

# Hping ve Dos Atak Denemesi

İyi Günler arkadaşlar. Bilindiği üzere BT alanında son yıllarda canımızı son derece sıkkan 2 önemli tehdit unsuru var. Bunlardan 1.si fidye yazılımları bir diğeri ise tabii ki siber saldırılar.

Her gün Bilgi Sistemleri ile alakalı web sitelerinde , gazetelerin teknoloji bölümlerinde, bir yerlere siber saldırı gerçekleştirildiğini , bu saldırıların bilmem kaç milyon pc ya da iot cihazı üzerinden gerçekleştirildiği belirtilmektedir.

En son yaklaşık 3 hafta önce bazı sosyal medya platformlarına erişimlerde problem yaşatan dns sunucularına yapılan saldırıları hatırlarsınız. Yaklaşık 1 milyon adet iot cihazından geldiği söylenmişti. Bu cihazların büyük kısmını ip kameralar oluşturmaktaydı.



## **Peki Bu saldırılar nasıl Gerçekleşiyor ?**

Bir çoğumuzun yanıtını bilmek istediği soru bu aslında . Tehditi bilmeden, yapısını bilmeden nasıl tedbir alacağız? Aslında TCP/IP ve OSI modeli bilgisi sahibi olmadan tam anlamıyla lokal bazlı tedbirler almakta mümkün değil.

Siber saldırıların en bilinen saldırı tiplerindendir DDos atak. Bir yada birden fazla hedefe , önceden ele geçirilen kaynaklardan (botnet) saldırı yapılarak, hedefteki servislerin devre dışı bırakılmasının sağlanmasıdır.

Dos saldırıların ise en bilinen yöntemlerinden birisi syn flood saldırısıdır. Binlerce kaynaktan hedefe , hedef sistemin kaynağını tüketecek ve trafik oluşturacak sayıda ardışık syn paketi gönderilmesi olayıdır.

Siber saldırılara meraklı iseniz, teorik olarak bu sizi cezbedebilir ama uygulamada hayal kırıklığı olabilir. Hedef sistemdeki güvenlik tedbirleri , internet erişim sağlayıcılarının DDOS çözümleri sizi yanıltabilir.

1 syn paketinin 65 byte olduğunu düşünürsek evinde 8Mbit adsl kullanan arkadaşımızın bir kahramanlık yaparak kendini syn flood saldırısına adanması istediği sonuca ulaşması anlamında hayal kırıklığı oluşturacaktır.

## **DOS Atak Önlemleri**

Ben en başından beri dos atakların internet servis sağlayıcısı (ISP), tarafından tespit edilip başka bir alan yönlendirilerek, hedef sistemin etkilenmesini minimize etmesinin gerekli olduğunu düşünüyorum.Firewall hizmetini ISP tarafından alan kurumlarda böyle bir işlevin olduğunu farzediyorum (umarım öyledir)

## **Böyle olmadığı durumlarda ne yapacağız ?**

Burası sizin kabiliyetinize kalmış. Güvenlik firmalarından danışmanlık hizmeti ve bilgi güvenliği çözümleri ile destek alınarak da çözümler üretilebilir. Lokal ağdaki kişisel cihazların analizi, network cihazların konfigürasyonu, bunların yapılandırılması, firewall cihazının konfigürasyonları, TCP/Ip ve OSI bilgileri ile çözümler üretilebilir.

Ben kendi işimi kendim göreceğim diyen arkadaşlar için aşağıda Fortigate Firewall üzerinde (firmware 5.2 ve üzeri ) Dos denemesi ile ilgili paylaşımlarım var umarım yardımcı olur.

## Fortigate Firewall üzerinde Dos Denemesi

Öncelikle testimiz için ne tür araçlar ve sistemler kullandık onu belirteyim

Firewall : Fortigate 600 D firmware 5.2

Saldırgan sistem : Kali Linux

Saldırgan araç: Hping

Bağlantı Türü: Noktadan noktaya

Bağlantı Bant Genişliği: 10Mbit

Testimize başlayalım :

- 1- Öncelikle Firewall üzerinde, Dos atak için konfigürasyonumuzu yapalım (Resim 1)

**FortiGate 600D**

**Edit DoS Policy**

Incoming Interface: [Redacted]

Source Address: [all]

Destination Address: [all]

Service: [ALL]

**Anomalies**

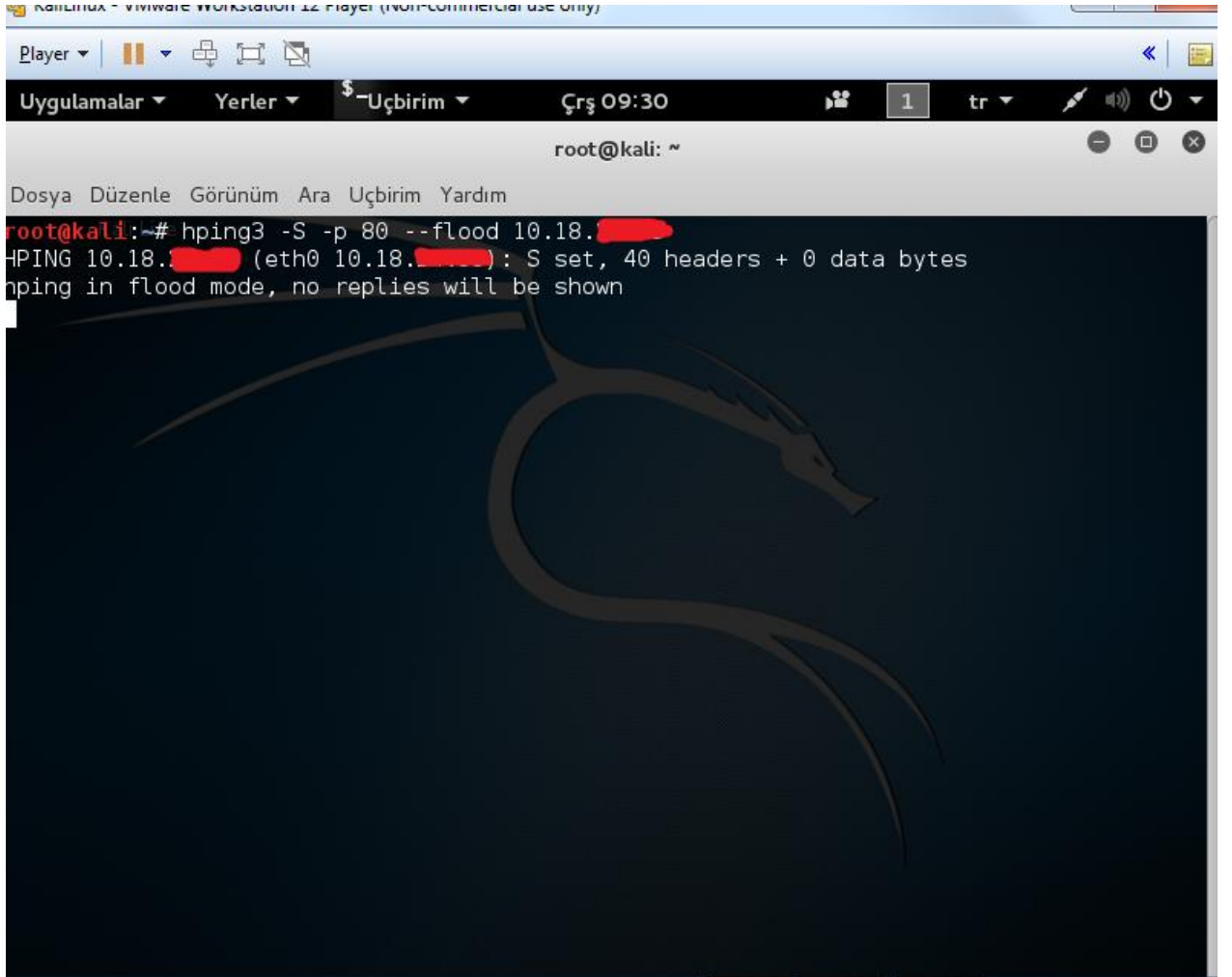
Name	Status	Logging	Action	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
tcp_port_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	1000
tcp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
tcp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
udp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
udp_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
udp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
udp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
icmp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	250
icmp_sweep	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	100
icmp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	300
icmp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	1000
ip_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
ip_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
sctp_flood	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	2000
sctp_scan	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	1000
sctp_src_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000
sctp_dst_session	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Block	5000

☒ Enable this policy

OK Cancel

Resim :1

- 2- Firewall üzerinde gerekli policy tanımlaması yaptık. Şimdi saldırgan tarafına geçelim ve syn flood saldırısı başlatalım



```
Kali Linux - VMware Workstation 12 Player (non-commercial use only)
Player
Uygulamalar Yerler $-Uçbirim Çrş 09:30 1 tr
root@kali: ~
Dosya Düzenle Görünüm Ara Uçbirim Yardım
root@kali:~# hping3 -S -p 80 --flood 10.18.1.1
HPING 10.18.1.1 (eth0 10.18.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Saldırgan sisteminde (kali Linux) terminali açıp, saldırı aracımız hping'e erişiyoruz. Sistemde default olarak hping3 versiyonu kurulu gelmekte.

Yukarıdaki resimdeki komutları açarsak ;

-S = SYN saldırısını yapacağımızı belirttik

-p = Hedef sistemdeki hedef port

--flood = flood mod

Ve en sonda hedef sistem ip bilgisi yer alıyor . Yukarıdaki ekranda bir reply dönmeyecek. Ekran öyle kalacak , peki saldırının başladığından nasıl emin olabiliriz diyorsanız firewall loglarına bakın.

System

Router

Policy & Objects

Security Profiles

User & Device

Log & Report

Traffic Log

- Forward Traffic
- Local Traffic
- Sniffer Traffic

Event Log

Security Log

- Antivirus
- Web Filter
- Application Control
- Intrusion Protection
- Anomaly
- Email Filter
- Data Leak Prevention

Report

Log Config

Monitor

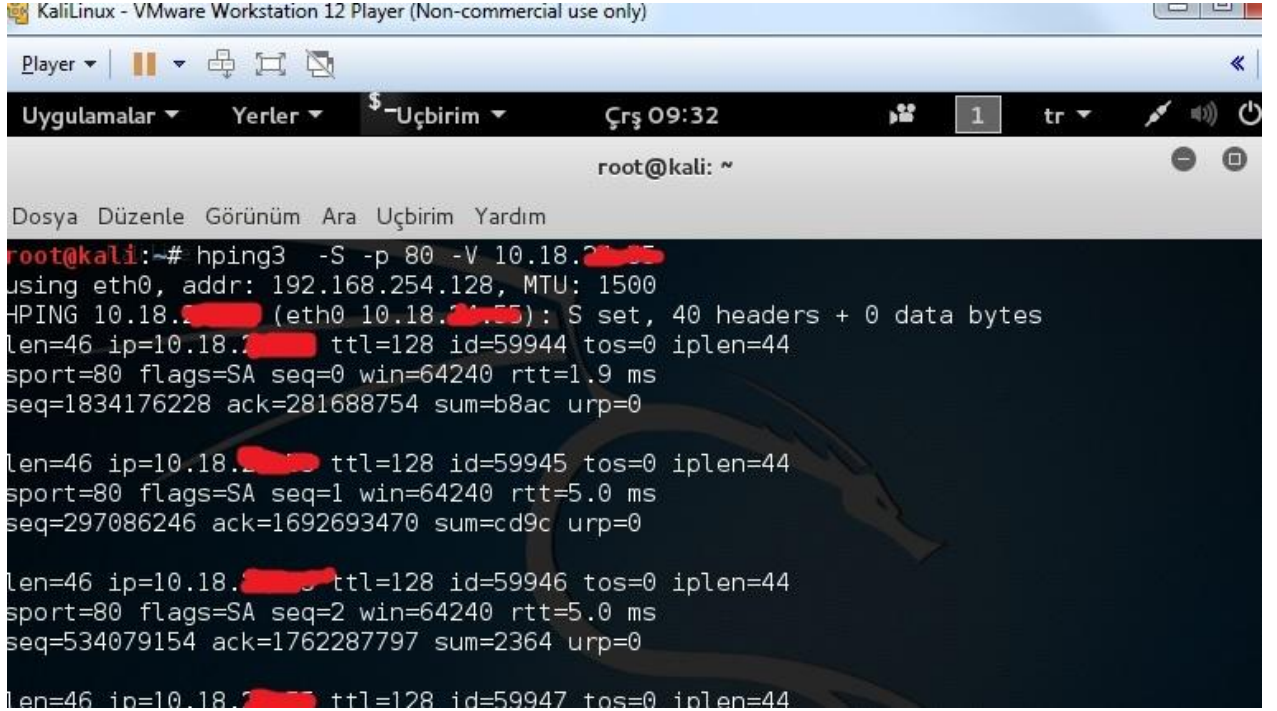
Add Filter

#	Date/Time	Severity	Source	Protocol	User	Action	Count	Attack
1	10:29:35	10.0.0.0	10.0.0.0	6		clear_session	627	tcp_syn_flood
2	10:29:35	10.0.0.0	10.0.0.0	6		clear_session	2055	tcp_port_scan
3	09:37:36	10.0.0.0	10.0.0.0	6		clear_session	5026	tcp_syn_flood
4	09:37:36	10.0.0.0	10.0.0.0	6		clear_session	587	tcp_port_scan
5	11-23 15:19	10.0.0.0	10.0.0.0	6		clear_session	491	tcp_port_scan
6	11-23 15:18	10.0.0.0	10.0.0.0	6		clear_session	2	tcp_port_scan
7	11-23 15:17	10.0.0.0	10.0.0.0	1		clear_session	723	icmp_sweep
8	11-23 14:42	10.0.0.0	10.0.0.0	1		clear_session	392	icmp_sweep
9	11-23 14:42	10.0.0.0	10.0.0.0	6		clear_session	3764	tcp_port_scan
10	11-23 14:39	10.0.0.0	10.0.0.0	1		clear_session	327	icmp_sweep
11	11-23 14:38	10.0.0.0	10.0.0.0	1		clear_session	402	icmp_src_session
12	11-23 14:38	10.0.0.0	10.0.0.0	1		clear_session	325	icmp_sweep
13	11-23 14:37	10.0.0.0	10.0.0.0	1		clear_session	327	icmp_sweep
14	11-23 14:36	10.0.0.0	10.0.0.0	1		clear_session	553	icmp_sweep
15	11-22 15:40	10.0.0.0	10.0.0.0	1		clear_session	1109	icmp_sweep
16	11-22 15:40	10.0.0.0	10.0.0.0	1		clear_session	362	icmp_src_session
17	11-22 15:40	10.0.0.0	10.0.0.0	1		clear_session	1	icmp_src_session
18	11-22 15:39	10.0.0.0	10.0.0.0	1		clear_session	1	icmp_sweep
19	11-21 13:23	10.0.0.0	10.0.0.0	6		clear_session	1	tcp_syn_flood
20	11-21 13:23	10.0.0.0	10.0.0.0	6		clear_session	1	tcp_port_scan

Log sekmesinde , anomaly alt sekmesinde , yaptığımız saldırının logları yer almakta. Tcp\_syn\_flood saldırı yöntemi olarak loglanmış. Yaptığınız saldırı girişimi bilirsiniz ki anlık loga düşmez. Biraz gecikmeli olarak ekranda göreceksiniz . (Ekranda tcp\_port\_scan saldırısı yer almakta. Nmap yada benzeri port scan araçları ile çalışma yaparken port taraması vb, fortigate bunlarında logunu tutup dos atak olarak algılıyor. )

Ben saldırıyı flood mode değilse Verbose moda yapmak istiyorum diyorsanız alttaki resimde yer alan komutları üreteceksiniz.

Bu komutlar resimde görüldüğü gibi bir reply döndürmekte.



```
KaliLinux - VMware Workstation 12 Player (Non-commercial use only)
Player
Uygulamalar Yerler $-Uçbirim Çrş 09:32 1 tr
root@kali: ~
Dosya Düzenle Görünüm Ara Uçbirim Yardım
root@kali:~# hping3 -S -p 80 -V 10.18.2.55
using eth0, addr: 192.168.254.128, MTU: 1500
HPING 10.18.2.55 (eth0 10.18.2.55): S set, 40 headers + 0 data bytes
len=46 ip=10.18.2.55 ttl=128 id=59944 tos=0 iplen=44
sport=80 flags=SA seq=0 win=64240 rtt=1.9 ms
seq=1834176228 ack=281688754 sum=b8ac urp=0

len=46 ip=10.18.2.55 ttl=128 id=59945 tos=0 iplen=44
sport=80 flags=SA seq=1 win=64240 rtt=5.0 ms
seq=297086246 ack=1692693470 sum=cd9c urp=0

len=46 ip=10.18.2.55 ttl=128 id=59946 tos=0 iplen=44
sport=80 flags=SA seq=2 win=64240 rtt=5.0 ms
seq=534079154 ack=1762287797 sum=2364 urp=0

len=46 ip=10.18.2.55 ttl=128 id=59947 tos=0 iplen=44
```

Herkese iyi çalışmalar Dilerim ..

Faruk GÜNGÖR

Bilgisayar Mühendisi