SWOT Analizi – CAN Bus ID Spoofing (Şarj Esnasında)

Strengths (Güçlü Yönler)

- Gerçek dünyada karşılığı olan bir **siber saldırı senaryosu** seçilmesi (CAN Bus ID Spoofing).
- **Simülasyon ortamı (vcan0 + OCPP–CAN köprüsü)** kullanılarak saldırının **test edilebilir** hale getirilmesi.
- Proje ekibinde açık görev dağılımı ve **Scrum yönetimiyle disiplinli ilerleme**.
- **Standartlara dayalı (ISO 11898, 15118, 26262)** teknik analiz.
- Güvenlik açıklarının **çok katmanlı çözüm önerileriyle (donanım, yazılım, protokol)** ele alınması.

Weaknesses (Zayıf Yönler)

- CAN Bus hattında **yerleşik kimlik doğrulama veya şifreleme** mekanizması bulunmaması.
- Saldırı tespiti için **gerçek donanım testleri yapılamadı**, yalnızca simülasyon ortamı kullanıldı.
- **Zaman kısıtı** nedeniyle yalnızca tek saldırı türü (ID Spoofing) derinlemesine incelendi.
- ECU yazılımına müdahale gerekmesi, **uygulama maliyeti** ve **entegrasyon zorluğu** oluşturabilir.
- **Yanlış pozitif/negatif** tespiti riski (IDS modeli tam optimize edilmedi).

Opportunities (Fırsatlar)

- CANsec, Secure Gateway veya **IDS/IPS sistemleriyle** gelecekteki araştırmalara temel oluşturabilir.
- **Elektrikli araç üreticileri ve şarj istasyonları** için güvenli iletişim protokolleri geliştirme imkânı.
- TÜBİTAK ve üniversite **Ar-Ge destek programlarıyla** projeyi ileri seviyeye taşıma potansiyeli.
- Şarj istasyonlarıyla **ortak saha testleri** yaparak gerçek veriler üzerinden iyileştirme fırsatı.
- **Makine Öğrenmesi tabanlı anomali tespiti** modellerine dönüştürülebilir.

Threats (Tehditler)

- Araç servisleri veya halka açık alanlarda **fiziksel erişim riski** (OBD-II portu üzerinden saldırı).
- **Tedarik zinciri zafiyetleri** (yan sanayi donanımlar, üçüncü parti modüller).
- Güvenlik önlemlerinin donanıma eklenmesiyle **maliyet artışı** ve üretici direnci.

- Standartların farklı uygulanması nedeniyle **uyumsuzluk sorunları**.
- Gerçek dünyada benzer saldırıların **güvenlik, itibar ve hukuki risk** doğurması.