# RedELK Aracı Kurulum ve Kullanım Rehberi

## 1. RedELK Nedir?

RedELK, Red Team’ler için geliştirilen bir SIEM çözümüdür. Cobalt Strike beacon logları, redirector trafiği, ekran görüntüleri ve keylogger çıktıları gibi verileri toplayarak merkezi olarak izlenmesini sağlar. ELK (Elasticsearch, Logstash, Kibana) mimarisi üzerinde çalışır ve zenginleştirilmiş log analizi sunar.

## 2. Mimari Yapı

- Filebeat: Logları toplar  
- Logstash: Veriyi işler ve filtreler  
- Elasticsearch: Veriyi depolar  
- Kibana: Görselleştirme ve analiz  
- Rsync: C2 sunucularından log eşitleme  
- Nginx: Güvenli erişim ve oturum yönetimi

## 3. Özellikler

- Cobalt Strike beacon ve komut loglarını indeksler  
- Redirector (Apache/HAProxy) loglarını analiz eder  
- Greynoise, TOR, kötü niyetli IP enrichment işlemleri  
- Alarmlar ve IOC tespiti ile Blue Team izlerini gözlemler

## 4. Kurulum Seçenekleri

1. Manuel kurulum (RedELK GitHub dokümantasyonuna göre)  
2. Ansible ile otomatik kurulum (TrustedSec tarafından sağlanan playbook)  
3. Workshop senaryoları ile kurulum (RedELK Workshop deposu)

## 5. Kullanım Akışı

1. Filebeat ile C2 ve redirector loglarının toplanması  
2. RedELK sunucusunda ELK stack kurulumu  
3. Python betikleriyle IOC zenginleştirme, tarama tespiti  
4. Kibana üzerinden Cobalt Strike aktivitelerinin izlenmesi

## 6. Hedef Kullanıcılar

- Red Team Operatörleri: Tüm operasyonel görünürlük  
- White Team / Denetleyiciler: İzleyici rolü ile genel erişim  
- Blue Team: Test sırasında yapılan keşif ve saldırı tespiti

## 7. Kaynaklar

- https://github.com/outflanknl/RedELK  
- https://github.com/outflanknl/RedELK/wiki  
- https://trustedsec.com/blog/automating-a-redelk-deployment-using-ansible  
- https://github.com/outflanknl/RedELK-workshop