T.C. SAKARYA ÜNİVERSİTESİ
BİLGİSAYAR VE BİLİŞİM BİLİMLERİ FAKÜLTESİ

BSM471 – AĞ GÜVENLİĞİ

PROJE

Saldırı Tespit Ve Önleme Sistemleri

Hazırlayan

Ferdi Sönmez

B211210375

ferdi.sonmez3@ogr.sakarya.edu.tr

İçindekiler

Saldırı Tespit Sistemleri (STS)

(Intrusion Detection Systems (IDS)), ağlara veya sistemlere karşı yapılan kötü niyetli aktiviteleri ya da politika ihlallerini izlemeye yarayan cihaz ya da yazılımlardır. Tespit edilen herhangi bir aktivite veya ihlal, ya bir yöneticiye bildirilir ya da bir güvenlik bilgi ve olay yönetimi (SIEM) sistemi kullanılarak merkezi olarak toplanır. SIEM sistemi, çeşitli kaynaklardan gelen çıktıları birleştirir ve kötü niyetli alarmı yanlış alarmlardan ayırmak için alarm filtreleme teknikleri kullanır.

Antivirüs yazılımından bütün ana omurga ağının trafiğini izleyen hiyerarşik sistemlere kadar çeşitleri olan geniş bir STS yelpazesi vardır. En yaygın sınıflandırmalar, ağ saldırı tespit sistemleri (NIDS) ve bilgisayar tabanlı saldırı tespit sistemleri (HIDS) 'dir. Önemli işletim sistemi dosyalarını izleyen sistem, bir HIDS örneğiyken gelen ağ trafiğini analiz eden sistem, bir NIDS örneğidir. STS'yi tespit etme yaklaşımına göre sınıflandırmak da mümkündür: En iyi bilinen çeşitleri, imza tabanlı yaklaşım (kötü modelleri tanıma, örnek zararlı yazılım) ve anomali tabanlı yaklaşım ("iyi" trafik modellerinden sapmaları tespit etmek, makine öğrenmeye bağlıdır). Bazı STS'lerin tespit edilen saldırılara cevap verme yeteneği vardır. Yanıt verme özellikli sistemler genelde bir saldırı önleme sistemi (Intrusion Prevention Systems (IPS)) olarak adlandırılır.

Bu sistemin temel görevi kötü niyetli aktiviteleri belirlemek ve saldırının türünü rapor etmektir.Saldırı Tespit Sistemleriyle (Intrusion Detection Systems) Saldırı Engelleme Sistemleri (Intrusion Prevention Systems) arasındaki temel fark; saldırı tespit sistemlerinin, saldırıları sadece tespit edip raporlamasına karşılık saldırı engelleme sistemlerinin, yapılan saldırıları önleme yeteneğine sahip olmasıdır.

Saldırı Tespit Sistemleri; saldırıları tespit ettikleri ortama ve tespit yöntemlerine göre sınıflandırılabilir.

Ağ Tabanlı Saldırı Tespit Sistemi

Ağ saldırı tespit sistemleri (NIDS), ağdaki tüm aygıtlardan gelen trafiği izlemek için ağ içindeki stratejik bir noktaya veya noktalara yerleştirilir. Alt ağın tamamında geçen trafiği analiz eder ve alt ağlarda geçirilen trafiği bilinen atakların kütüphanesiyle eşleştirir. Bir saldırı tespit edilir edilmez veya anormal bir davranış algılanırsa, yöneticiye uyarı gönderilebilir. İdeal olarak, gelen ve giden tüm trafiği tarar, ancak bunu yapmak ağın genel hızını bozan bir tıkanıklık oluşturabilir. OPNET ve NetSim, simülasyon ağı saldırı tespit sistemleri için yaygın olarak kullanılan araçlardır. Sisteme etki özelliğine göre ağ tabanlı saldırı tespit sistemi tasarımı sınıflandırıldığında iki tür vardır: çevrimiçi ve çevrimdışı ağ tabanlı saldırı tespit sistemi, sırasıyla inline ve tap-modu olarak adlandırılır. Çevrimiçi ağ tabanlı saldırı tespit sistemi, ağ ile gerçek zamanlı ilgilenir. Bir saldırı olup olmadığına karar vermek için Ethernet paketlerini

analiz eder ve bazı kurallar uygular. Çevrimdışı ağ tabanlı saldırı tespit sistemi, depolanan verileri ele alır ve bir saldırı olup olmadığına karar vermek için bazı işlemlerden geçirir.

Bilgisayar Tabanlı Saldırı Tespit Sistemi

Bilgisayar tabanlı saldırı tespit sistemi (HIDS), ağdaki tek tek makinelerde veya cihazlarda çalışır. Bir bilgisayar tabanlı saldırı tespit sistemi, gelen ve giden paketleri yalnızca üzerinde çalıştığı izler ve şüpheli durum algılanırsa kullanıcıyı veya yöneticiyi uyarır. Sistemde bulunan dosyaların anlık görüntüsünü alır ve onu önceki anlık görüntü ile eşleştirir. Kritik sistem dosyaları değiştirilmiş veya silinmişse, araştırmak için yöneticiye bir uyarı gönderilir. Bilgisayar tabanlı ağ saldırı tespit sisteminin kullanımına bir örnek olarak bunu kritik makinelerde görmek mümkündür; bu makinelerin yapılandırmalarını değiştirmesi beklenmemektedir.

Saldırı tespit sistemleri, özel araçlar ve bal küpü kullanılarak sisteme özgü hale getirilebilir.

Tespit Yöntemi

İmza Tabanlı

İmza tabanlı saldırı tespit sistemi, ağ trafiğinde örneğin bayt dizileri veya kötü amaçlı yazılım tarafından kullanılan kötü amaçlı komut dizileri gibi belirli modeller aramak amacıyla saldırıların tespit edilmesi anlamına gelir. Bu terminoloji, tespit edilen modelleri imza olarak ifade eden anti-virüs yazılımından kaynaklanmaktadır. İmza tabanlı saldırı tesit sistemi bilinen saldırıları kolayca tespit edebilmesine rağmen, mevcut modeli olmayan yeni saldırıları tespit etmesi imkânsızdır.

Anomali Tabanlı

Anormalliğe tabanlı saldırı tespit sistemleri, kötü niyetli yazılımların hızla gelişmesi nedeniyle bilinmeyen saldırıları tespit etmek için tasarlandı. Temel yaklaşım makine dilini kullanarak güvenilir öğrenme modeli oluşturmak daha sonra yeni davranışları bu modelle karşılaştırmaktır. Bu yaklaşım daha önce bilinmeyen saldırıların tespit edilmesine olanak tanımasına rağmen, yanlış alarmlar üretebilir: önceden bilinmeyen yasal etkinlik de kötü alarm olarak sınıflandırılabilir.

Anomali tabanlı saldırı tespit sistemleri olarak adlandırılabilecek yeni türler, Gartner tarafından Kullanıcı ve Varlık Davranış Analizi (UEBA) (kullanıcı davranışı analiz kategorisinin bir gelişimi) ve ağ trafiği analizi (NTA) olarak görülüyor. Özellikle NTA, bir kullanıcı makinesini veya hesabı tehlikeye atan hedefli harici saldırıların yanı sıra kötü niyetli içerikleri de ele alır. Gartner, bazı kuruluşların NTA'yı daha geleneksel saldırı tespit sistemlerine tercih ettiğini belirtti.

Saldırı Önleme Sistemi

Bazı sistemler bir saldırı girişimi durdurmaya çalışabilir ancak bu bir izleme sistemi için ne zorunlu ne de gereklidir. Saldırı tespit ve önleme sistemleri (IDPS) öncelikli olarak olası olayların tespiti, bunlarla ilgili bilgileri kaydetme ve girişimleri raporlama üzerine odaklanmıştır. Buna ek olarak kuruluşlar, güvenlik ilkeleri ile ilgili sorunları belirlemek, mevcut tehditleri belgelemek ve kişilerin güvenlik politikalarını ihlal etmekten alıkoymak gibi diğer amaçlarla saldırı tespit ve önleme sistemlerini kullanmaktadır.

Saldırı tespit ve önleme sistemleri gözlenen olaylarla ilgili bilgileri kaydeder, güvenlik yöneticilerine önemli gözlemlenen olayları bildirir ve raporlar üretir. Birçok saldırı tespit ve önleme sistemi, kendisinin başarılı olmasını önlemeye çalışan bir tehdide yanıt verebilir. Saldırı tespit ve önleme sistemleri saldırıyı kendisi durdurması, güvenlik ortamının değiştirilmesi (örneğin bir güvenlik duvarının yeniden yapılandırılması) veya saldırının içeriğini değiştirmesini içeren çeşitli yanıt teknikleri kullanır.

Saldırı tespit ve önleme sistemleri olarak da bilinen saldırı önleme sistemleri (IPS), ağ veya sistem faaliyetlerini kötü niyetli etkinlikler için izleyen ağ güvenliği aygıtlarıdır. İzinsiz giriş önleme sistemlerinin başlıca işlevleri, kötü amaçlı etkinliği saptamak, bu etkinlikle ilgili bilgileri günlüğe kaydetmek, raporlamak ve bunları engellemek veya durdurmaktır.

Saldırı önleme sistemleri, saldırı tespit sistemlerinin uzantıları olarak kabul edilir, çünkü hem ağ trafiğini ve / veya kötü amaçlı etkinlik için sistem faaliyetlerini izlerler. Temel farklılıklar, saldırı tespit sistemlerinin aksine, izinsiz giriş önleme sistemlerinin sıraya yerleştirildiğini ve tespit edilen müdahaleleri aktif bir şekilde önleyebildiğini veya engelleyebildiğini göstermektedir. Saldırı önleme sistemleri, alarm gönderilmesi, algılanan kötü niyetli paketlerin bırakılması, bağlantıyı sıfırlama veya trafik akışını rahatsız edici IP adresinden engelleme gibi eylemleri gerçekleştirebilir. Bir saldırı önleme sistemi ayrıca, CRC hatalarını düzeltebilir, paket akışlarını birleştirebilir, TCP sıralama sorunlarını azaltabilir ve istenmeyen aktarım ve ağ katmanı seçeneklerini temizleyebilir.

Sınıflandırma

Saldırı önleme sistemleri dört farklı türe ayrılabilir:

Ağ Tabanlı Saldırı Önleme Sistemi (NIPS): Protokol etkinliğini analiz ederek şüpheli trafik için tüm ağı izler.

Kablosuz Saldırı Önleme Sistemleri (WIPS): Kablosuz ağ protokollerini analiz ederek şüpheli trafik için kablosuz bir ağ izleyebilirsiniz.

Ağ Davranış Analizi (NBA): Dağıtılmış hizmet engellemesi (DDoS) saldırıları, belirli kötü amaçlı yazılım şekilleri ve politika ihlalleri gibi alışılmadık trafik akışı üreten tehditleri tanımlamak için ağ trafiğini inceler.

Bilgisayar Tabanlı Saldırı Önleme Sistemleri (HIPS): Bu yöntem, gözlemlenen olayları, "iyi huylu etkinlik tanımlarının önceden belirlenmiş profilleri" ile karşılaştırarak protokol devletlerinin sapmalarını tanımlar.

Tespit Yöntemleri

Saldırı Tespit Sistemlerinin çoğunluğu, üç algılama yönteminden birini kullanır: imza tabanlı, istatistiksel anormalliğe dayalı ve durum tabanlı protokol analizi.

İmza Tabanlı Tespit: İmza tabanlı saldırı tespit sistemi, Ağdaki paketleri izler ve imzalar olarak bilinen önceden yapılandırılmış ve önceden belirlenmiş saldırı düzenleri ile karşılaştırır.

Statik Anomali Tabanlı Tespit: Anomali temelli bir saldırı tespit sistemi, ağ trafiğini izleyecek ve kurulu bir taban çizgiye karşı karşılaştıracaktır. Temel olarak, o ağ için “normal” olan neyse o tanımlanacaktır - hangi bant genişliği genellikle kullanılır ve hangi protokol kullanılır. Ancak, temeli akıllıca yapılandırılmadıysa, bant genişliğinin meşru kullanımı için yanlış bir alarm verebilir.

Durum Protokolü Analiz Tespiti: Bu yöntem, gözlemlenen olayları, “iyi huylu etkinlik tanımlarının önceden belirlenmiş profilleri ” ile karşılaştırarak protokol devletlerinin sapmalarını tanımlar.

- -Suricata- -

Suricata ücretsiz ve açık kaynak kodlu, olgun, hızlı ve sağlam bir **ağ tehdidi algılama motorudur**. Suricata motoru, gerçek zamanlı saldırı algılama (IDS), satır içi saldırı önleme (IPS), ağ güvenliği izleme (NSM) ve çevrimdışı pcap işleme yeteneğine sahiptir. Suricata, güçlü ve kapsamlı bir kurallar ve imza dili kullanarak ağ trafiğini inceler ve karmaşık tehditlerin tespiti için güçlü Lua komut dosyası desteğine sahiptir. Mevcut SIEM'ler, Splunk, Logstash / Elasticsearch, Kibana ve diğer veritabanları gibi araçlarla YAML ve JSON entegrasyonu gibi standart giriş ve çıkış formatları ile zahmetsiz hale gelir. Suricata'nın hızlı tempolu topluluk odaklı gelişimi, güvenlik, kullanılabilirlik ve verimliliğe odaklanır. Suricata projesi ve kodu, Suricata'nın gelişimini ve açık kaynaklı bir proje olarak sürdürülebilir başarısını sağlamayı taahhüt eden kar amacı gütmeyen bir kuruluş olan Open Information Security Foundation (OISF) tarafından sahiplenilmiş ve desteklenmiştir.

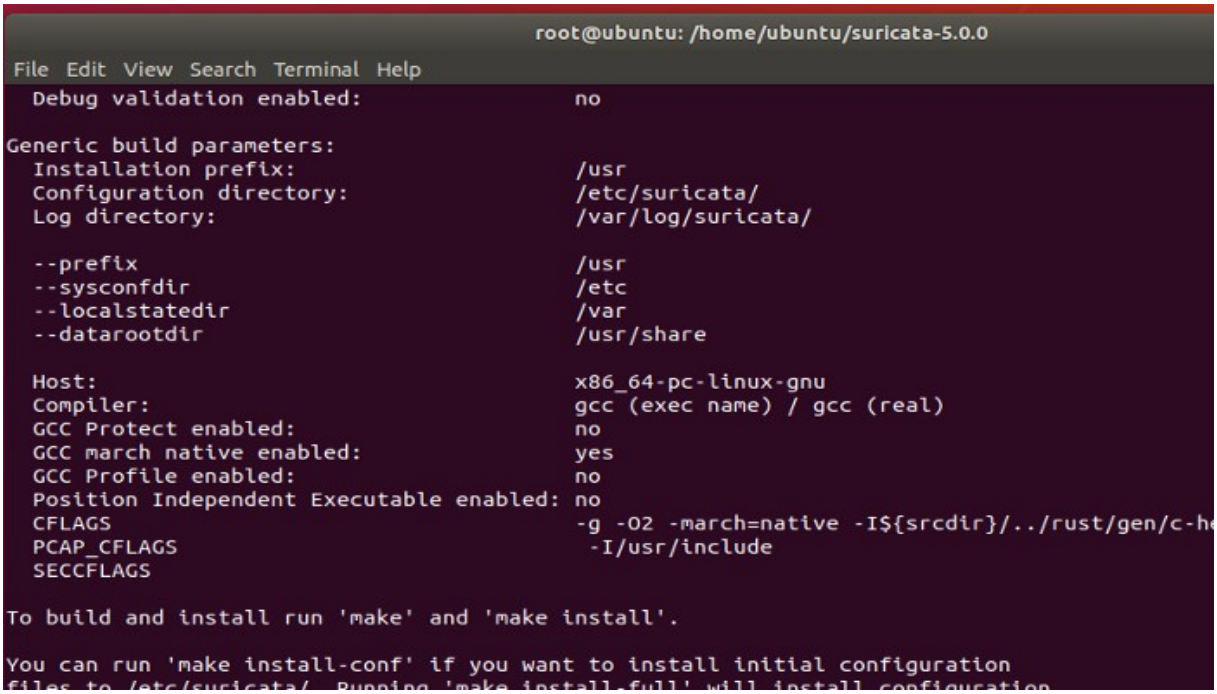
Kurulum:

1-Gerekli olan paket ve kütüphaneler indirildi.

```
$sudo apt update
$sudo apt-get install libpcre3-dbg libpcre3-dev autoconf automake libtool libpcap-dev libnet1-dev libyaml-dev libjansson4 libcap-ng-dev libmagic-dev libjansson-dev zlib1g-dev pkg-config rustc cargo -y
```

2-Suricata web sitesinden https://www.openinfosecfoundation.org/download/ 5.0.0 versiyonu indiriyoruz.

```
$wget https://www.openinfosecfoundation.org/download/suricata-5.0.0.tar.gz
$tar -xvzf suricata-5.0.0.tar.gz
$cd suricata-5.0.0
$./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
```

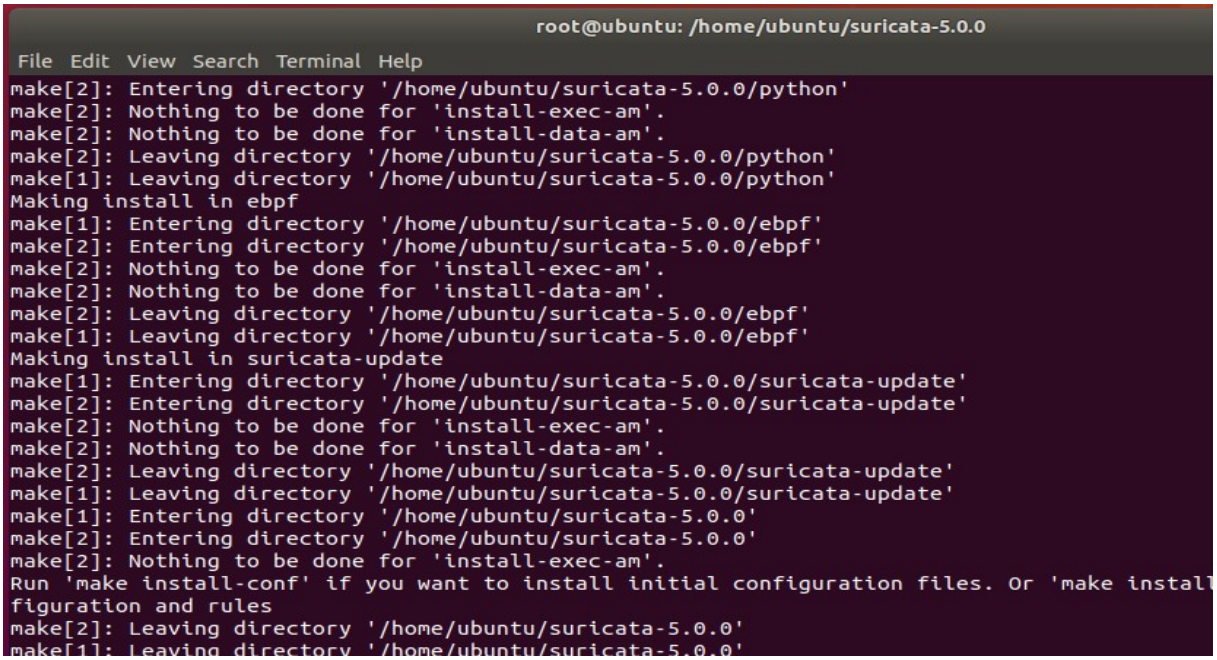


3-Suricata'nın İzinsiz Giriş Önleme Sistemini (IPS) etkinleştirmek için birkaç ek pakete ihtiyacımız var. IPS özelliği, algılanan saldırıları engellemek için sistemin dinamik olarak güvenlik duvarı kuralları eklemesine olanak tanır.

```
$sudo apt install libnetfilter-queue-dev libnetfilter-queue1 libnfnetlink-dev
```

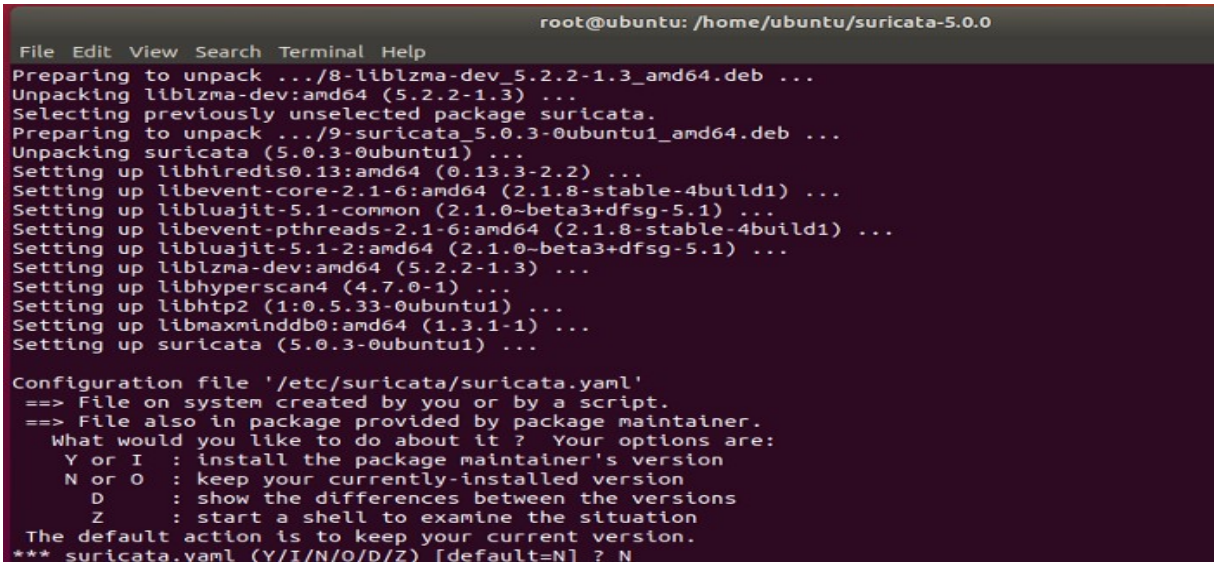
4-Configure ediyoruz.

```
$./configure --enable-nfqueue --prefix=/usr --sysconfdir=/etc --localstatedir=/var$make
$make install
$make install-conf
```



5-Ubuntu Paketlerinin Kurulumu:

```
$sudo add-apt-repository ppa:oisf/suricata-stable
$sudo apt update
$sudo apt install suricata
```



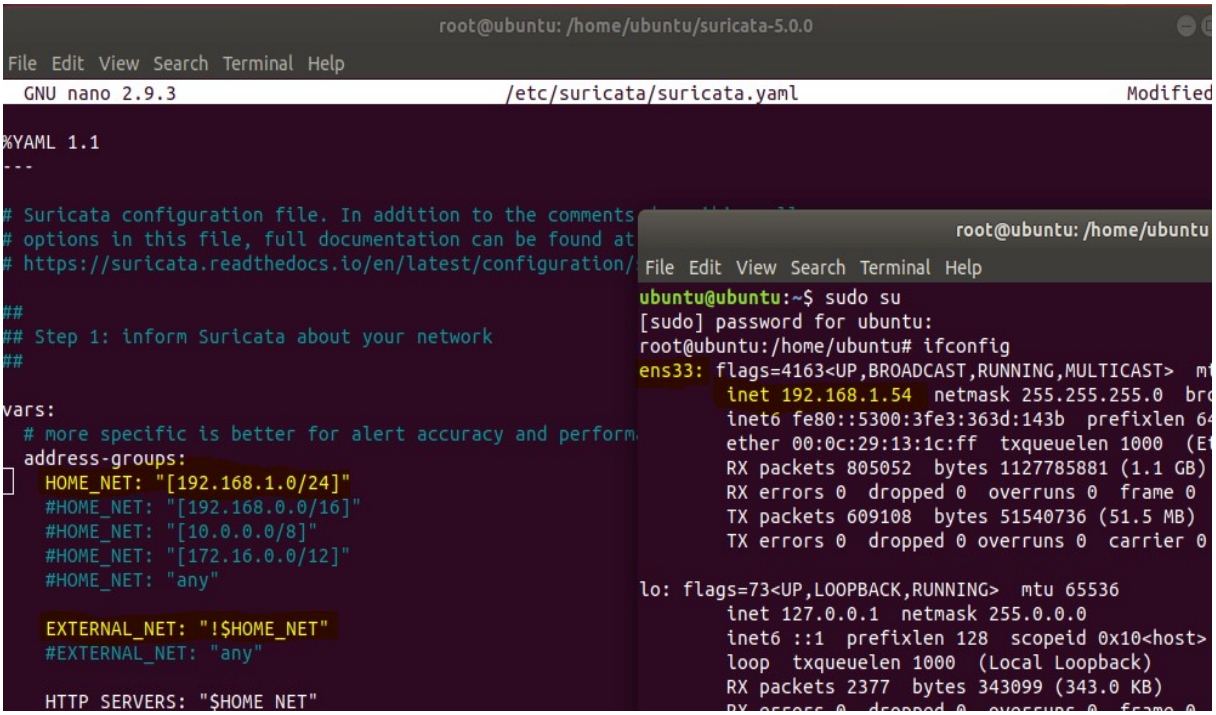
Suricata kurulumu tamamlandı.

```
root@ubuntu:/home/ubuntu/suricata-5.0.0# service suricata status
● suricata.service - LSB: Next Generation IDS/IPS
   Loaded: loaded (/etc/init.d/suricata; generated)
   Active: active (exited) since Tue 2020-10-06 06:27:29 PDT; 2min 18s ago
     Docs: man:systemd-sysv-generator(8)

Oct 06 06:27:29 ubuntu systemd[1]: Starting LSB: Next Generation IDS/IPS...
Oct 06 06:27:29 ubuntu suricata[85721]: Starting suricata in IDS (af-packet) mode... done.
```

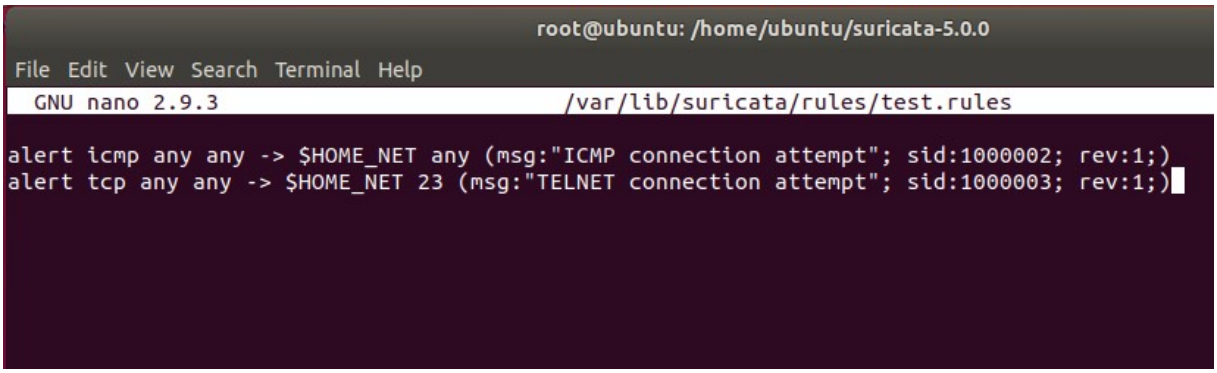
6-Suricata'in çalıştığı konfigürasyon dosyasını düzenlememiz gerekiyor.

```
$sudo nano /etc/suricata/suricata.yaml
```



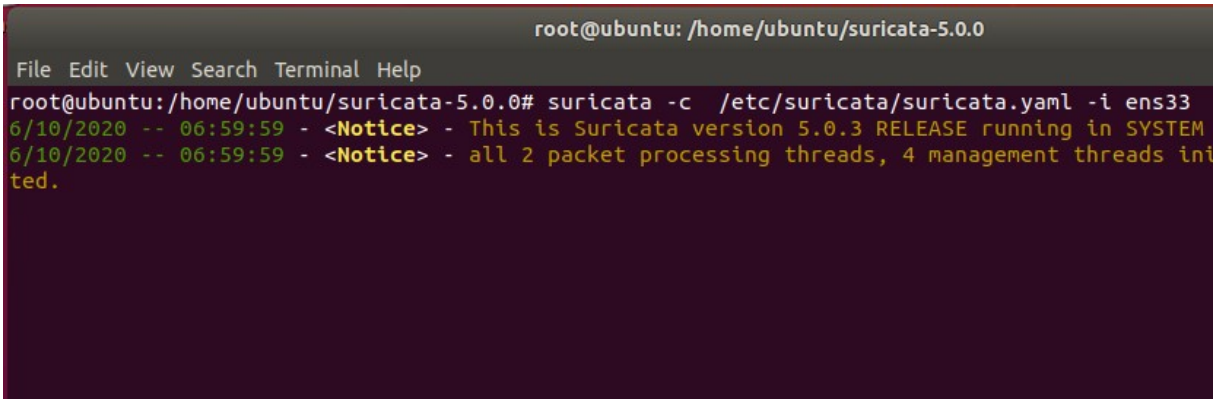
7-Ping attığımızda yakalayabilmesi için kural yazıyoruz.

```
alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 23 (msg:"TELNET connection attempt"; sid:1000003; rev:1;)
```

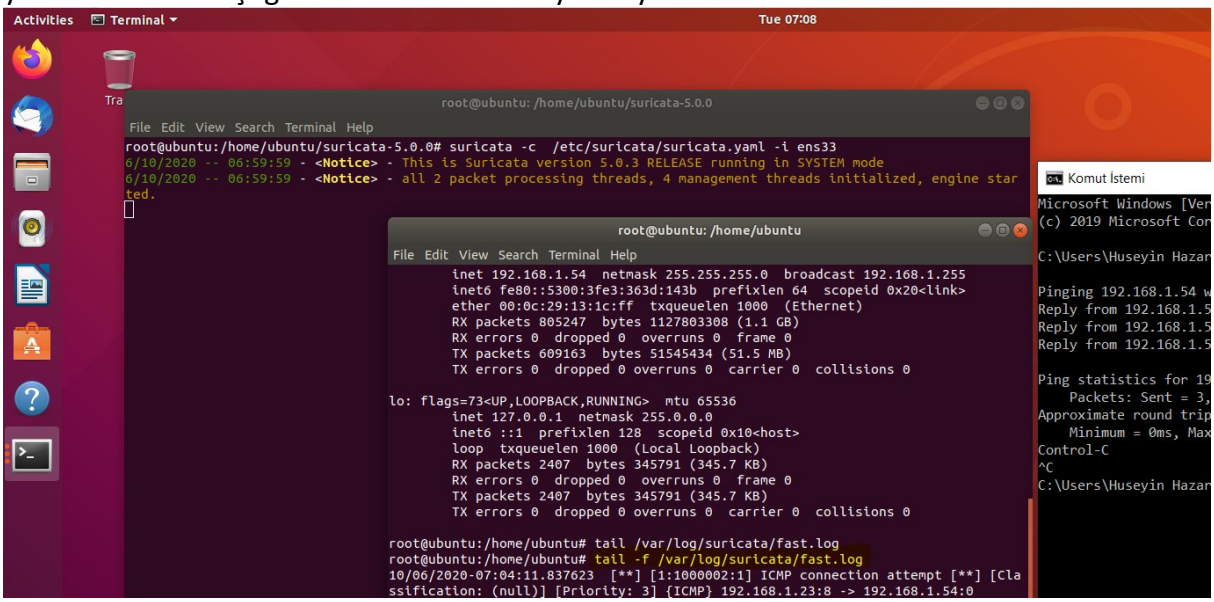


8-Suricata yı çalıştırıyoruz.

```
$sudo suricata -c /etc/suricata/surita.yaml -i ens33
```



Sonuç:
Suricata yazdığımız kural aracılığı ile yaptığımız ping işlemini yakaladı ve fast.log dosyasına yazdı.Bu kuralları çoğaltarak farklı atakları yakalayabiliriz.



Kaynakça

1. ^ Abdullah A. Mohamed, "Design Intrusion Detection System Based On Image Block Matching", International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.
2. "Gartner report: Market Guide for User and Entity Behavior Analytics". September 2015.
3. Michael E. Whitman; Herbert J. Mattord (2009). Principles of Information Security. Cengage Learning EMEA. ISBN 978-1-4239-0177-8. Retrieved 25 June 2010
4. Smaha, Stephen E., "Haystack: An Intrusion Detection System," The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988
5. https://www.beyaz.net/tr/guvenlik/cozumler/saldiri_tespit_ve_onleme_sistemi.html
6. https://terabilisim.com/saldiri-tespit-ve-onleme-sistemleri-ips-ids-nedir/
7. https://fordefence.com/saldiri-tespit-ve-onleme-sistemleri-ids-ips/
8. https://www.barikat.com.tr/teknolojiler/saldiri-tespit-ve-onleme-sistemi
9. https://www.siberdinc.com/siber/snort-ids-saldiri-tespit-sistemi-nedir-ornek-ile-anlatim/.html