P2P engellemek için Snort IDS kullanılması

Vedat Fetah, Ege Üniversitesi Network Güvenlik Grubu

Ege Üniversitesi'nde kurulan sistemde Linux işletim sistemi üzerinde çalışan Snort saldırı tespit sistemi ile P2P engellemesi yapılmaktadır. Ağ switch'inde, yönlendiriciye giden hattın trafiği snort'un dinlediği ethernet portuna yönlendirilmektedir.

Sistem mesai saatlerinde çalışmakta ve P2P yakaladığı zaman diğer bir ethernet portu üzerinden “TCP END” paketi göndererek bağlantı (connection) kurulmasını engellemektedir.

Hattı sadece dinlediği için hatta bir yavaşlığa yol açmamaktadır. Süreçte yaşanan tek sorun, gece saatlerinde başlayan bağlantıların devam etmesidir ama bu ip'ler de trafik istatistikleri takip edilerek tespit edilmekte ve kapatma yaptırımları uygulanmaktadır.

Snort'un bu şekilde kullanılabilmesi için özel bir kurulum gerekmektedir ve detaylar aşağıda anlatılmıştır. Snort kuralları dinamik olarak hazır kuralları www.snort.org sitesinden almak veya Oinkmaster adlı yazılımla bu işlem otomatik olarak kural güncellemesini yapmak mümkündür. Bundan sonar yapılması gereken ise newsgroup’ları takip ederek p2p programlarının yapacağı değişikliklerin kural tablolarına aksettirilerek kurallların güncel olmasını sağlamaktır.

Kuruluma başlamadan önce sunucuda Apache ve Mysql’in Debian’da varsayılan ayarları ile kurulu olduğundan emin olunmalıdır.

Debian Sarge Dağıtımı Üzerine Snort-Mysql Kurulumu

1. Tcp paketlerine cevap (response) yapabilmek için kullanılacak **resp** desteğini kullanabilmek için önce Libnet-1.0.2a kurulur. Libnet konfigürasyonu sırasında include dizini altındaki libnet.h dosyasının 87. satırında hata verirse 87. satırın alt satırında devam eden yorum tek satır olarak şöyle yazılır;

```
#error "byte order has not been specified, you'll need to

#define either LIBNET_LIL_ENDIAN or LIBNET_BIG_ENDIAN. See the documentation regarding the libnet-config script."
```

şeklindeki iki satır, aşağıdaki gibi tek satır olacak şekilde yazılır ve tekrar ./configure make & make install çalıştırılarak sisteme kurulur.

```
#error "byte order has not been specified, you'll need to #define either LIBNET_LIL_ENDIAN or LIBNET_BIG_ENDIAN. See the documentation regarding the libnet-config script."
```

2. Daha sonra snort-mysql aşağıdaki parametrelerle konfigüre edilir;

```
./configure –prefix=/usr –bindir=/usr/sbin –sysconfdir=/etc/snort –enable-flexrsp –with-mysql=/usr –with-openssl
```

Konfigure edilen snort make, make install ile sisteme kurulur.

3. Snortreport /var/www/report dizini altına açılır. Srconf.php dosyası metin editörü yardımıyla açılarak

```
$server = "localhost";

$user = "snort";

$pass = "Vereceginiz_şifre";
```

```
$dbname = "snort-mysql";
```

satırları kendi sisteminize göre derlenir. Burada snort-mysql tablosu logların tutulacağı tablodur.

4. Son olarak aşağıdaki komut yardımıyla report'un web erişiminin hızlı olması için yazılır;

```
zcat /usr/share/doc/snort-mysql/create_mysql | mysql -p snort-mysql
```

Bu işlemler bittikten sonra snort-mysql çalıştırılır.

Snort Çalıştırma Modları

Snort 3 modda çalıştırılabilmektedir. Bunlar Sniffer, “packet logger”, “network intrusion detection system” olarak 3 farklı modda kullanılabilir.

Sniffer Modu: Ağ trafiğini izleme modudur. Bu modda çalıştırmak için aşağıdaki komutlar kullanılabilir;

./snort -v (TCP/IP) başlıklarını gösterir.

./snort -vd (TCP/IP ve Paket başlıklarını gösterir

./snort -dev ayrıntılı bilgi modu (Paket başlıkları ve akan veri)

Paket Logger Modu: Kayıt işlemlerini kütük dosyası şeklinde yapan çalışma şeklidir. Aşağıdaki komutlarla bu mod çalıştırılır;

./snort -dev -l ./log Önceden belirlenmiş bir dizine (LOG) kayıt alır.

./snort -dev -l ./log -h 155.223.0.0/16 Bu komut satırı belirtilen ip aralığını log dosyasına kaydeder.

./snort -l ./log -b Log dosyasını binary olarak tcp dump formatında kayıt eder.

./snort -dv -r packet.log Log dosyasını (binary olarak kaydedilen) okur.

./snort -dvr packet.log icmp Log dosyasındaki (binary olarak kaydedilen) sadece icmp paketlerini okumak için kullanılır.

Network Intrusion Modu:

Saldırı ve ağdaki kötü davranışlara akıllı tepki vermek için kullanılır.Bu modu açabilmek için snort.conf dosyası içinde ağınızı tanımlamanız gerekmemektedir. Bu işlem kısaca var HOME_NET 155.223.0.0/16 satırı ile yapılır. Bu sayede snort'un her çalıştırılışında network tanımı yapmamış olduk.

Snort.conf içinde tanımlama yapmadan;

./snort -dev -l ./log -h 155.223.0.0/16 -c /etc/snort/snort.conf

Snort.conf içinde tanımlandıktan sonra;

./snort -c /etc/snort/snort.conf -i eth0 -D

Bir üst satırdaki gibi log dosyasının yolu belirtilmezse snort /var/log/snort dizini altında tutacaktır log dosyasını.

Komutların Kullanımı

- **msg:** Alarm verme ve paketlerin kaydedildigini belirten mesaji ekrana yazar.
- **logto:** Paketi kullanıcının belirlediği bir dosya adında kaydeder.
- **ttl:** IP başlığının TTL alan değerini test eder.
- **tos:** IP başlığının TOS alan değerini test eder.
- **id:** IP başlığının ID kısmının alan değerini test eder.
- **ipoption:** Spesifik kodlar için IP seçeneklerini izler.
- **fragbits:** IP başlığının bit parçalarını test eder.
- **dsize:** Bir değere karşı paketin taşıdığı veri yükünü test eder.
- **flags:** Belirli değerler için TCP segmentlerini test eder.
- **seq:** TCP sıra numara alanlarını belirli bir değer için test eder.
- **ack:** TCP onay alanlarını belirli bir değere göre test eder.
- **itype:** ICMP tipindeki alanları belirli bir değere göre test eder.
- **icode:** ICMP kodundaki alanlarını belirli bir değere göre test eder.
- **icmp_id:** ICMP ECHO ID sini belirli bir değere göre test eder.
- **icmp_seq:** ICMP ECHO sıra numaralarını belirli bir değere göre test eder.
- **content:** Veri paketinde belirli bir örneği arar.
- **content-list:** Veri paketinde belirli bir grup örnek için arama yapar.
- **offset:** İçerik opsiyonunu değiştirir.
- **depth:** İçerik opsiyonunu ve maksimum arama derinliğini değiştirir.
- **nocase:** Uygun içeriği büyük küçük harfe bakılmaksızın bulur.
- **session:** Uygulama tabakasını ekrana çıkarır.
- **rpc:** Belirli uygulama ve prosedür çağrıları için RPC servislerini izler.
- **resp:** Aktif cevaplama (bağlantıyı keser)
- **react:** Aktif cevaplama (web sitelerini bloklar)
- **reference:** Dış atak referans id'lerini ortaya çıkarır.
- **sid:** Snort kural id'sini gösterir.
- **rev:** Kural revizyon numarasını gösterir.
- **classtype:** Kural sıralama göstericisidir.

- **priority:** Kural keskinliği göstericisidir.
- **uricontent:** Paketin URI porsiyonunda seçilen bir örneği arar.
- **ip_proto:** IP başlığının protokol değeridir.
- **sameip:** Kaynak ip'sinin hedef ip'sine eşit olup olmadığına kararlaştırır.

Yukarıdaki seçeneklerin tek tek kullanımlarını anlatmak yerine sadece resp seçeneğinin kullanımı hakkında bilgi vereceğiz.

resp: Bu komutla beraber kullanabilir seçenekler:

1. rst_snd - TCP-RST paketlerini gönderme soketine yollar.
2. rst_rcv - TCP-RST paketlerini alma soketine yollar.
3. rst_all - TCP_RST paketlerini her sokete yollar.
4. icmp_net - Bir ICMP_NET_UNREACH'i göndericiye yollar.
5. icmp_host -Bir ICMP_HOST_UNREACH'i göndericiye yollar.
6. icmp_port - " ICMP_PORT_UNREACH'i göndericiye yollar.
7. icmp_all – Bütün ICMP paketlerini göndericiye yollar.

resp: ;

alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg: "BLEEDING-EDGE P2P Ares traffic"; flow: established; content:"User-Agent\: Ares"; reference: url,www.aresgalaxy.org; classtype: policy-violation; sid: 2001059; rev:3; resp:rst_all;)

alert tcp any any -> 155.223.0.0/16 1524 (flags: S \
resp: rst_all; msg: "Root shell backdoor attempt";)

alert udp any any -> 155.223.0.0/16 31 (resp: icmp_port, icmp_host; \
msg: "Hacker's Paradise erisim denemesi";)

şekillerinde kullanımı mevcuttur. Ancak biz p2p trafiğini denetlemek için çalışmalar yaptığımız için sadece ilk satırdaki örnek kural tarzı kurallarla

çalışmalıyız aksi taktirde daha yüksek kapasitede bir sunucuya ihtiyacımız olacaktır.

Resp response rst_all ise reset all anlamı taşımaktadır. Kuralda tanımladığımız üzere alert tcp $HOME_NET any içeriden dışarıya giden tüm isteklerin “ -> $EXTERNAL_NET any “ resetlenmesi anlamını taşımaktadır. Burada bağlantısı resetlenecek makinanın gönderdiği paket sid: 2001059. Bu kurala uyan paket sahiplerinin göndermiş olduğu paketler resetlenecektir. Kuralları içerden dışarı ya da dışardan içeri tanımlayabiliriz.

Snort kurallarını kendi yazamayanlar için hazır kuralları www.snort.org sitesinden almaları mümkündür. Oinkmaster adlı yazılımla bu işlem otomatik olarak yapılabilir. Bunun için oinkmaster kurulduktan sonra snort’un web sitesinden kendinize özel bir id numarası alarak oinkmaster.conf içine yazıp çalıştırmanız gerekir.

oinkmaster -o /etc/snort/ -b /etc/snort/eski/ komutuyla yeni kurallar /etc/snort/rules dizini altına konulmadan önce bu dizin /etc/snort/eski dizini altına sıkıştırılarak alınır. Yeni çekilen kurallar direk rules dizini altına yerleştirilir.