# 🔒 CyberSecNetAnalyzer

**CyberSecNetAnalyzer**, kullanıcının Wireshark (.pcap/.pcapng) dosyasını yükleyerek içerdiği ağ trafiğinde siber saldırı belirtileri olup olmadığını analiz eden bir Flask tabanlı web uygulamasıdır. LLM (GPT-4) desteğiyle analiz sonucu kullanıcı dostu biçimde yorumlanır.

## ✨ Özellikler

* 📂 .pcap/.pcapng dosyası yükleme
* ⚖️ Trafik içinde aşağıdaki siber saldırıları tespit:
  + SYN Flood (DDOS)
  + Port Tarama
  + ARP Spoofing / MITM
  + ICMP / UDP Flood
* 🧠 GPT-4 ile LLM yorumu (“tehlike varsa yorumla, yoksa sade ve net bilgi ver”)
* 🌐 Flask + HTML5 frontend
* 🌈 Modern, koyu temalı UI

## 📁 Kurulum

1. Bu repoyu klonlayın:

git clone https://github.com/kullaniciadi/CyberSecNetAnalyzer.git  
cd CyberSecNetAnalyzer

1. Sanal ortam ve bağımlılıklar:

python -m venv venv  
venv\Scripts\activate # Linux/macOS: source venv/bin/activate  
pip install -r requirements.txt

1. .env dosyası oluşturun:

OPENAI\_API\_KEY=sk-...

1. Sunucuyu başlatın:

python app.py

## 🔍 Desteklenen Dosya Formatları

* .pcap
* .pcapng

## ⚖️ Algılanabilir Saldırılar

| Saldırı | Tespit Durumu |
| --- | --- |
| SYN Flood | ✅ Var |
| Port Scan | ✅ Var |
| ARP Spoofing | ✅ Var |
| ICMP Flood | ✅ Var |
| UDP Flood | ✅ Var |

## 🤖 Katkı

Pull request ve issue açmaya çekinmeyin. Önerileriniz bu projenin daha da gelişmesini sağlar.

## 📄 Ekran Görüntüsü

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

## ✨ Teşekkürler

Bu proje bir öğrenci projesi olarak siber güvenlik çalışmalarını desteklemek amacıyla geliştirilmiştir.

Proje için kullanılan wireshark ağ trafiği dosyaları (.pcap) eğitim amacı ile kullandığım sanal bir windows cihazdan alınmıştır. Alınan dosyalar gerçek zamanlı saldırı anlarında alınmış olup o şekilde oluşturulmuştur. Yapılan saldırılar da yine eğitim amaçlı olarak şahsım tarafından Linux üzerinden yapılmış olup herhangi bir gerçek siber saldırı içermemektedir. Eğitim amaçlı olarak kendi yaptığım saldırılardır.