**Zeek (Bro) Nedir?**

**Zeek**, daha önceki adıyla **Bro**, ağ trafiğini analiz etmek için kullanılan, açık kaynaklı, güçlü ve esnek bir **network security monitoring (NSM)** ve olay analiz aracıdır. Geleneksel saldırı tespiti sistemlerinden (IDS) farklı olarak, sadece saldırı imzalarını aramaz; trafik içeriğini zenginleştirerek detaylı günlük kayıtları üretir. Bu sayede siber tehdit avcılığı, olay inceleme, adli bilişim ve güvenlik denetimi gibi çok çeşitli alanlarda kullanılır.

**Zeek’in Temel Özellikleri**

1. **Protokol Analizi**  
   HTTP, DNS, SSL/TLS, FTP, SMTP gibi birçok yaygın protokolü tanır ve ayrıştırır.
2. **Olay Tabanlı Mantık**  
   Zeek, her ağ olayına özel betikler (scripts) aracılığıyla tepki verir. Örneğin; şüpheli bir bağlantı tespit edilirse özel bir log kaydı veya e-posta uyarısı oluşturulabilir.
3. **Zengin Loglama**  
   Zeek, ağda olup biten her şeyi farklı log dosyalarında ayrıntılı şekilde tutar:
   * conn.log: Bağlantı kayıtları
   * http.log: HTTP istekleri
   * dns.log: DNS sorguları
   * ssl.log: TLS el sıkışmaları
   * files.log: Transfer edilen dosyalar vb.
4. **Genişletilebilir Script Sistemi**  
   Özel analizler yapmak için Zeek Script diliyle kolayca yeni kurallar yazılabilir.
5. **Pasif Çalışır**  
   Ağ üzerinde herhangi bir değişiklik yapmadan, genellikle SPAN port ya da TAP cihazı üzerinden trafiği dinleyerek çalışır.
6. **Topluluk ve Modül Desteği**  
   Zeek topluluğu tarafından geliştirilen çok sayıda modül, eklenti ve entegrasyon desteği bulunur (Elastic, Kafka, SIEM vs.).

**Kullanım Alanları**

* Ağ davranış analizi
* Olay müdahalesi ve adli bilişim
* Tehdit avcılığı (threat hunting)
* Veri ihlali tespiti
* Dosya aktarım takibi
* Güvenlik denetimleri

**Zeek Kurulumu (Debian/Ubuntu/Kali İçin)**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Bu komut, sistem paketlerini günceller. Eğer güncellenecek paketler varsa onları indirip yükler.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Bu işlem Zeek’in kaynak koddan derlenmesi için gerekli kütüphaneleri kurar.

metin, yazı tipi, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Ve artık çalıştırıyoruz;

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Avantajları**

* ✅ Derin ağ analizi sağlar (paket düzeyinin ötesinde).
* ✅ Yüksek özelleştirilebilirlik (script tabanlı).
* ✅ Pasif dinleme sayesinde güvenli.
* ✅ Zengin log yapısı ile olay incelemesi kolaylaşır.
* ✅ Topluluk desteği geniştir.
* ✅ SIEM ve Elastic Stack ile kolay entegre edilebilir.

**Dezavantajları / Zorlukları**

* ❌ Yeni başlayanlar için kurulum ve kullanım eğrisi dik olabilir.
* ❌ Loglar çok ayrıntılı olduğu için büyük ağlarda ciddi disk alanı ve analiz gücü gerekebilir.
* ❌ Zeek Script dili başlangıçta karmaşık gelebilir.
* ❌ Gerçek zamanlı uyarılar için ek entegrasyon gerekebilir (örneğin ELSA, Splunk, Kibana gibi).

**Sonuç**

**Zeek**, siber güvenlik dünyasında ağ olaylarının görünürlüğünü artıran en güçlü açık kaynak araçlardan biridir. Klasik IDS sistemlerinden farklı olarak sadece imzaları değil davranışları da analiz eder. Ağınıza ne girdiğini ve ne çıktığını anlamak, potansiyel tehditleri erken fark etmek ve olay sonrası incelemeler yapmak için Zeek eşsiz bir çözümdür.

İyi yapılandırılmış bir Zeek sistemi, siber tehditleri tespit etmede ve analiz etmede güvenlik ekiplerine büyük avantaj sağlar.