**1. Arkime Nedir?**

Arkime (eski adıyla Moloch), ağ üzerinden geçen tüm verileri (trafikleri) kaydedip, bu veriler üzerinde arama, filtreleme ve analiz yapmamıza olanak sağlayan, açık kaynak kodlu bir ağ güvenliği analiz aracıdır.

Ağdan geçen paketleri yakalar, diske kaydeder ve bu paketleri daha sonra analiz edebilmeniz için saklar. Sadece ham verileri değil, aynı zamanda bu verilere ait özet bilgileri de web arayüzünde sunar.

**2. Ne İşe Yarar?**

Arkime, aşağıdaki amaçlar için kullanılır:

* **Ağ trafiğini kaydetmek:** Hangi cihaz, ne zaman, nereye bağlandı?
* **Geçmiş olayları incelemek:** Örneğin bir siber saldırı olduğunda saldırganın izini sürmek.
* **Adli bilişim (Forensics) çalışmaları:** Şüpheli davranışları geriye dönük incelemek.
* **Gerçek zamanlı izleme:** Ağda anlık neler olduğunu görmek.
* **Eğitim ve analiz:** Öğrenciler için gerçek trafik verilerini analiz etmeyi öğretmek.

**3. Arkime Nasıl Çalışır?**

Arkime’nin 3 ana bileşeni vardır:

**1. Capture (Yakalama)**

* Ağ trafiğini dinleyip diske kaydeder.
* .pcap uzantılı dosyalar oluşturur.

**2. Elasticsearch**

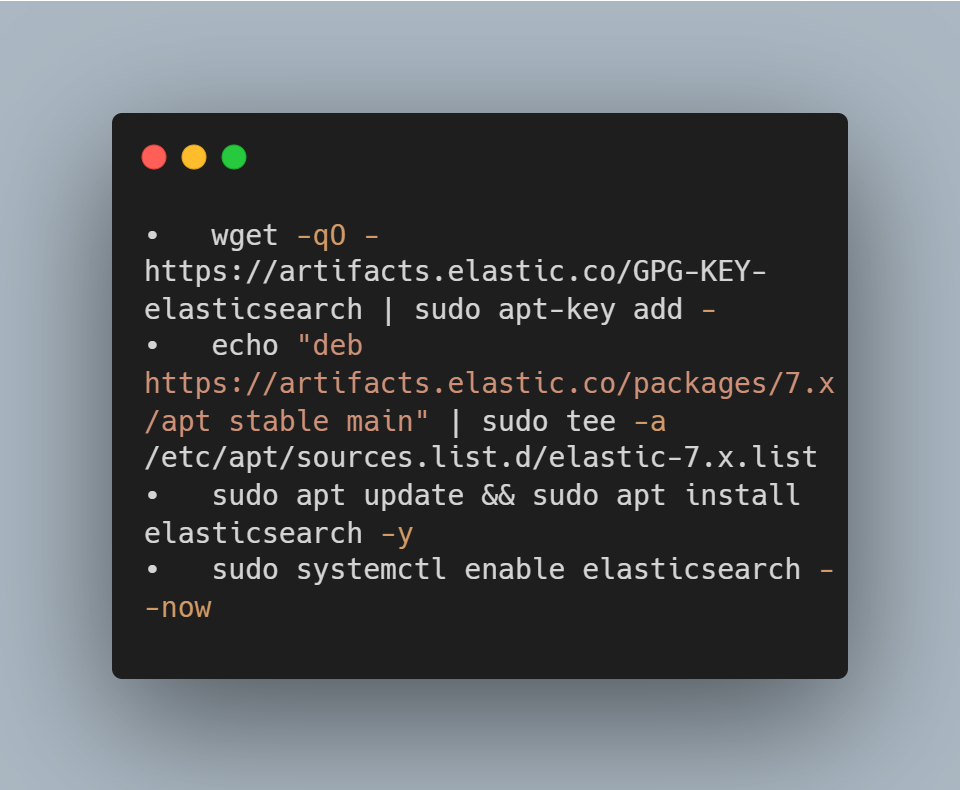
* Capture tarafından toplanan verileri indeksler.
* Böylece web arayüzünde hızlı arama yapılabilir.

**3. Viewer (Web Arayüzü)**

* Kaydedilen verilerin görselleştirilmesini sağlar.
* Web tarayıcı üzerinden kullanılır.

Adım Adım Kurulum: ***sudo apt update && sudo apt upgrade -y***

Elasticsearch Kurulumu:



Arkime Kurulumu:

***wget https://s3.amazonaws.com/files.molo.ch/builds/arkime\_4.3.0-1\_amd64.deb***

***sudo dpkg -i arkime\_4.3.0-1\_amd64.deb***

Yapılandırma:***cd /opt/arkime***

***sudo ./configure***

Bu adımda: kullanıcı adı, ağ arayüzü (eth0 gibi) ve şifre belirlemeniz istenecektir.

Elasticsearch Veritabanını Hazırlama:

***sudo /opt/arkime/db/db.pl http://127.0.0.1:9200 init***

Adım 6: Hizmetleri Başlatma (bash)

***sudo systemctl start arkimecapture***

***sudo systemctl start arkimeviewer***

Adım 7: Web Arayüzüne Giriş (cpp)

Tarayıcıdan:

***cpp***

***http://<sunucunun-ip-adresi>:8005***

Giriş bilgisi olarak kurulumda belirlediğiniz kullanıcı adı ve şifreyi girin.

**4. Artı ve Eksi Yönleri**

**Avantajlar:**

* Açık kaynak ve ücretsizdir.
* Büyük ağ trafiğini uzun süre saklayabilir.
* Kolay arayüz ile analiz yapmak kolaydır.
* Elasticsearch ile hızlı arama yapılabilir.

**Dezavantajlar:**

* Kaynak tüketimi yüksektir (özellikle Elasticsearch).
* İngilizce arayüz bazı kullanıcılar için zor olabilir.
* Kurulum aşamaları ilk başta karmaşık gelebilir.

Arkime, ağ güvenliği ve adli bilişim çalışmaları için çok güçlü ve ücretsiz bir araçtır. Eğitim ortamlarında öğrencilerin gerçek trafik üzerinde analiz yapabilmesini sağlar. Özellikle lise düzeyindeki siber güvenlik öğrencileri için hem öğretici hem de uygulamalı bir deneyim sunar.