Hosting Firmalarına yönelik DDoS Saldırıları ve Çözüm Önerileri

Huzeyfe ÖNAL
Bilgi Güvenliği AKADEMİSİ
honal@bga.com.tr
www.bga.com.tr

Konuşmacı Hakkında |Huzeyfe ÖNAL

- Bilgi Güvenliği Danışmanı (iş hayatı)
  - Bilgi Güvenliği AKADEMİSİ(www.bga.com.tr)
- Ağ Güvenliği Araştırmacısı (gerçek hayat)
- Kıdemli DDoS Uzmanı
- Blogger
  - www.lifeoverip.net

Ajanda

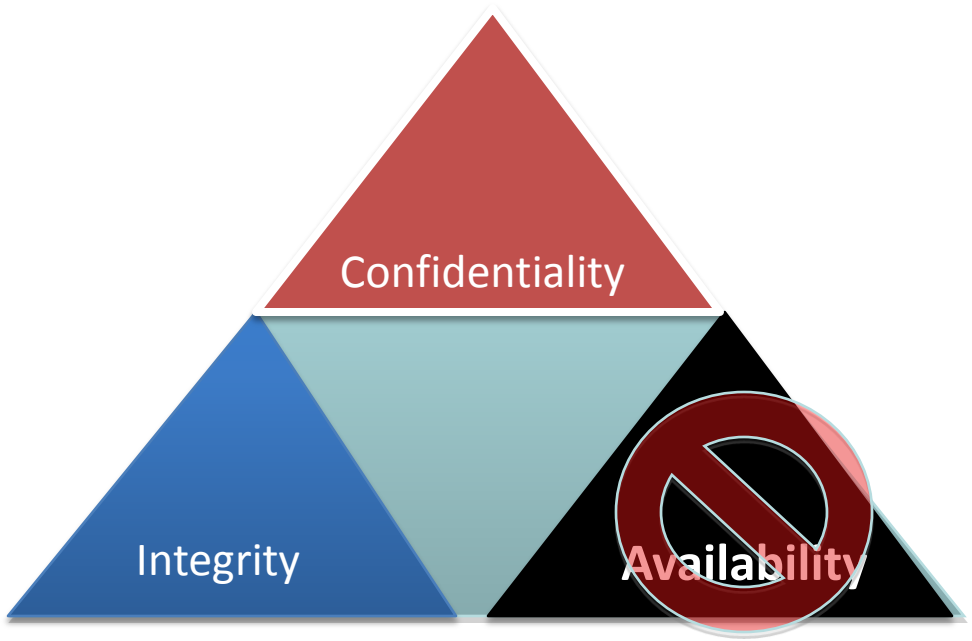
- DoS/DDoS hakkında genel terim ve tanımlar
- DDoS saldırıları hakkında hatalı bilgiler ve düzeltmeler
- Türkiye'den güncel örnek
- DDoS ürünleri
- Açık kaynak yazılımlar kullanarak DDoS analizi
- Açık kaynak sistemler kullanarak DDoS engelleme

Neden DDoS ?

- Cloud computing, Virtulization, Web 2.0, Green IT vs gibi afilli konular varken neden DDoS konusu?
- Herşeyin temeli “networking”
- Teknolojiler değişir, gelişir ama TCP/IP değişmedikce DdoS saldırıları tehlike olmaya devam edecektir.

Standart Güvenlik Bileşenleri

- Hatalı bilgi
  - En güvenli sistem fişi çekilmiş sistemdir!



Başlamadan Önce...

- Gelen DDOS saldırısı sizin sahip olduğunuz bantgenişliğinden fazlaysa yapılabilecek çok şey yok!
- DDOS saldırılarının büyük çoğunluğu bantgenişliği taşırma şeklinde gerçekleşmez!

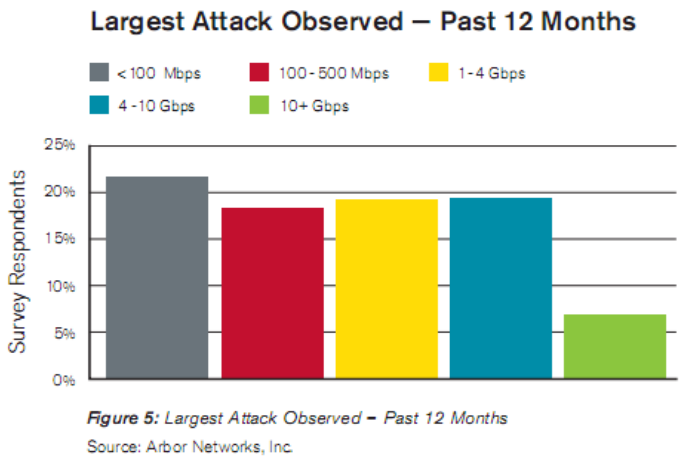


Figure 5: Largest Attack Observed – Past 12 Months

Source: Arbor Networks, Inc.

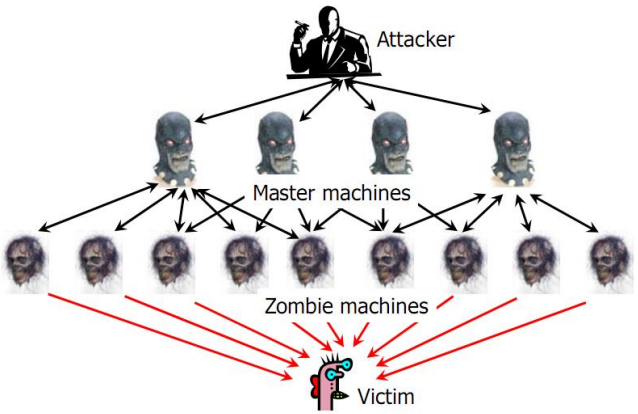
Gürcistan DDOS saldırısı 200-800 Mbps arası

DOS

- DOS(Denial Of Service) = sistemleri çalışamaz hale getirmek için yapılan saldırı tipi.
- DOS saldırılarında kaynak yüzlerce, binlerce farklı sistem değildir.
- Bazı saldırılar özünde DoS, sonuçlarına göre DDoS'tur
  - DDoS görünümlü DoS
  - Tek bir sistemden yapılan spoof edilmiş IP kullanılan SYN flood saldırıları gibi
- DoS saldırılarını engelleme kolaydır

DDoS

- DDOS(Distrubuted Denial of Service) =Dağıtık Servis Engelleme
- Binlerce, yüzbinlerce sistem kullanılarak gerçekleştirilir.
- Genellikle sahte IP adresleri kullanılır
- BotNet'ler kullanılır
- Saldırgan kendini gizler
- Engellemesi zordur!



(ro)BOTNET(works)

- Zombi(roBOT)lerdan oluşan yıkım orduları!
- Her an emir almaya hazır sanal askerlerden oluşur
- Uzaktan yönetilebilirler
  - Sahibi adına istenen bilgileri çalar, saldırı düzenler
- Hiyerarşik yapıda değildir
  - Genelde tek bir yönetici/komutan olur
- Internet üzerinde çeşitli amaçlar için satılmaktadır

IP Spoofing

- TCP/IP paketlerini farklı IP adreslerinden geliyormuş gibi göstermek!
- DoS/DDoS saldırılarında sıkça kullanılır
- IP spoofing UDP tabanlı protokollerde kolaylıkla yapılabilir
  - Udp flood, dns flood, vs
- IP spoofing TCP tabanlı protokollerde sadece bağlantı başlangıç paketi olarak yapılabilir
  - SYN flood, FIN flood gibi
- HTTP GET flood saldırılarında IP spoofing yapılamaz

IP Spoofing-II

- Her sistem ip spoofinge izin vermez
  - NAT arkasındaki sistemler
  - İp spoof korumalı ağlar
- Türkiye'de ADSL aboneleti nat arkasında olduğu için saldırılarda ip spoofing yapılamaz
  - 3g için aynı durum geçerli değil
- Hping ve benzeri araçlarla ip spoofing yapılabilir.
- Hping –a microsoft.com –S –p –flood linux.com

IP Spoof Engelleme

- ISP'ler isterse kendi korumaları altında olan sistemlerden sahte ip adresli paketlerin çıkmasını engeller!
- DDoS saldırılarını engellemedeki en büyük sıkıntı olan IP spoofing çözülürse saldırgan kimliğini/aracı sistemleri bulma kolaylaşacaktır
- URPF kullanarak ip spoofing (internetten gelen paketler için dğeil) engellenebilir
- Urpf RFC'si olan denenmiş bir yöntemdir.

DDoS Hakkında Yanlış Bilinenler

- DDoS saldırıları sizin trafiğinizden daha yüksek boyutta olduğu için engellenemez.
- Yapılan çalışmalar DDoS saldırılarının çok küçük bir bölümünün bandwith şişirme yöntemiyle gerçekleştirğini ortaya koymaktadır.

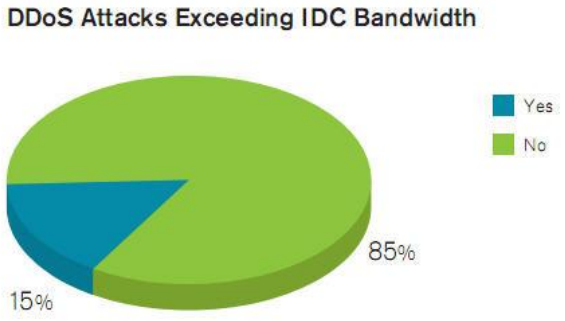


Figure 63
Source: Arbor Networks, Inc.

Attack Subclass	Number of Attacks	Percentage
Total Traffic	209	22.1%
TCP SYN	371	39.3%
TCP RST	49	5.2%
Protocol	12	1.3%
other	260	27.5%
DNS	23	2.4%
Bandwidth	20	2.1%

DDoS Saldırılarında Amaç

- Sistemlere sızma girişimi değildir!!
- Bilgisayar sistemlerini ve bunlara ulaşım yollarını işlevsiz kılmak
- Web sitelerinin ,

E-postaların, telefon

Sistemlerinin, bankacılık

sistemlerinin çalışmaması

BotNet Oluşturma Teknikleri

- Temelde iki tür yöntem vardır
  - Son kullanıcı bilgisayarlarını ele geçirme
  - Sunucuları ele geçirip kullanma
- Sunucular son kullanıcılara göre daha fazla kaynağa sahip olduğu için değerlidir
  - ADSL abonesi max upload 1Mbps
  - Sunucu 100Mbps, 1Gbps ...
- Son dönem moda botnet o luşturma tekniği
  - Sık kullanılan open source web yazılımı sitesini ele geçir, kodlar arasında ajan yazılım yükle ve binlerce sunucuyu aynı anda ele geçirmiş ol!

Türkiye'den Güncel Örnek

- Haziran ayında çok kullanılan blog/portal yazılımının Türkçe sayfası hacklendi
- Hackerlar sisteme sızıp bir sonraki blog sürümüne uzaktan yönetim amaçlı kod eklediler
- İlgili siteden portal yazılımını indiren herkes aynı anda sistemlerini hackerların yönetimine teslim etmiş oldu
  - Bu hacking olayını engelleyecek herhangi bir güvenlik cihazı yok.

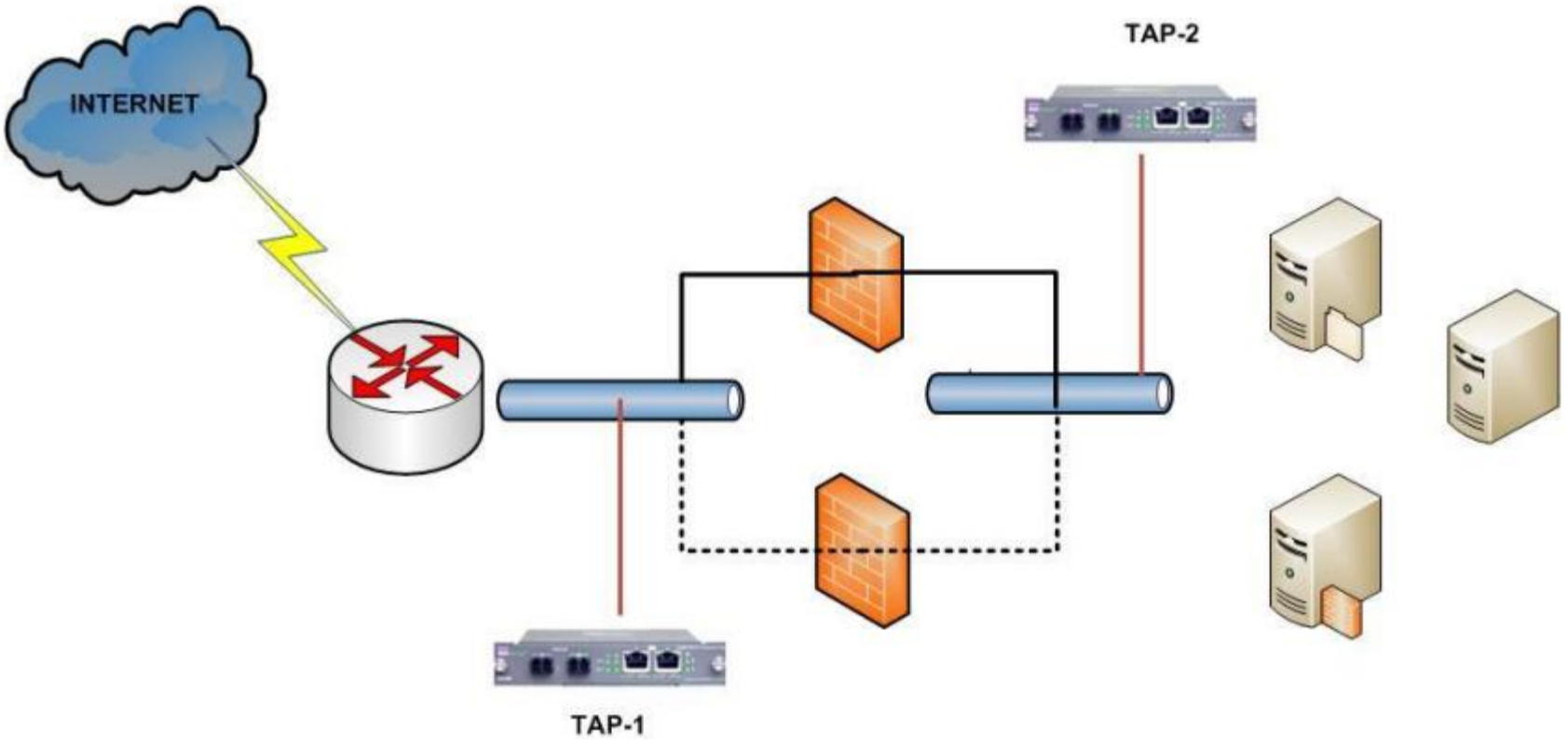
DDOS Saldırı Analizi

- DDoS saldırılarında dikkate alınması gereken iki temel husus vardır.
  - İlki saldırıyı engelleme
  - ikincisi saldırının kim tarafından ne şiddetde ve hangi yöntemler, araçlar kullanılarak yapıldığınının belirlenmesidir.
- Analiz kısmı genellikle unutulur fakat en az engelleme kadar önemlidir
  - Aynı saldırı tekrar ederse nasıl engelleme yapılacağı konusunda yol haritası çıkarılmış olmalı

DDoS Analizi İçin Gerekli Yapının Kurulması

- Amaç DDoS saldırılarında otomatik olarak devreye girip saldırıya ait delil olabilecek paketlerin kaydı
- Saldırı anında paketler kaydedilirse saldırıya ait tüm detaylar istenildiği zaman öğrenilebilir
- Paket kaydı hedef sistem üzerinde (Windows/Linux) veya ağ ortamında TAP/SPAN portu aracılığıyla yapılabilir
- Paket kaydında tcpdump, Wireshark kullanılabilir

DDoS Analizi İçin Gerekli Yapının Kurulması



Saldırı Analizinde Cevabı Aranan Sorular

- Gerçekten bir DDoS saldırısı var mı?
- Varsa nasıl anlaşılır?
- DDoS saldırısının tipi nedir?
- DDoS saldırısının şiddeti nedir?
- Saldırı ne kadar sürmüş?
- DDoS saldırısında gerçek IP adresleri mi spoofed IPadresleri mi kullanılmış?
- DDoS saldırısı hangi ülke/ülkelerden geliyor?

Saldırı Analizinde Kullanılan Araçlar

- Tcpstat
- Tcpdstat
- Tcptrace
- Tcpdump, Wireshark
- Ourmon,
- Argus
- Urlsnarf
- Snort
- Aguri
- Cut, grep, awk, wc gibi UNIX araçları

DDoS Saldırılarında Delil Toplama

- DDoS saldırılarında sonradan incelenmek üzere paketler kaydedilmelidir.
- Kydedilen trafik miktarına bağlı olarak ciddi sistemlere(CPU, RAM, Disk alanı bakımından) ihtiyaç olabilir.
- Paket kaydetme işlemi kesinlikle aktif cihazlar tarafından (IPS, DDoS engelleme Sistemi, Firewall) yapılmamalıdır.
- Tüm paket detayları kaydedilmelidir!
  - Tcpdump –s0

Tcpdump ile DDoS Paketlerini Kaydetme

- #tcpdump –n -w ddostest1.pcap –C 2000 –s0
  - -n isim-ip çözümlemesi yapma
  - -w ddostest1.pcap dosyasına kaydet
  - Dosya boyutu 2GB olduktan sonra başka dosyaya yaz
  - -s0 pakete ait başlık ve payload bilgilerini kaydet

DDoS Saldırı Tipi Belirleme

- Amaç yapılan saldırının tipini belirlemek
- Hangi protokol kullanılarak gerçekleştirilmiş
  - TCP mi? UDP mi? ICMP mi?
- İlk olarak protokol belirlenmeli
- Protokol tipini belirlemek için tcpdstat aracı kullanılabilir
  - **tcpdstat -n ddos.pcap**

Tcpdstat İle DDoS tipini Belirleme

```
# tcpdstat -n ddos.pcap

DumpFile: ddos.pcap
FileSize: 45.58MB
Id: 201005181114
StartTime: Tue May 18 11:14:57 2010
EndTime:   Tue May 18 11:16:19 2010
TotalTime: 81.59 seconds
TotalCapSize: 37.38MB  CapLen: 96 bytes
# of packets: 537187 (170.55MB)
AvgRate: 17.55Mbps  stddev:7.87M

### Packet Size Distribution (including MAC headers) ###
<<<<
 [  32-  63]:    337610
 [  64-  127]:    13257
 [  128-  255]:    5341
 [  256-  511]:    19289
 [  512- 1023]:    104016
 [ 1024- 2047]:    57674
>>>>

### Protocol Breakdown ###
<<<<
   protocol        packets            bytes        bytes/pkt
-------------------------------------------------------------------------
[0] total       537187 (100.00%)     178836761 (100.00%)   332.91
[1] ip          537082 ( 99.98%)     178830375 (100.00%)   332.97
[2] tcp         529590 ( 98.59%)     178126550 ( 99.60%)   336.35
[3]  http(s)    169318 ( 31.52%)     123244600 ( 68.91%)   727.89
[3]  http(c)    113553 ( 21.14%)      34132760 ( 19.09%)   300.59
[3]  squid           9 (  0.00%)           540 (  0.00%)    60.00
[3]  smtp       238109 ( 44.33%)      14288975 (  7.99%)    60.01
[3]  nntp            3 (  0.00%)           180 (  0.00%)    60.00
```

```
[2] tcp         529590 ( 98.59%)      178126550 (
99.60%)   336.35
[3]  smtp       238109 ( 44.33%)      14288975
( 7.99%)    60.01
```

Saldırının Şiddetini Belirleme

- Saldırının şiddetini iki şekilde tanımlayabiliriz
  - Gelen trafiğin ne kadar bant genişliği harcadığı
  - Gelen trafiğin PPS değeri
- PPS=Packet Per Second
- Tcpstat aracı kullanılarak trafik dosyaları üzerinde saldırının PPS değeri, ne kadar bantgenişliği harcandığı bilgileri detaylı olarak belirlenebilir.

Tcpstat

```
[root@netdos1 ~]# tcpstat -i br0  -o "Byte/s:%B MinPacketSize:%m  PPS:%p  TCP:%T  UDP:%U \n"  5
pcap_open():
[root@netdos1 ~]# tcpstat -i em0  -o "Byte/s:%B MinPacketSize:%m  PPS:%p  TCP:%T  UDP:%U \n"  5
Byte/s:2853864.00 MinPacketSize:40  PPS:4625.80  TCP:22581  UDP:545
Byte/s:3163546.00 MinPacketSize:40  PPS:5025.20  TCP:24659  UDP:462
Byte/s:3341800.60 MinPacketSize:40  PPS:5332.80  TCP:26007  UDP:651
Byte/s:2213971.80 MinPacketSize:40  PPS:3709.60  TCP:17993  UDP:551
Byte/s:2828787.00 MinPacketSize:40  PPS:5639.40  TCP:27704  UDP:448
Byte/s:2027139.80 MinPacketSize:40  PPS:7679.20  TCP:37505  UDP:654
Byte/s:2153821.80 MinPacketSize:40  PPS:6045.40  TCP:29641  UDP:427
Byte/s:2183682.20 MinPacketSize:40  PPS:5952.00  TCP:28907  UDP:703
Byte/s:2027648.60 MinPacketSize:40  PPS:3296.60  TCP:15966  UDP:506
Byte/s:2413845.20 MinPacketSize:40  PPS:6031.20  TCP:29434  UDP:622
Byte/s:2619756.40 MinPacketSize:40  PPS:7170.60  TCP:35050  UDP:629
Byte/s:2311282.00 MinPacketSize:40  PPS:7137.80  TCP:34933  UDP:567
```

Saldırı Kaynağını Belirleme

- DDoS saldırılarında en önemli sorunlardan biri saldırıyı gerçekleştiren asıl kaynağın bulunamamasıdır.
- Bunun temel sebepleri saldırıyı gerçekleştirenlerin zombie sistemler kullanarak kendilerini saklamaları ve bazı saldırı tiplerinde gerçek IP adresleri yerine spoof edilmiş IP adreslerinin kullanılmasıdır.
- Saldırı analizinde saldırıda kullanılan IP adreslerinin gerçek IP'ler mi yoksa spoofed IPler mi olduğu rahatlıkla anlaşılabilir.

Spoof IP Belirleme

- Saldırının gerçek IP adreslerinden mi Spoof edilmiş IP adreslerinden mi gerçekleştirildiği nasıl belirlenebilir?
  - Internet üzerinde sık kullanılan DDoS araçları incelendiğinde IP spoofing seçeneği aktif kullanılırsa random üretilmiş sahte IP adreslerinden tek bir paket gönderildiği görülecektir.
- Fazla sayıda tek bağlantı gözüküyorsa saldırının spoof edilmiş IP adresleri kullanılarak gerçekleştirildiği varsayılabilir.

Spoof IP Belirleme-II

- Tek cümleyle özetleyecek olursak: **Eğer aynı IPden birden fazla bağlantı yoksa spoofed IP kullanılmış olma ihtimali yüksektir.**

```
#tcpdump -n -r ddos.pcap |awk -F" " '{print $3}'|cut -f1,2,3,4 -d"."|sort -n|uniq -c
   1 6.65.194.168
   1 6.65.208.248
   1 6.65.226.233
   1 6.65.232.125
   1 6.65.235.140
   1 6.65.248.199
   1 6.65.249.104
   1 6.65.32.97
   1 6.65.44.199
   1 6.65.48.49
   1 6.65.62.221
   1 6.65.62.30
   1 37.83.136.81
   1 37.83.14.12
   1 37.83.152.203
   1 37.83.164.223
   1 37.83.165.146
   1 37.83.166.132
   1 37.83.185.89
   1 37.83.194.21
   1 62.185.46.86
   1 62.185.60.100
   1 62.185.64.248
```

Açık Kaynak Yazılımlarla DDoS Engelleme

- Açık kaynak yazılımlar kullanılarak DDoS saldırıları büyük oranda engellenebilir
- Linux ve türevleri DDoS engellemede yetersiz kalmaktadır
  - İptables'in syncookie, syn proxy özelliği yok
- OpenBSD, FreeBSD packet filter ve Snort (+diğer yazılımlarla) tam teşekküllü DDoS analiz ve engelleme sistemi kurulabilir

OpenBSD Packet Filter

- *BSD dünyasının de fakto güvenlik duvarı yazılımı
- Piyasadaki tüm ticari-açık kod güvenlik duvarlarının teknik kabiliyetlerinin üzerindedir
  - 100Mb hat %3 CPU kullanımı (100.000 session)
- Kullanımı UNIX/Linux sistemlerin tersine çok kolaydır
  - İngilizce yazar gibi kural yazma kolaylığı
  - Pass in on $ext_if proto tcp from 1.1.1.1 to 1.1.1.2 port 80

Packet Filter Firewall Özellikleri

- IP başına session başına limit koyma özelliği
- SYN Proxy özelliği
  - TCP authentication özelliği
- HA(Yüksek bulunurluk) özelliği
- Anormal paketleri (port tarama, işletim sistemi saptama, traceroute vs) engelleme özelliği

DDoS Koruma:Anormal Paketler

- TCP bağlantılarında ilk paket mutlaka SYN olmalıdır
- FIN flood, ACK flood, PUSH flood gibi saldırılarda ilk paket SYN değildir

State Tablosu Belirleme

- Toplamda kaç adet session(durum) tutulacağını belirler
  - Fiziksel ram miktarıyla doğru orantılıdır
  - set limit states 10500000
- Kaç adet kaynak IP adresine ait bilgi tutulacağını belirler
  - set limit src-nodes 5000000

Durum Tablosu Görüntüleme

```
Status: Enabled for 145 days 20:56:40          Debug: Urgent

Interface Stats for em0                 IPv4              IPv6
  Bytes In                    5332984625231          29739690
  Bytes Out                  14370657365878                 0
  Packets In
    Passed                    13580471481            222550
    Blocked                     788635885                 0
  Packets Out
    Passed                    20182481531                 0
    Blocked                     150586291                 0

State Table                          Total             Rate
  current entries                     8908
  searches                      67593686319         5363.1/s
  inserts                         353680459           28.1/s
  removals                        353671551           28.1/s
Counters
  match                         35025741018         2779.1/s
  bad-offset                            0            0.0/s
  fragment                           4244            0.0/s
  short                           3728791            0.3/s
  normalize                             0            0.0/s
  memory                            52669            0.0/s
  bad-timestamp                         0            0.0/s
  congestion                            0            0.0/s
  ip-option                         75916            0.0/s
  proto-cksum                       85428            0.0/s
  state-mismatch                   828435            0.1/s
  state-insert                      16403            0.0/s
  state-limit                           0            0.0/s
  src-limit                       2418414            0.2/s
  synproxy                      472858114           37.5/s
```

FIN/ACK/PUSH Flood Engelleme

- TCP connection flood engelleme özelliği
- Temel mantık:İlk gelen paketin SYN olma zorunluluğu
- pass in log(all) on $ext_if proto tcp to $WEB_SUNUCU port 8000 **flags S/SA keep state**

Syn Flood Engelleme

- Packet Filter syn flood engelleme yöntemlerinden syn cookie değil syn proxy'i kullanır
- Syn proxy sesssion tuttuğu için sistemdeki fiziksel ram miktarı önemlidir

Packet Filter SynProxy Kullanımı

- pass in log(all) on $ext_if proto tcp to $web_server port {80 443} ***flags S/SA*** **synproxy state**

HTTP GET/POST Flood Engelleme

- HTTP GET/POST flood saldırılarında IP spoofing yapılamaz
- Saldırının başarılı olması için binlerce IP adresinden onlarca HTTP GET paketi gönderilmelidir
- OpenBSD PF kullanarak bir IP adresinden eş zamanlı veya belirli süree gelebilecek paket sayısını kısıtlayabiliriz
  - Rate limiting özelliği
- Belirli seviyenin üzerinde paket gönderenler engellenir!

HTTP GET Flood Engelleme-II

- HTTP GET paketi boyutu 400 Byte
- TCP SYN paketi boyutu 60 Byte
- HTTP GET flood saldırılarında sahip olduğumuz bandwith'in 8 katına kadar DDoS saldırılarını başarıyla engelleyebiliriz
  - Nasıl mı?

Packet Filter HTTP Flood Engelleme

- pass in log(all) quick on $ext_if proto tcp\

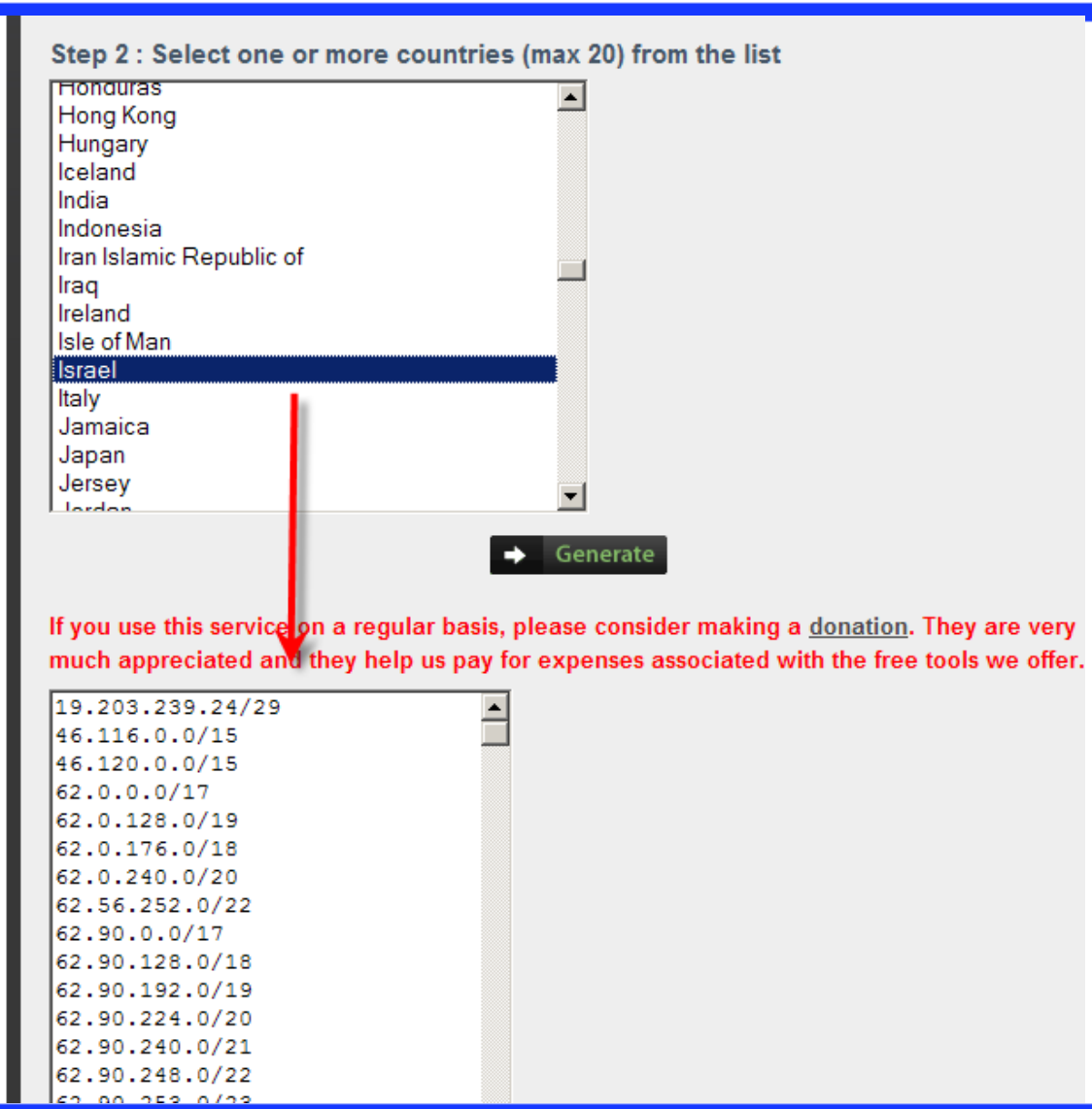
to $web_server port {80 443} flags S/SA\

synproxy state (max-src-conn 400, max-src-conn-rate 90/3, overload <ddos_host> flush global)

Ülkelere Göre IP Adresi Engelleme

- Özellikle spoof edilmeiş IP kullanılan saldırılarda trafik yoğun olarak bir ülkeden geliyorsa o ülkeye ait ip blokları tümden engellenebilir!
  - O ülkeden glecek ziyaretcilere farklı bir sayfa gösterilmelidir!

Ülke IP Aralıkları



Packet Filter Ülkeye Göre Bloklama

```
table <Turkiye> persist file "/etc/TR"
table <israil> persist file "/etc/Israil"
table <Cin> persist file "/etc/Cin"
table <Rusya> persist file "/etc/Rusya"
table <Usa> persist file "/etc/Usa"
table <India> persist file "/etc/India"
```

```
block in quick log on $ext_if from <israil>
```

```
[root@seclabs ~]# more /etc/israil
19.203.239.24/29
46.116.0.0/15
46.120.0.0/15
62.0.0.0/17
62.0.128.0/19
62.0.176.0/18
62.0.240.0/20
62.56.252.0/22
62.90.0.0/17
62.90.128.0/18
62.90.192.0/19
62.90.224.0/20
62.90.240.0/21
62.90.248.0/22
62.90.253.0/23
```

Unicast Reverse Path Forwarding

- IP spoofing yapılmasını engelleme amaçlı standart bir özelliktir.

```
block in quick from urpf-failed label uRPF
```

DDoS-BotNet Çalışma Grubu

- DDoS&BotNet konusundaki bilinç düzeyini arttırmak ve bu konudaki gelişmeleri paylaşmak amacıyla 2010 yılında kurulmuştur.
  - E-posta listesi ve çalışma grubu olarak faaliyet göstermektedir.

- http://www.lifeoverip.net/ddos-listesi/ adresinden üye olabilirsiniz.
  - Sadece kurumsal katılıma açıktır.

NetSec Ağ Ve Bilgi Güvenliği Topluluğu

- Türkiye'nin en geniş katılımlı bilgi güvenliği e-posta listesi ve topluluğu
  - ~1200 üye

- Ücretsiz üye olabilirsiniz.
- Güvenlik dünyasında yayınlanan önemli haberler, güvenlik yamaları ve birçok teknik konuda tartışma...
- Üyelik için
  - http://www.lifeoverip.net/netsec-listesi/

Bilgi Güvenliği AKADEMİSİ