Kali Purple Aracı - Eğitim Materyali

# 🎯 Kali Purple Nedir?

Kali Purple, Offensive Security tarafından geliştirilen, siber savunma (defensive security) ve tehdit tespiti amaçlı özel olarak yapılandırılmış bir Kali Linux dağıtımıdır.  
Hedefi, SOC analistleri, Blue Team uzmanları ve güvenlik operasyon ekiplerine kapsamlı araçlar sunmaktır.

# 🔧 Özellikleri

- Ağ izleme ve saldırı tespiti (IDS/IPS)  
- Olay müdahale araçları  
- Güvenlik analizi ve korelasyon sistemleri (SIEM)  
- Honeypot araçları  
- Tehdit istihbaratı analizi  
- MITRE ATT&CK uyumluluğu

# 📌 Kullanım Alanları

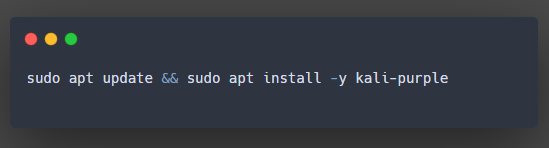
- SOC (Security Operations Center) eğitimleri  
- Tehdit avcılığı (Threat Hunting)  
- Ağ güvenliği izleme (Network Security Monitoring)  
- Honeypot simülasyonları  
- Güvenlik ihlallerine müdahale ve analiz

# 💻 Kurulum Seçenekleri

1. ISO dosyasını https://www.kali.org/get-kali/#kali-purple adresinden indir.  
2. VMware, VirtualBox ya da fiziksel cihaza kurulum yap.  
3. Önerilen minimum sistem gereksinimleri:  
 - 4 CPU  
 - 8 GB RAM  
 - 50 GB disk alanı  
4. Kurulumdan sonra ilk kullanıcı adı: kali, parola: kali

## 📥 Terminal Üzerinden Kurulum (Mevcut Kali Üzerinden)

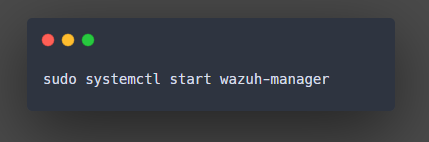
Mevcut bir Kali Linux sistemine Kali Purple araç setini yüklemek için aşağıdaki komutu kullanabilirsiniz:



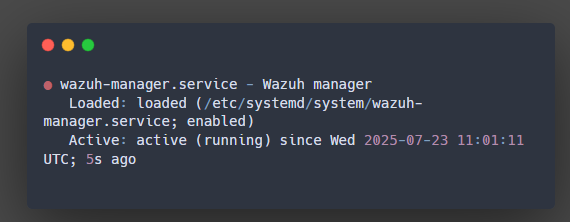
# 🧪 Kali Purple Arayüzü ve Araçlar

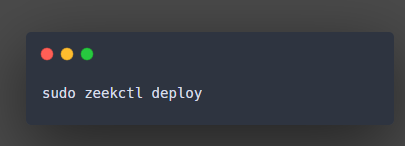
Kali Purple, klasik Kali XFCE masaüstü ortamını kullanır ancak "Purple Tools" adı altında özel menüler barındırır. Başlıca araç kategorileri:  
  
- SIEM Tools: Wazuh, OpenSearch, Kibana  
  
- IDS/IPS: Suricata, Zeek  
  
- Network Monitoring: Arkime, ntopng  
  
- Threat Intel: MISP, TheHive  
  
- Honeypot: Cowrie, Dionaea

# 🔍 Örnek Terminal Komutları

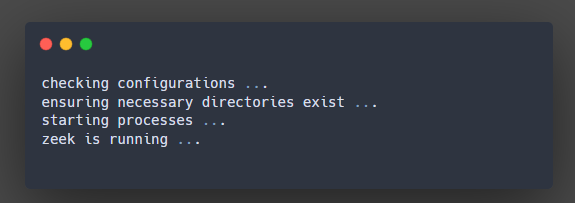
Wazuh servislerini başlatma:  


**Açıklama:**  
Wazuh, SIEM (Security Information and Event Management) işlevi gören bir güvenlik izleme aracıdır. Bu komut ile Wazuh servisi başlatılır.

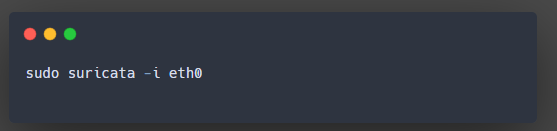


Zeek başlatma:  


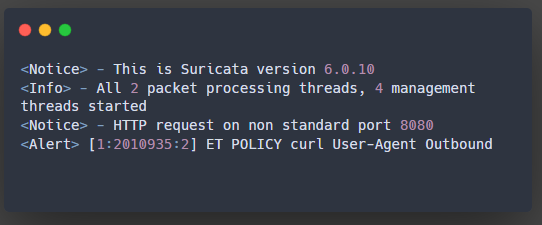
Açıklama: Zeek (eski adıyla Bro), ağ trafiğini analiz eden güçlü bir IDS sistemidir. Bu komut Zeek'in yapılandırmasını yükleyip servisleri başlatır.



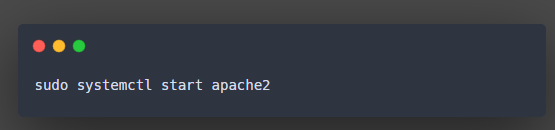
# Suricata ile Gerçek Zamanlı Ağ Analizi:



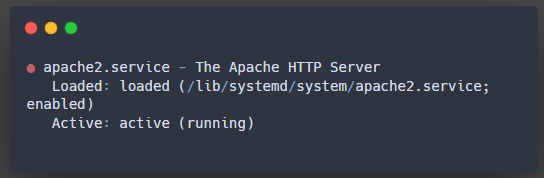
**Açıklama:**  
Suricata, ağ arabirimini dinleyerek trafiği analiz eder ve kural setlerine göre şüpheli aktiviteleri tespit eder.



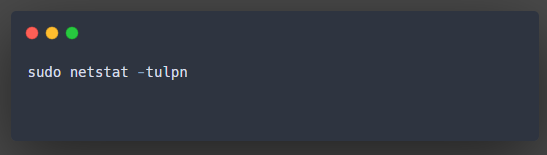
MISP Servisini Başlatmak:



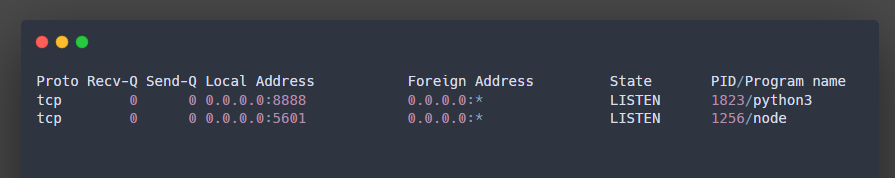
**Açıklama:**  
MISP (Malware Information Sharing Platform) web arayüzü üzerinden çalışır. Apache servisi ile başlatılır.



Netstat ile Güvenlik İzleme Portları:



**Açıklama:**  
Sistem üzerinde hangi servislerin çalıştığını ve dinlediği portları görmek için kullanılır.



# 📎 Notlar

- Kali Purple büyük ölçüde Blue Team odaklıdır.  
- Test ortamında kullanılması tavsiye edilir.  
- Ağ trafiği analiz araçları, sistem kaynaklarını yoğun kullanabilir.