**Security Onion: Güvenlik İzleme ve Sızma Tespiti Platformu**

**Security Onion Nedir?**

**Security Onion**, ağ güvenliği izleme, saldırı tespiti (IDS), olay analizi ve tehdit avcılığı (threat hunting) için kullanılan açık kaynaklı bir Linux dağıtımıdır. Doug Burks tarafından geliştirilen bu sistem, genellikle siber güvenlik operasyon merkezleri (SOC), tehdit avcıları ve adli bilişim uzmanları tarafından kullanılır. Adını “soğan” katmanlarından alır; çünkü güvenlik, katmanlı bir yapıyı gerektirir.

Security Onion, sızma testi aracı olmasa da, sızma testleri sonrasında tespit edilen saldırıların analizinde, tehditlerin ortaya çıkarılmasında ve ağda anomali izleme süreçlerinde çok etkili bir çözümdür.

**Temel Özellikler**

Security Onion, birçok güçlü açık kaynaklı güvenlik aracını entegre bir şekilde sunar. Bu araçlardan bazıları şunlardır:

* **Suricata / Zeek (eski adıyla Bro)**: Ağ tabanlı saldırı tespit sistemi (NIDS).
* **Wazuh / OSSEC**: Host tabanlı saldırı tespit sistemi (HIDS).
* **Elasticsearch, Logstash, Kibana (ELK stack)**: Veri toplama, analiz ve görselleştirme.
* **TheHive & Cortex**: Olay müdahalesi ve tehdit istihbaratı entegrasyonu.
* **CyberChef**: Kod çözme, veri işleme, analiz için güçlü bir araç.
* **Stenographer**: Ağ trafiğini sürekli kaydeden paket yakalama sistemi.

Bu araçların birleşimi sayesinde Security Onion, sadece saldırı tespiti değil aynı zamanda tehdit avı, adli analiz ve sürekli güvenlik izlemede oldukça kapsamlı bir platform sunar.

**Kullanım Alanları**

* Ağ trafiği analiz etmek
* Anormal davranışları tespit etmek
* Olay müdahalesi ve kök neden analizi yapmak
* Sızma testi sonuçlarını loglarda takip etmek
* Güvenlik politikalarını doğrulamak
* IDS/IPS sistemlerini yapılandırmak ve gözlemlemek

**Kurulum ve Kullanım**

Security Onion, ISO formatında bir Linux dağıtımıdır. Fiziksel makinelerde, sanal makinelerde veya bulut ortamlarında kurulabilir. Ayrıca Docker ve Kubernetes ortamlarında dağıtımı da desteklenmektedir.



**Kurulum Sonrası Sistem Yapılandırma Komutu :**

**metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.**

**Avantajları**

* ✅ **Ücretsiz ve açık kaynaklı**
* ✅ **Modüler ve genişletilebilir yapı**
* ✅ **Grafik arayüzlerle kullanım kolaylığı**
* ✅ **Gerçek zamanlı uyarı ve analiz**
* ✅ **Geniş topluluk desteği**
* ✅ **Siber tehditleri proaktif yakalama olanağı**
* ✅ **Sızma testi sonrası analiz için ideal**

**Dezavantajları / Zorluklar**

* ❌ Kurulum ve yapılandırma başlangıçta karmaşık olabilir
* ❌ Yüksek sistem kaynağı tüketimi (özellikle ELK)
* ❌ Ağ trafiği çok yoğunsa performans düşebilir
* ❌ IDS imzalarının düzenli olarak güncellenmesi gerekir

**Security Onion ile Entegrasyon Örnekleri**

* **Metasploit**: Simüle edilmiş saldırı sonrası logları incelemek
* **Cuckoo Sandbox**: Malware analizi ve sonuçlarını Security Onion’a aktarmak
* **Sysmon + Wazuh**: Host tabanlı olay izleme ve korelasyon