**SECURITY ONION**

**1. Nedir?**

**Security Onion**, ağ güvenliği için geliştirilmiş **Linux tabanlı açık kaynaklı bir izleme ve saldırı tespit sistemidir (IDS/NSM)**.

Basitçe şöyle diyebiliriz:

**Security Onion = Güvenlik için Soğan Katmanları gibi koruma sağlayan bir sistemdir.**

İçerisinde birden fazla güçlü güvenlik aracı bir arada çalışır (Snort, Suricata, Zeek, Wazuh, Kibana vb.).



**2. Ne İşe Yarar?**

Security Onion şu işleri yapar:

* Ağ trafiğini dinler ve analiz eder.
* Saldırıları tespit eder (IDS).
* Sistem olaylarını (logları) toplar ve görselleştirir.
* Güvenlik analistinin ağdaki tüm hareketleri izlemesini sağlar.

Örneğin: **Okul ağına bir saldırı olursa, bu saldırıyı tespit edip seni uyarır.**

**3. Neden Önemlidir?**

* **Tümleşik:** İçinde Snort, Zeek, Suricata, Wazuh gibi araçlar entegredir.
* **Kolay Arayüz:** Gelişmiş görsel arayüzü (Kibana, Squert) sayesinde analiz yapmak kolaydır.
* **Gerçek Zamanlı İzleme:** Ağda ne olup bittiğini anlık olarak görebilirsin.
* **Eğitim İçin Süper:** Siber güvenlik öğrenen öğrenciler için mükemmel bir laboratuvar ortamı sunar.

Kısaca: **Güvenlik uzmanlarının ağdaki kötü niyetli faaliyetleri izlemesi için güçlü bir gözdür.**

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

Security Onion genellikle bir ISO dosyası ile kurulur. Sanal makine ya da fiziksel makineye yüklenebilir.

**🧩 Kurulum Adımları:**

1. Resmi siteden ISO dosyasını indir.
2. ISO'yu bir sanal makineye (VirtualBox, VMware) bağla.
3. Makineyi başlat, kurulum yönergelerini takip et.

**sudo sosetup**

****

1. Sistem seni adım adım yönlendirir (hangi araçlar kurulacak, ağ kartı vs.).
2. Kurulumdan sonra web arayüzüne şu şekilde girilir:

**https://[senin-ip-adresin]**

**Tavsiye:**

* Minimum 8 GB RAM ve 2 CPU önerilir.
* Sanal ağ trafiğini analiz etmek için **“bridged adapter”** kullan.

**5. Örnek Bir Anlatım (Senaryo):**

**Senaryo: Okul Ağına Sızma Girişimi**

Lise öğrencisi Zeynep, siber güvenlik kulübünde görevlidir. Okulun ağı yavaşlamaktadır. Öğretmeni, Zeynep’ten bu sorunu araştırmasını ister.

Zeynep, bir sanal makineye **Security Onion** kurar ve okul ağına bağlar.

* Zeek, ağda bazı bilgisayarların şüpheli IP’lerle iletişim kurduğunu gösterir.
* Suricata, bu bağlantıların bir “botnet” ile ilişkili olduğunu bildirir.
* Wazuh, birkaç sistemde şüpheli dosyalar olduğunu log'lar.
* Zeynep, bu bilgileri okulun teknik sorumlusuna sunar.
* Sorun çözülür ve ağ tekrar güvenli hale gelir
* Bu olaydan sonra Zeynep, okuldaki siber güvenlik kulübüne başkan olur.