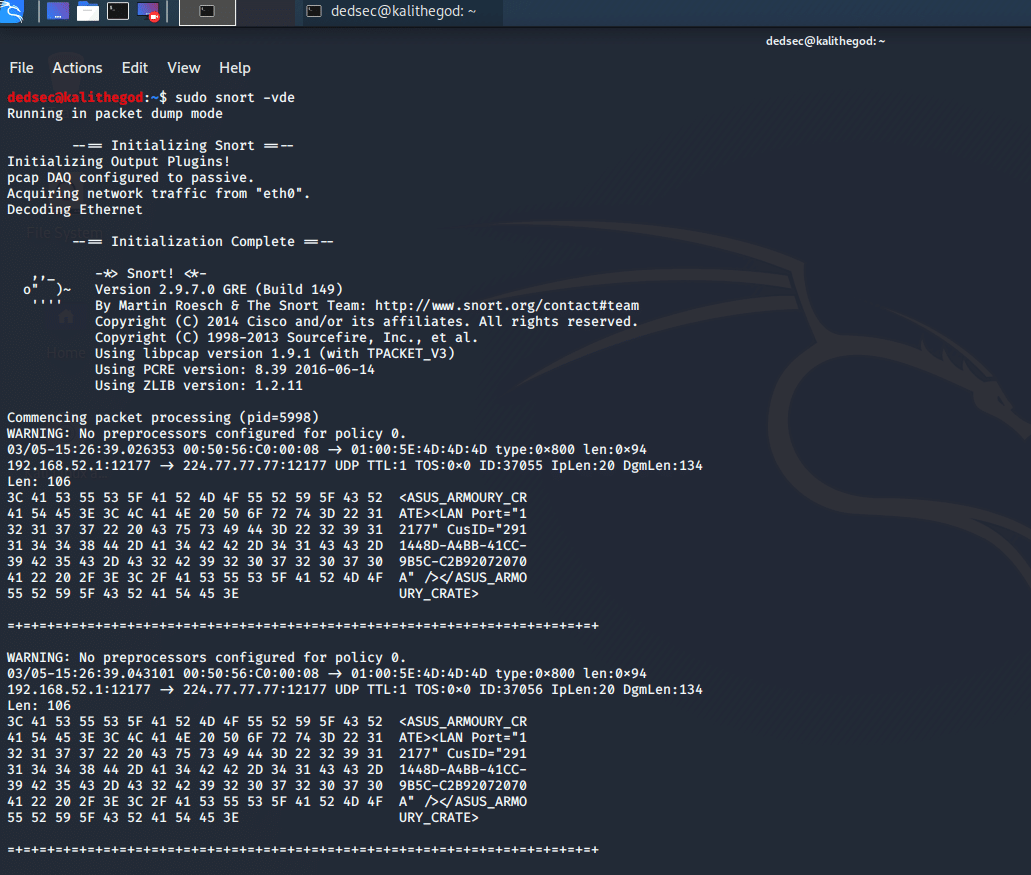
**Snort Nedir?**

Snort, açık kaynak kodlu bir Network Intrusion Detection System (NIDS) yani Ağ Saldırı Tespit Sistemi’dir. Cisco tarafından geliştirilmiş ve desteklenmektedir. Ağ trafiğini gerçek zamanlı olarak izler, analiz eder ve potansiyel tehditlere karşı sistem yöneticisini uyarır. Snort, aynı zamanda saldırı önleme sistemi (IPS) olarak da yapılandırılabilir.

Temel amacı; ağdan geçen veri paketlerini inceleyerek belirli kurallara göre zararlı trafiği tespit etmek, kaydetmek veya engellemektir.



Snort’un başlatılması ve paketleri terminalde detaylı olarak göstermek üzere yapılandırılması sürecini yansıtır.

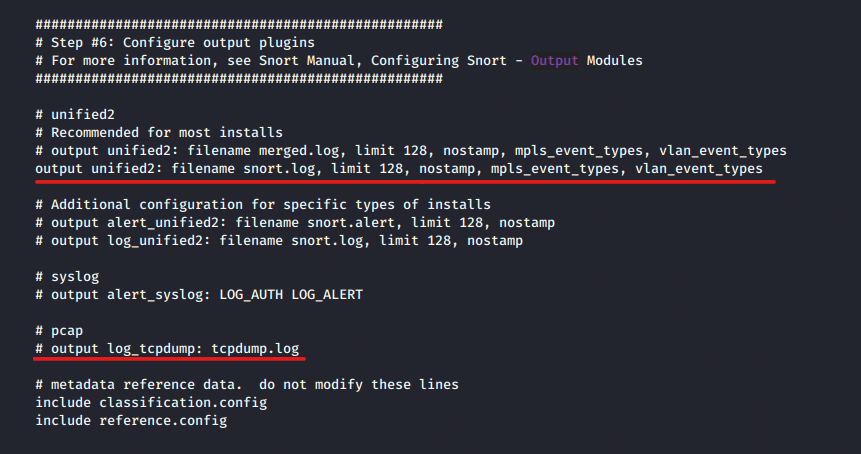
**Snort Ne İşe Yarar?**

* **Gerçek zamanlı trafik izleme:** Ağ üzerinden geçen tüm trafiği analiz eder.
* **Kural tabanlı saldırı tespiti:** XSS, SQLi, port tarama, DoS saldırıları gibi çeşitli tehditleri algılayabilir.
* **Loglama:** Olay günlükleri oluşturur ve şüpheli aktiviteleri kayıt altına alır.
* **IDS/IPS olarak yapılandırılabilir:** Sadece uyarı verme modunda (IDS) çalışabileceği gibi, saldırıları engelleyecek şekilde (IPS) de konfigüre edilebilir.

**Çalışma Modları**

Snort üç farklı modda çalışabilir:

| **Mod** | **Açıklama** |
| --- | --- |
| **Sniffer Mode** | Paketleri analiz eder, çıktıyı terminale yazdırır. |
| **Packet Logger Mode** | Paketleri analiz eder ve dosyaya loglar. |
| **Network Intrusion Detection Mode (NIDS)** | Kurallar ile trafiği değerlendirip saldırıları tespit eder. |

****

Exploring Snort” dokümanından alınmış; Snort’un verbose modda protokol analizini terminalde sunduğu ekranı içeriyor.

**Temel Kullanım Örneği**

Sniffer modunda çalıştırmak için: ***sudo snort -i eth0***

Kural dosyasıyla saldırı tespiti yapmak için:

***sudo snort -A console -q -c /etc/snort/snort.conf -i eth0***

* **-A console:** Çıktıyı terminale verir.
* **-q:** Sessiz mod.
* **-c:** Konfigürasyon dosyası.
* **-i:** Kullanılacak ağ arayüzü.

**Snort Kuralları (Rules)**

Snort’un gücü kurallarındadır. Kurallar belirli bir kalıba uyan ağ trafiğini tespit eder. Örnek bir Snort kuralı:

**alert tcp any any -> 192.168.1.0/24 80 (msg:"HTTP bağlantı algılandı"; sid:1000001;)**

Bu kural, hedef IP bloğundaki 80 numaralı porta gelen tüm TCP bağlantılarını tespit eder ve loglar.

**Avantajları**

* Ücretsiz ve açık kaynak.
* Esnek ve genişletilebilir kurallar dizisi.
* Gerçek zamanlı tehdit algılama sağlar.
* Dünya genelinde büyük bir topluluk desteği vardır.