

P2P ile Mücadele ve KSU-NET Örneği

Ali Çaylı¹, Adil Akyüz¹, Ercan Efe², Sait Üstün¹

¹ Kahramanmaraş Sütçü İmam Üniversitesi, Enformatik Bölümü, 46100, Kahramanmaraş

² Kahramanmaraş Sütçü İmam Üniversitesi, BAUM , 46100, Kahramanmaraş

alicayli@ksu.edu.tr, akyuz@ksu.edu.tr, eefe@ksu.edu.tr, ustun@ksu.edu.tr

Özet: P2P yazılım paylaşım programları son yıllarda en çok internet trafiğini kullanan uygulamalardır. Yazılım paylaşımı ile yasal yazılım dağıtımın yanında yasal olmayan yazılım ve lisans gerektiren içerik dağıtımları için de sıkça kullanılmaktadır.

Günümüzde kullanılan P2P yazılımları daha öncelilere göre oldukça gelişmiş özelliklere sahiptir. Bu tür yazılımların oluşturduğu trafiği kontrol altına almak, gerekiyorsa engellemek Akademik Ağın amacına uygun kullanılmasını sağlamak üzere çeşitli yöntemler mevcuttur.

Bu çalışmada Kahramanmaraş Sütçü İmam Üniversitesi'nde Snort ve SnortSam yazılımları ile yapılan mücadele detaylı bir şekilde verilmiştir.

Anahtar Kelimeler: P2P, IDS, IPS, SnortSam, Kampus Ağ Yönetimi

Struggle With P2P and KSU-NET Example

Abstract: P2P sharing software is the main programs that use for internet traffic application. Also it is used to distribute software sharing, formal and informal software and their contents.

Today used P2P software is fairly improved as previously used software. There are many methods, to use academic network for its main purposes or to control or, if necessary, to prevent the traffic of this kinds of software.

In this study, struggling with the Snort and SnortSam software in Kahramanmaraş Sutcu Imam University were explained in detail.

Giriş

P2P protokolün temeli 1999 yılında geliştirilen napster'a dayanmaktadır. Napster çalışma mantığı oldukça basittir. Buna göre napster şirket merkezinde tutulan sunucularda istemcilerin paylaşımına açtığı dosyaların listesi tutulmaktadır. İstemci napster programında arama yaptığında sunucuda bu dosyaları paylaşımına açan kullanıcılara rastlanırsa o istemcinin bilgileri istekte bulunan istemciye gönderilmekte ve dosyalar karşıdaki istemciden alınabilmektedir.

İnternet kullanımının yaygınlaşması ile müzik dosyalarının kolaylıkla kullanıcıların bilgisayarlarına indirilip kullanılması müzik yapımcısı firmaları harekete geçirmişti. 2000 yılında müzik yapımcılarının açtığı davalar sonucunda napster sunucuları mahkeme kararı ile kapatılmıştır.[2]

Bunun sonucu olarak 2. nesil paylaşım programları yazılmış ve kullanılmaya başlanmıştır. Bunlarda tek bir sunucu yerine birden fazla sunucu üzerinde arama yapılabilirken sonraki dönemlerde P2P üzerinde bazı değişikliklerle günümüzde kullanılan yazılımlara ulaşılmıştır.

P2P trafiğinin tespit edilmesi

Önceki nesil paylaşım programlarında sunucu sayısı belli olduğundan sunucu ip adresine doğru giden trafiğin kolayca P2P trafiği olduğu anlaşılıyordu. Ancak yeni nesil P2P programlarında birden çok sunucu kullanılabilirdiğinden akan trafiğin içerisinde P2P paketlerini bulmak oldukça zahmetli ve zordur. Bu programlar ilk önceleri sabit bir port kullanırken daha sonraları değişken sunucu bağlantı portlarını kullanmaya başlamaları sistem yöneticilerinin işlerini bir hayli zorlaştırmıştır. P2P trafiğinin belirlenmesi için en iyi yol önceden belirlenmiş paket kurallarının akan trafikteki paketlerle karşılaştırılmasıdır. Bu yöntemle paketlerin ne tür bir veri taşıdığı belirlenebilmektedir. Bu noktada da paket kurallarının önceden ve hızlı bir şekilde belirlenip paket karşılaştırma programlarına (Intrusion Detection System - IDS) tanımlanması gerekmektedir.

SnortSam

SnortSam, Snort Saldırı Tespit Sistemi için yazılmış bir eklentidir. Çalışma prensibi snort kurallarına uyan paketler tespit edildiğinde bu ip adreslerinden gelen-giden trafiği belirli bir süre engellemek şeklindedir. Birçok güvenlik duvarı yazılımı ile beraber çalışabilir. Bunlardan bazıları Checkpoint Firewall-1, Cisco PIX firewalls, Cisco Routers (using ACL's or Null-Routes), Former Netscreen, Juniper firewalls, IP Filter (ipf), Linux IPTables'dir. Snortsam iki temel parçadan oluşur. Bunlardan biri snort çıktı eklentisi diğeri ise güvenlik duvarı ile haberleşen ve komutlar gönderen aracı yazılım. Otomatik olarak çalışan bu sistem, snort çıktı eklentisinden aldığı ip adres bilgisi ile güvenlik duvarı yazılımına gerekli komutları göndererek o ip adresine bloklama yapılmasını sağlar. Kurulum için gerekli yazılım <http://www.snortsam.net/> adresinden indirilebilir veya son sürümü cvs sunucusundan alınabilir.

SnortSam Kurulumu

İndirilen paketler bir klasör içerisine açılır.

```
# tar zxvf snortsam-src-50.tar.gz
```

Klasör içindeki make script'te çalışma izni verildikten sonra çalıştırılır.

```
# chmod +x makesnortsam.sh  
# ./makesnortsam.sh
```

Derleme işleminden sonra derlenmiş program çalıştırılabilir dosyaların bulunduğu dizine (/usr/local/bin) kopyalanır. [3]

Snort'un Snortsam Yama Paketleri ile Derlenmesi

Snort programına snortsam yaması yapılması gereklidir. Bu işlem için gerekli dosya snortsam-patch.tar.gz snortsam sitesinden indirilmelidir. İndirilen bu dosya bir klasör içerisine açılır. Klasör içerisinden bulunması gereken dosyalar patchsnort.sh, snortpatch8, snortpatch9, snortpatchb dir. Ayrıca snort programı da snort web sitesinden indirilerek bir başka klasör içerisine açılır.

Snortsam yama dosyalarının bulunduğu klasördeki patchsnort.sh dosyasına çalışma izni verildikten sonra script çalıştırılır. Script'e parametre olarak snort kaynak kodlarının bulunduğu klasörün yolu verilir.

```
# chmod +x patchsnort.sh  
# ./patchsnort.sh /usr/local/src/snort
```

Daha sonra Snort programı da derlenerek sisteme yüklenir.

```
# cd /usr/local/src/snort  
# ./configure  
# make  
# make install
```

SnortSam Ayarlarının Yapılması

Snortsam örnek konfigürasyon dosyası "snortsam.conf.sample" kaynak kod dizini içerisinde bulunabilir. Bu dosya etc klasörü altına kopyalanabilir (/etc/snortsam.conf). Bu dosya içerisindeki anahtarlar ve değerleri Tablo.1' de verilmiştir.

Anahtar	Kullanım	Varsayılan	Açıklama
accept	accept <host>/<mask>, <key>	-	Hangi Ağdan gelen isteklere cevap vereceğini belir
defaultkey	defaultkey parola	-	Bağlantı parolası
Port	port portnumarası	898	Bağlantı portu
dontblock	dontblock <host>/<mask>	-	Bloklanması istenmeyen ip veya ağ
logfile	logfile <filename>		Günlük Dosyası
daemon	daemon	-	Servis olarak çalışır
email	email <smtpserver> : <port> <recipient> <sender>	-	
ipf	ipf <adapter> <loglevel>	-	Güvenlik duvarı seçimi

Tablo.1. SnortSam.conf dosyası içerisindeki anahtarlar ve değerler.

Snort Ayarlarının Yapılması

Snort çalıştırılmadan önce snort.conf dosyası içerisinde de yapılması gereken bazı ayarlamalar vardır. Bunlara ilişkin kullanımlar aşağıdaki gibidir.

```
output alert_fwsam: <snortsambox>
```

Snortsam bir parola gerektiriyorsa aşağıdaki şekilde kullanılmalıdır.

```
output alert_fwsam:  
<snortsambox>:<port>/<password>
```

Birden fazla Snortsam programına gönderilecekse aşağıdaki şekilde kullanılabilir.

```
output alert_fwsam: localhost/  
myhostpass  
sam.corp.com:1050/corppass
```

FreeBSD kullanılıyorsa aşağıdaki parametrelerin rc.conf dosyasına girilmesi gerekecektir.

```
snort_enable="YES"  
snort_interface="fxp0"  
#snort_flags="-D -A fast"  
snort_flags="-D -b"  
snort_conf="/usr/local/etc/snort/  
snort.conf"
```

Snort -A fast parametresi ile çalıştırılmamalıdır. Bu durumda snortsam çalışmayacaktır.

Snort kural paketleri içerisinde de snortsam ip bloklama eklentisini çalıştıracak kodların yazılması gerekir. Bu dosyalar snort /etc/snort/rules veya /usr/local/share/snort altında olabilir. Dosyalar metin dosyasıdır. Bunlar herhangi bir editörle açılıp kuralların sonuna **"fwsam: <who>, <duration>"** formatında eklemeler yapılır. Burada fwsam eklentisinin adı, who ne yöne doğru engelleme yapılacağını ve duration da ne kadar süre ile engelleme yapılacağını göstermektedir.

```
alert tcp $EXTERNAL_NET any ->  
$HTTP_SERVERS $HTTP_PORTS (msg:"WEB-  
ATTACKS /bin/ps command  
attempt"; flow:to_server,established;  
uricontent:"ps%20"; nocase;  
sid:1329; classtype:web-application-  
attack; rev:4; fwsam: src, 5  
minutes;)
```

```
alert tcp $HOME_NET 4711 ->  
$EXTERNAL_NET any (msg:"P2P  
eDonkey server response";  
flow:established,from_server;  
content:"Server|3A| eMule";  
reference:url,www.emule-project.net;  
classtype:policy-violation;  
sid:2587; rev:2; fwsam: src, 5  
minutes;)
```

```
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:4;fwsam: src, 5  
minutes;)
```

```
alert tcp $HOME_NET any ->
$EXTERNAL_NET any (msg: "BLEEDING-
EDGE P2P Ares GET"; flow:
established; content:"ares"; nocase;
pcre:"/(GET |GET (http|https)\:\
\/\[-0-9a-z.]*)\\/ares\/\i";
reference:url,www.aresgalaxy.
org; classtype: policy-violation;
sid: 2001060; rev:6; fwsam: src, 5
minutes;)
```

Snort kural dosyaları www.snort.org sitesinden indirilebilir. Bu işlemi oinkmaster programı ile otomatik olarak ta yapmak mümkündür. Bunun için oinkmaster kurulduktan sonra snort'un web sitesinden özel bir id numarası alınarak oinkmaster.conf içine yazılıp çalıştırılması gerekir.

```
# oinkmaster -o /etc/snort/ -b /etc/
snort/eski/
```

Yukarıda verilen komutla yeni kurallar /etc/snort/rules klasörü altına konulmadan önce bu dizin /etc/snort/eski dizini altına sıkıştırılarak alınır. Yeni çekilen kurallar da rules klasörü altına yerleştirilir [1]. Ancak bu işlem sonunda yeni kural dosyaları içerisinde fwsam parametresini tekrardan düzenlemek gereklidir.

Sonuç ve Öneriler

Son zamanlarda P2P yazılımlarla dosya paylaşımının yanında doğrudan dosya indirilebilen sunucular da yaygın olarak kullanılmaktadır. Bu sunuculardan indirilen dosyaların içeriği dosyalar indirilirken tespit etmek mümkün değildir. Bu tür P2P dışında dosya indirme sunucuları için engelleme güvenlik duvarı yazılımlarından yapılabilir.

P2P dışında istenmeyen diğer trafiğin de Virus, DoS, backdoor, porno, shellcode, malware vb. gibi Snort ve Snortsam yazılımlarını kullanılarak engellenmesi mümkündür. Bilinen kurallar dışında kalan diğer yazılımların oluşturduğu trafiğin de tespit edilmesi için tcpdump gibi programlarla paket içeriklerine göz atıp gerekli kurallar oluşturulabilir.

Alınacak her türlü önlem hiçbir zaman yeterli olmayacaktır. Alınan önlemlere karşı programcılar da karşı önlem alarak bu tür yazılımların kurallara takılmasını engellemeye çalışmaktadırlar. Bu noktada kullanıcıların bilinçlendirilmesi ve içinde buldukları ağın amacına uygun kullanılması gerekliliği anlatılmalıdır.

Kaynaklar

[1] Fetah V. "P2P engellemek için Snort IDS kullanılması", *Ege Üniversitesi Network Güvenlik Grubu*, <http://csirt.ulakbim.gov.tr/> dokumanlar

[2] Soysal M., Akın G., Fetah V., Karaarslan E., "P2P ile Yaşamak", <http://csirt.ulakbim.gov.tr/> dokumanlar/

[3] Snortam Web sitesi, www.snortsam.net

[4] Snort Web sitesi, The de facto standard for intrusion detection/prevention, <http://www.snort.org>