**Malcolm Nedir?**

Malcolm, büyük ölçekli ağ trafiğini analiz etmek ve görselleştirmek için geliştirilmiş açık kaynaklı bir ağ güvenliği analiz platformudur. Özellikle IDS/IPS sistemlerinden gelen verileri merkezi bir şekilde analiz etmek isteyen siber güvenlik uzmanları tarafından tercih edilir.

Malcolm, pcap (packet capture) dosyalarını veya Zeek gibi IDS sistemlerinden gelen logları alarak, bunları Elasticsearch ve OpenSearch altyapısı üzerinde arayüzlerle (Kibana, Arkime gibi) kullanıcıya sunar.

**Temel Özellikleri**

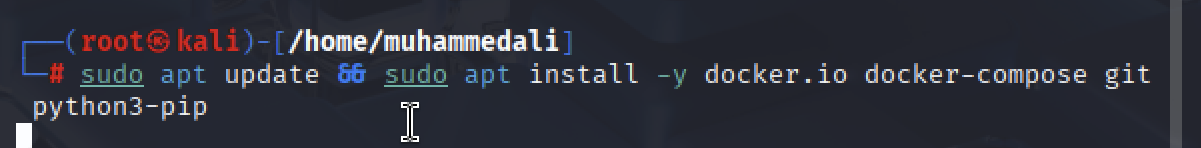
* **Pcap Analizi:** Ağdan alınan .pcap dosyalarını analiz ederek oturum bilgisi, DNS sorguları, HTTP trafiği, TLS oturumları gibi verileri çıkarır.
* **IDS/IPS Entegrasyonu:** Suricata ve Zeek gibi saldırı tespit sistemleri ile entegre çalışır.
* **Görsel Arayüz:** OpenSearch Dashboards (eski adıyla Kibana) ve Arkime ile grafiksel kullanıcı arayüzü sunar.
* **Elasticsearch/Logstash Tabanlı:** Logları indeksler, arama yapılabilir hale getirir.
* **Docker Tabanlı Kurulum:** Tamamen konteyner tabanlıdır, kolay kurulabilir.
* **Erişim Kontrolü:** Kimlik doğrulama sistemi ile güvenli erişim sağlar.
* **Günlük Otomasyonu:** Log’ları zamanlanmış şekilde analiz edebilir ve raporlar üretebilir.

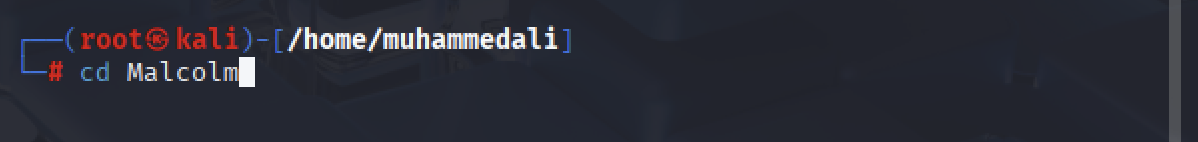
**Kullanım Alanları**

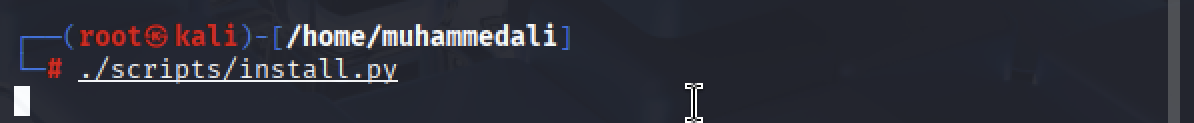
* **Saldırı Tespiti ve Olay İncelemesi:** Geniş pcap arşivlerini analiz ederek saldırı örüntülerini ortaya çıkarır.
* **Adli Bilişim:** Olay sonrası analiz için kullanılabilir. Örneğin, bir ihlal sonrası ağ trafiği incelemesi.
* **Ağ Güvenliği Görselleştirmesi:** Kurumsal ağ üzerindeki davranışları grafiksel olarak izleme imkânı sağlar.
* **Zeek/Suricata Log Analizi:** IDS/IPS loglarını merkezi olarak toplayıp analiz eder.
* **Tehdit İstihbaratı:** Şüpheli IP, domain veya imzaları trafiğe göre eşleştirebilir.

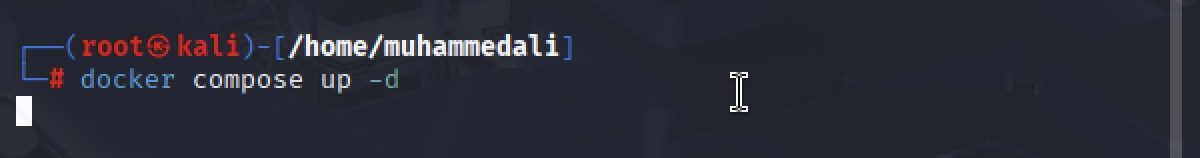
**Kurulum**

Malcolm genellikle Docker ile kurulur. Sistem gereksinimleri karşılandıktan sonra aşağıdaki adımlar izlenir:









**Öne Çıkan Entegrasyonlar**

* **Zeek:** Ağ protokol analizi
* **Suricata:** Saldırı imzası tespiti
* **Arkime:** Pcap görselleştirme
* **OpenSearch:** Log analizi ve arama
* **Filebeat/Logstash:** Log toplama

**Avantajlar**

* Kurumsal düzeyde güçlü analiz ve görselleştirme
* Büyük pcap dosyalarında yüksek performans
* Açık kaynak ve sürekli geliştirilen topluluk desteği
* Modüler yapı: Her bileşen ayrı ayrı yönetilebilir

**Dezavantajlar / Dikkat Edilmesi Gerekenler**

* Donanım ihtiyacı yüksek (özellikle RAM ve disk I/O)
* Docker ve Elasticsearch bilgisi gerektirir
* İlk kurulumda yapılandırma karmaşık olabilir
* Web arayüzleri HTTPS zorunlu, sertifika ayarları yapılmalı.