SAKARYA ÜNİVERSİTESİ

SAKARYA ÜNİVERSİTESİ

BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ

AĞ GÜVENLİĞİ DERSİ

SALDIRI TESPİT VE ÖNLEME SİSTEMLERİ PROJESİ

A KRİTERİ

AD SOYAD: BARIŞ YILMAZ, CEMAL ASLAN, AHMET FARUK SEZGENÇ

ÖĞRENCİ NO: G191210303, G191210387, G140910027

E-POSTA: xbarisyilmaz@gmail.com, cemalss_1999@outlook.com, g140910027@sakarya.edu.tr

ÖĞRENİM TÜRÜ/ŞUBE: 1/A

SNORT

Snort, açık kaynak kodlu ve **kural** mimarisiyle çalışan bir saldırı tespit ve önleme sistemidir (IDS/IPS).

Kötü amaçlı ağ hareketlerinin tanımlamasında yardımcı olan kurallar kullanır. Bu kurallar kendileri ile eşleşen paketleri bulmak için kullanılmakta ve sistem kullanıcılarına gerekli uyarıları yapmaktadır.

Snort, saldırı tespitini ağ paketlerini inceleyerek IP ağları üzerinde gerçek zamanlı trafik analizi yaparak sağlamaktadır.

Snort'un bir ağ üzerindeki olayları gözlemleyebilmek için ağ üzerinde iletilen tüm paketleri gözlemlemesi gereklidir. Ancak yüksek hacimli bir trafiği izlemeye uygun değildir.

Snort, GNU lisanslıdır. Windows ve Linux üzerinde çalışabilmektedir. Kurulumu için doğrudan derlenmiş kodlar kullanılabileceği gibi kaynak kodları snort makinesinde derlenerek de yapılabilmektedir.

İçerik arama, arabellek taşıma ve port taraması gibi konularda da kullanılmaktadır.

2013'ten sonra Cisco tarafından satın alınıp geliştirilmiştir.

Kurumlar genelde satın aldıkları ticari **IPS veya IDS** sistemini kullanırlar.

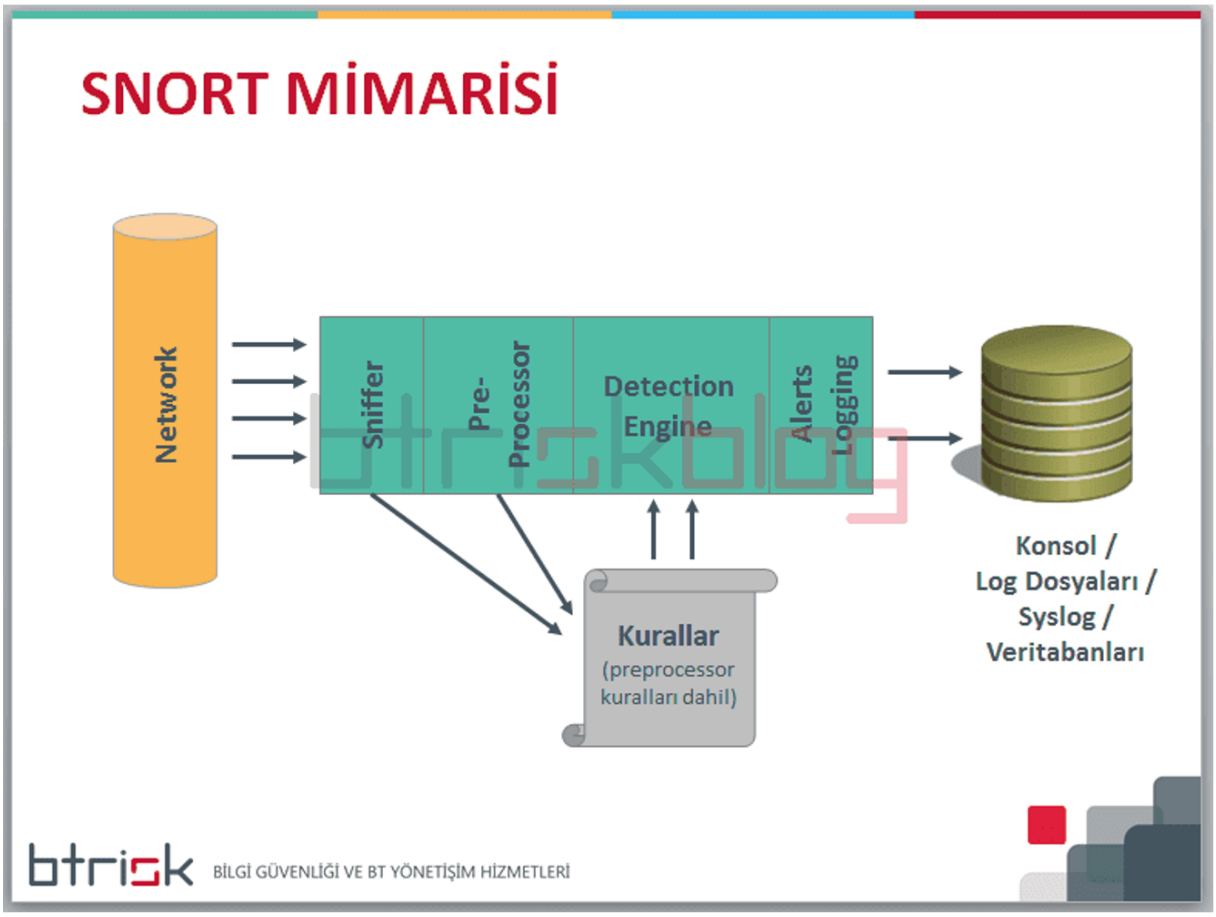
IDS (Intrusion Detection System)

IDS, güvenlik sistemlerinin zararlı hareketlerini tanımlayan yani saldırıları tespit etmeyi amaçlayan bir sistemdir.

IPS (Intrusion Prevention System)

IPS, ağ trafiği içindeki zararlı hareketlerin veya bağlantıların tespitiyle birlikte, önlenmesi, durdurulması için kullanılan bir güvenlik sistemidir.

SNORT MİMARİSİ



Sniffers : Ağ arayüzünden çeşitli tiplerdeki paketleri alır ve bir sonraki snort bileşeni için hazırlar.

Pre-Processors : Paket başlıklarındaki anormalliklere göre saldırı belirlemeye çalışır. Pre-processor genellikle parça parça gelen büyük veri parçalarını bir araya getirmek için çalışır.

Detection Engine : Paket içindeki saldırı türlerini belirlemekten sorumludur. Bu saldırıları tespit etme noktasında da snort kurallarını kullanmaktadır. Snort kurallarında belirtilmiş bir saldırı işareti ile preprocessor bileşeninden gelen paket içeriği karşılaştırılır ve tehlikeli bir durum varsa kural başlığında yer alan eylem gerçekleştirilmek için bir sonraki modüle geçilir.

Alerts Logging : Detection engine bileşeni paket içeriğinin hangi kural ile örtüştüğünü tespit ettikten sonra kural başlığında belirtilen eyleme göre loglama, uyarı verme gibi işlemler yapar.

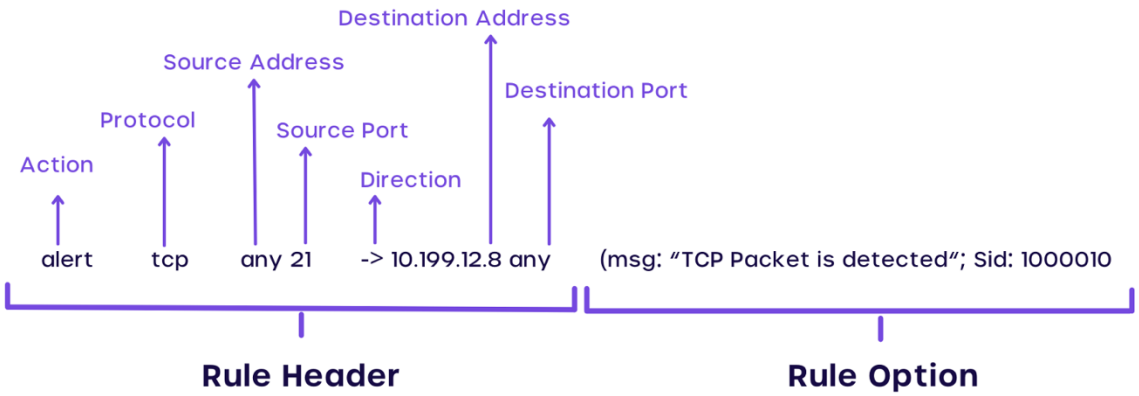
SNORT KULLANIM MODLARI

PASSIVE MOD : IDS görevi görür. Drop kuralları yüklenmez, paket drop edilemez.

INLINE MOD : IPS görevi görür. Paketler drop edilebilir.

INLINE-TEST MODE : trafiği etkilemeden davranışın değerlendirilebilmesini sağlar. Paketler drop edilebilir.

SNORT KURAL YAPISI



Kendimiz yazacağımız kuralları snort klasörü içerisindeki local.rules dosyasına yazarız.

Actionslar;

alert : Kurallara uyan paketleri belirleyerek o paketler için uyarı vermektedir.

pass : Paketleri önemsemeyerek basit bir şekilde geçirilmesini sağlar.

log : Alertde olduğu gibi kurallara uyan paketleri alır ancak uyarı vermez. Sadece log olarak kaydeder.

activate : İlk olarak alarm vererek sonrasında başka bir kuralı etkinleştirmektedir.

dynamic : Activeden gelen kuralı bekler, active edilince de kuralları uygular.

drop : Paketin drop edilerek log olarak kaydedilmesi sağlar.

sdrop : Paketin drop eder fakat log olarak kaydedilmez.

reject : Paketin drop edilerek log olarak kaydedilmesi sağlar ve protokole göre hata mesajı üretir.

ÖRNEK KURAL

drop icmp any any -> $HOME_NET any (msg:"ICMP Packet! DOS/DDOS Attempt!!"; sid:10000001; rev:1; detection_filter:track by_dst, count 5, seconds 10;)

$HOME_NET -> snort.conf dosyasında verilen ip adresi

msg -> loglanırken görüntülenecek mesaj

sid (snort rule id) -> ilk 1.000.000 rezervedir, snortun kendi kuralları için kullanılır.

rev -> revizyon numarası

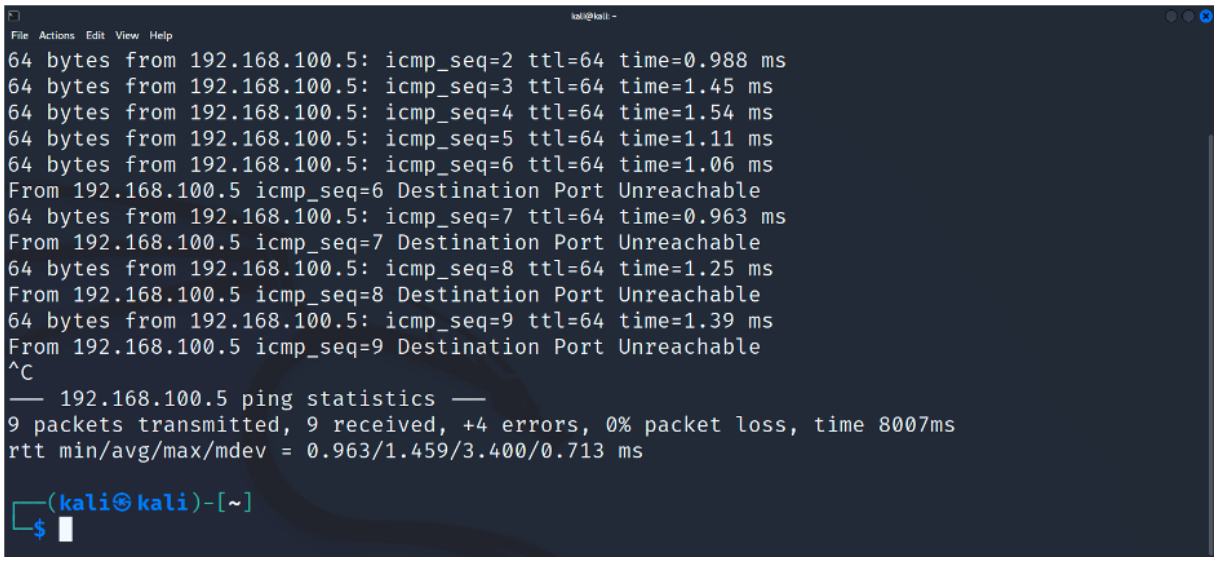
direction_filter -> kuralın uygulamaya geçeceği ön koşul

track by_dst veya track by_src -> eventin destination veya source ipye göre takibi

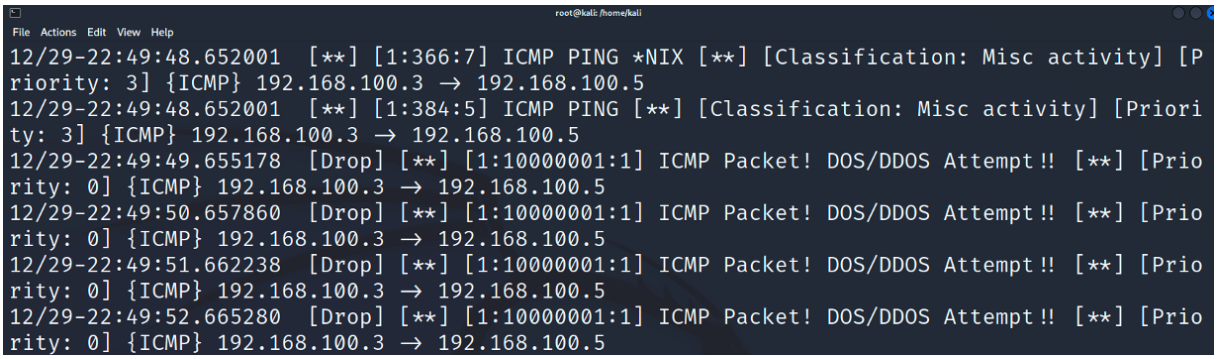
count -> eventlerin adedi

seconds -> counta giren parametrenin gerçekleşeceği zaman aralığı

Bu kural ile y bilgisayarından snort kurulu olan x bilgisayarına ping atarsak;



Görüleceği üzere 5. İcmp paketinden sonra giden her paket x tarafından drop edilmiş. X'in snort console'unda görünenen loglara bakıcak olursak;



İlk 5 paket için snortun kendi rules dosyalarında bulunan kurallar çalışıyor ve icmp paket bilgileri veriliyor, 6. ve sonraki paketler içinse bizim kendi local.rules dosyasına yazdığımız kural çalışıyor ve paketlerin drop edildiği bilgisi ile mesajımız yazılıyor.

KAYNAKÇA

https://snort.org

https://stackoverflow.com