BÜRKÜT-Proje Amacı

Amacım(Basit-İlk Çıkış):

Sadece bayrağı kapmak (CTF) değil; bir sistemi kendi ellerimle kurmak, ona saldırmak, wazuh siem ile saldırı anındaki logları analiz etmek, active response süreci ile saldırıları engelleme ve ardından o zafiyeti "kod" veya "konfigürasyon" seviyesinde kapatarak (Hardening) sistemi güvenli hale getirmektir.

Amacım(Geliştirilmiş):

Sadece bayrağı kapmak (CTF) değil; "Bürküt" kod adlı bu projede, modern kurumsal mimarilere uygun bir "Purple Team" laboratuvarını sıfırdan inşa etmektir. Temel hedefim; bir sisteme sızmak, saldırı anındaki logları merkezi bir SIEM üzerinde analiz etmek ve ardından o zafiyeti **öncelikle manuel olarak analiz edip kapatarak sistemin anatomisini kavramak; sonrasında ise edindiğim bu tecrübeyi** 'Infrastructure as Code' (IaC) felsefesiyle otomatize edilmiş scriptler (Bash/Ansible) yazarak kalıcı ve tekrarlanabilir hale getirmektir (Hardening).

Bunun yanı sıra, modern siber güvenliğin geleceği olan Yapay Zeka ajanlarını (MCP) saldırı ve kalite kontrol (QA) süreçlerine entegre ederek; insan zekası ile AI yeteneklerini "White Box", "Self-Correction" ve "Otonom Savunma" (Active Response) dinamikleriyle, sıkı güvenlik kilitleri (Fail-Safe) altında kıyaslamaktır.