirsin.

**VECTR Kullanımı**

1. **Kullanıcı Girişi:** Arayüz açıldığında kullanıcı hesabı oluştur ya da mevcut hesapla giriş yap.
2. **Test Planı Oluştur:** Yeni bir test planı başlat, saldırı tekniklerini seç.
3. **Simülasyonu Başlat:** Belirli tekniklere göre saldırı simülasyonunu başlat.
4. **Sonuçları Kayıt Et:** Testin başarı/başarısızlık durumlarını girerek kaydet.
5. **Raporla:** Sistem zayıflıklarını analiz et, rapor al.

**Dikkat Edilmesi Gereken Noktalar**

* Docker kullanıyorsan sistem kaynaklarının yeterli olması önemli.
* VECTR, kendi başına saldırı yapmaz; sadece simülasyonu takip eder. Saldırıyı kendin veya başka araçlarla yapman gerekir.
* Java ve MongoDB düzgün çalışmazsa VECTR açılmaz.
* Kurulumdan sonra arayüzde ilk kullanıcıyı sen oluşturursun, admin yetkisini unutma.
* Port çakışmalarına dikkat et (8081, 8080 gibi portlar başka servislerle çakışabilir).

**VECTR Kullanım Alanları**

* **Kırmızı-Mavi Takım Egzersizleri:** Simülasyonlarla kurum içi siber güvenlik testleri.
* **Siber Güvenlik Eğitimleri:** Öğrencilere veya ekiplere siber saldırı simülasyonu eğitimi.
* **Denetim ve Geliştirme:** Mevcut güvenlik sistemlerinin etkili çalışıp çalışmadığını test etme.
* **SOC (Security Operation Center) Performans Ölçümü:** Olaylara verilen tepkileri analiz etme.
* **Saldırı Tekniklerinin Haritalanması:** MITRE ATT&CK tekniklerinin ne ölçüde tespit edilebildiğini görme.