**🔍 1. MiterWarden Nedir?**

**MiterWarden**, sistemleri veya ağları **MITRE ATT&CK tekniklerine göre analiz eden** ve güvenlik zafiyetlerini tespit etmeye odaklanan açık kaynaklı bir araçtır.

📌 Temel Özellikler:

* ATT&CK tekniklerine dayalı tehdit modeli
* Zafiyet eşleştirme ve haritalama
* Proaktif güvenlik farkındalığı
* Kurumların savunma boşluklarını görselleştirme

**🛠️ 2. Ne İşe Yarar?**

| **Özellik** | **Açıklama** |
| --- | --- |
| 📊 MITRE ATT&CK eşleştirmesi | Sistem açıklarını ATT&CK tekniklerine göre analiz eder |
| 🔍 Güvenlik boşluğu analizi | Eksik kontrolleri ve zafiyetleri listeler |
| 📁 JSON/CSV raporlama | Raporları dışa aktarır |
| 🧠 Tehdit farkındalığı | Hangi tekniklere karşı savunmasızsınız, gösterir |
| 📌 Savunma planlaması | Blue Team’ler için yol haritası çıkarır |

**⚙️ 3. Kurulum (Linux / Kali)**

MiterWarden Go dilinde yazılmıştır.

**✅ 1. Golang yüklü değilse:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**✅ 2. Kurulum:**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🚀 4. Kullanım Komutları**

**✅ 1. Sistem taraması:**

MiterWarden scan

Bu komut, yerel sistemde savunmasız teknikleri tespit eder ve MITRE ATT&CK karşılıklarını gösterir.

**✅ 2. Sonuçları JSON formatında dışa aktar:**

MiterWarden scan --json > report.json

**✅ 3. CSV çıktısı almak için:**

MiterWarden scan --csv > results.csv

**📋 5. Örnek Terminal Çıktısı**

metin, ekran görüntüsü, yazılım, multimedya yazılımı içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🧠 6. MITRE ATT&CK Nedir?**

**MITRE ATT&CK**, siber saldırganların kullanabileceği taktik ve tekniklerin detaylıca açıklandığı, dünya genelinde kabul gören bir tehdit modeli veritabanıdır.

| **Kavram** | **Açıklama** |
| --- | --- |
| 🎯 Tactic | Saldırganın hedefi (örnek: Persistence) |
| 🧪 Technique | Bu hedefe ulaşmak için kullanılan yöntem (örnek: DLL Injection) |
| 🔧 Mitigation | Önleyici savunma önerileri |
| 🔎 Detection | Nasıl tespit edilir? |

MiterWarden bu modelle birebir eşleştirme yapar.

**📊 7. Raporlama Özellikleri**

| **Format** | **İçerik** |
| --- | --- |
| 📄 JSON | Teknik eşleştirmeler, açıklamalar, öneriler |
| 📄 CSV | Kolayca filtrelenebilir düz rapor |
| 🖼️ Haritalama (manüel) | ATT&CK navigator ile uyumlu çıktı alınabilir |

**🎯 8. Öğrenim Kazanımları**

* MITRE ATT&CK framework’ünü uygulamalı olarak öğrenme
* Zafiyet analizi ile tehdit eşleştirme farkındalığı kazanma
* Proaktif savunma bakış açısı geliştirme
* Blue Team ve Red Team arasındaki bakış farklarını anlama
* Kurumsal güvenlik haritalaması yapabilme becerisi