**OSSIM**

**1. Nedir?**

OSSIM, "Open Source Security Information Management" yani **Açık Kaynak Güvenlik Bilgi Yönetim Sistemi** anlamına gelir. AlienVault firması tarafından geliştirilmiş, farklı güvenlik araçlarını bir araya getirerek merkezi bir güvenlik izleme ve yönetim sistemi sunan bir platformdur.

En basit tanımıyla: **Farklı güvenlik araçlarını tek bir yerden yönetmeni sağlayan bir sistemdir.**



**2. Ne İşe Yarar?**

OSSIM şu işlere yarar:

* Ağdaki tehditleri ve saldırıları algılar.
* Güvenlik olaylarını (log, alarm) toplar ve analiz eder.
* Tehditlere karşı otomatik veya manuel müdahale edilmesini sağlar.
* Kurumdaki güvenlik durumunu görselleştirir (dashboard'lar ile).

Kısaca: **Bir sistemde neler oluyor, kim saldırıyor, nereden geliyor gibi soruları cevaplayarak seni bilgilendirir.**

**3. Neden Önemlidir?**

* **Tümleşik Yapı:** Snort (IDS), Nagios (izleme), Nmap (tarama), OpenVAS (zafiyet tarama) gibi araçları tek bir çatı altında toplar.
* **Açık Kaynak:** Ücretsizdir ve geliştirilebilir.
* **Tehdit Algılama:** Anormal hareketleri, saldırı girişimlerini veya zafiyetleri kolayca tespit eder.
* **Zaman Kazandırır:** Tüm logları tek yerden analiz etmeye olanak tanır.

**Bir okulda, hastanede ya da şirkette bilgisayar ağı varsa, orayı korumak için OSSIM gibi bir sisteme ihtiyaç duyulur.**

**4. Nasıl Kurulur? (Linux Üzerinden Kullanım)**

OSSIM kurulumu için bir Linux sistem (özellikle Ubuntu veya Debian) gereklidir. Genelde ISO dosyasıyla kurulur. Basit kurulum adımları:

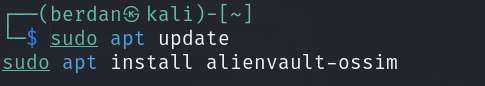
**OSSIM Kurulumu Adımları (Temel):**

1. AlienVault Resmi Sitesinden OSSIM ISO dosyasını indir.
2. ISO dosyasını bir sanal makineye (VirtualBox veya VMware) yükle.
3. Sanal makineyi başlat ve yönergeleri takip ederek kurulumu tamamla.
4. Kurulum sonrası IP adresi üzerinden web arayüzüne gir (örnek: **https://192.168.1.10).**
5. Giriş yaptıktan sonra sistem seni yapılandırma ekranına yönlendirecek.

**Gerekli Komutlar (örnek Debian üzerinde):**

**sudo apt update**

**sudo apt install alienvault-ossim**

****

Not: Genellikle tümleşik ISO kullanımı önerilir. Komutla kurulum ileri düzey bilgi ister.

**5. Örnek Bir Anlatım (Senaryo)**

**Senaryo: Lise Bilgisayar Laboratuvarı Güvende mi?**

Ahmet, okulun bilişim kulübü öğrencisidir. Bir gün okulun bilgisayar laboratuvarındaki sistemlerin yavaşladığını fark eder. Güvenlikten şüphelenir. Hocasıyla konuşur ve bir güvenlik çözümü araştırmaya başlar. OSSIM kurarak aşağıdaki işlemleri yapar:

1. Laboratuvardaki tüm bilgisayarlardan log (günlük) kayıtlarını toplamaya başlar.
2. OSSIM, bazı bilgisayarlardan internete şüpheli bağlantılar olduğunu tespit eder.
3. OSSIM’in içinde çalışan Snort sayesinde, bir virüsün yayılmakta olduğu fark edilir.
4. Ahmet ve hocası, virüslü makineleri izole ederek yayılmasını durdurur.
5. Okul yönetimi Ahmet’i tebrik eder, bilişim kulübü takdir toplar 🎉