“Siber Saldırı Aracı Olarak DDoS”

Huzeyfe ÖNAL

Bilgi Güvenliği AKADEMİSİ

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

Amaç

- Son yılların en popüler saldırılarından biri olan DDoS'un ne kadar kolay gerçekleştirilip ne kadar zor engellenebildiğinin uygulamalı olarak gösterimi..

Ajanda

- DoS/DDoS hakkında genel terim ve tanımlar
- DDoS saldırıları hakkında hatalı bilgiler ve düzeltmeler
- DDoS saldırı çeşitleri
- Türkiye ve dünyadan DDoS saldırı örnekleri
- “Teknik detay ve uygulamalar”

Siber Saldırılar

- İki türlüdür:
  - Bilginin gizliliğini ihlal etme amaçlı saldırılar
  - Bilgiye erişimi aksatma amaçlı saldırılar
- Gizlilik ihali
  - RSA, SONY örnekleri
- Erişim aksatma
  - Anonymous saldırıları(Türkiye, Malezya, Paypal, Mastercard)

- 62,000 random logins | http

13/06/11

- Senate.gov internal data | http
- Bethesda internal data press release | http | torrent
- Bethesda internal data | http | torrent

10/06/11

- Pron.com user database | http

06/06/11

- Sownage™ 2 press release | http | torrent
- Scedev.net source code | http | torrent
- Sony BMG internal network maps | http | torrent

03/06/11

- Fuck FBI Friday™ press release | http | torrent
- Infragard Atlanta users database | http | torrent
- Karim dox | http | torrent
- Karim IRC log | http | torrent
- Karim emails | torrent
- Nintendo.com webserver configuration | http
- Unveillance secret conference | http

02/06/11

- Sownage™ press release | http | torrent
- Sownage™ summary | http | torrent
- Sonypictures.com AutoTrader users database | http | torrent
- Sonypictures.com Summer of Restless Beauty users database | http | torrent
- Sonypictures.com Sony Wonder coupons database | http | torrent

30/05/11

- PBS.org defacement (pbs.org/lulz) snapshot | http
- PBS.org defacement (fake Tupac article) snapshot | http
- PBS.org internal hosts | http
- PBS.org database list | http
- PBS.org staffers database | http
- PBS.org authors database | http
- PBS.org pressroom users database | http
- PBS.org stations database | http
- PBS.org MySQL users database | http

23/05/11

- Sonymusic.co.jp database | http

15/05/11

- UK ATM database | http

10/05/11

- Fox.com innerworkings | http
- Fox.com/sales database (SQL) | http
- Fox.com/sales database (txt) | http
- Fox.com/sales database cracked passwords | http

```
user_id | user_guid | user_name | email | password_hash | date_of_birth | emailed_token | emailed_token_expires | email_authenticated | created | modified | data_cache
177028 | d28cbf54-ac04-102c-9aee-001e0b208928 | FoxSalesResearchM | FoxSalesResearchM@fox.com | $SNAP$177028FoxSalesResearchMav3lc572yl$a8e46e47495f301cba6894201a3004fd$
00:00:00 | 0 | 2008-05-09 10:10:26 | 2009-06-16 13:31:15 | a:4:{s:10:"first_name";s:6:"Audrey";s:9:"last_name";s:6:"Steele";s:12:"company_name";s:0:"";s:13:"company_title
177093 | d28ceec0-ac04-102c-9aee-001e0b208928 | amih | alan.mih@fox.com | $SNAP$177093amihp1f6HM3fH0$e6d037f1d7cda7cc3abcf47de28518e1$ | 1950-01-01 |  | 0000-00-00 00:00:
06-16 13:31:15 | a:4:{s:10:"first_name";s:4:"Alan";s:9:"last_name";s:3:"Mih";s:12:"company_name";s:0:"";s:13:"company_title";s:0:"";}
177620 | d28d0efa-ac04-102c-9aee-001e0b208928 | szimmerman | szimmerman@optaros.com | $SNAP$177620szimmermanSdoXu56QZn$f038f94a3f68b229368ba5f44832b2ba$ | 1950-01-01 |  |
11 18:43:26 | 2009-06-16 13:31:15 | a:4:{s:10:"first_name";s:5:"Steve";s:9:"last_name";s:9:"Zimmerman";s:12:"company_name";s:0:"";s:13:"company_title";s:0:"";}
177782 | d28d2c96-ac04-102c-9aee-001e0b208928 | abilioa | abilio.andries@fox.com | $SNAP$177782abilioaav3lc572yl$94e5cf83f04627e9f104e9d1556448bb$ | 1950-01-01 |  | 0000-
11:40:40 | 2009-06-16 13:31:15 | a:4:{s:10:"first_name";s:6:"Abilio";s:9:"last_name";s:7:"Andries";s:12:"company_name";s:0:"";s:13:"company_title";s:0:"";}
177812 | d28d4e10-ac04-102c-9aee-001e0b208928 | dmitri | steve.zimmerman@gmail.com | $SNAP$177812dmitriwq4celqpm6$d860791251be70567252edb1d7bbff1d$ | 1950-01-01 |  | 0000
13:15:43 | 2009-06-16 13:31:15 | a:4:{s:10:"first_name";s:6:"Dmitri";s:9:"last_name";s:6:"Dmitri";s:12:"company_name";s:0:"";s:13:"company_title";s:0:"";}
177881 | d28d6f30-ac04-102c-9aee-001e0b208928 | manan2 | mshah@fox.com | $SNAP$177881manan2bm9C6osCZF$4212f8a5b7c6775c3ab54bafa5ec1b43$ | 1950-01-01 |  | 0000-00-00 00:00
2009-06-16 13:31:15 | a:4:{s:10:"first_name";s:5:"Manan";s:9:"last_name";s:4:"Shah";s:12:"company_name";s:0:"";s:13:"company_title";s:0:"";}
178814 | d28d8cea-ac04-102c-9aee-001e0b208928 | dmaharaj | david.maharaj@fox.com | $SNAP$178814dmaharaj762lYhr2F1$81374494052aa4e81b266650ff42eb9f$ | 1950-01-01 |  | 0000
18:02:05 | 2009-06-16 13:31:15 | a:4:{s:10:"first_name";s:5:"David";s:9:"last_name";s:7:"Maharaj";s:12:"company_name";s:0:"";s:13:"company_title";s:0:"";}
```

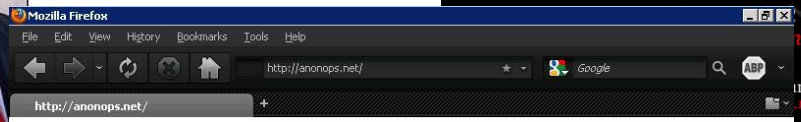
Anonymous TİB'e saldırdı!

**Dün akşam saatlerindeTürkiye'de bazı kamu kurumlarına siber sal
bulunan siber-aktivistler grubu Anonymous, ilk hedef olarak TİB'i s
Oluşum Meteorolojinin ve SGK'nın da sitelerini hedef aldı.**

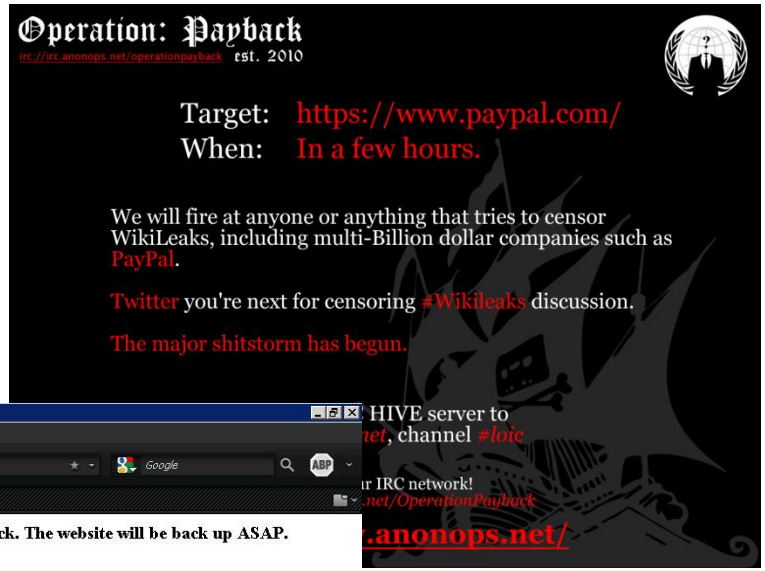
ntvmsnbc ve Ajanslar
Güncelleme: 20:22 TSİ 09 Haziran. 2011 Perşembe

İSTANBUL - Uluslararası siber-aktivistler grubu Anonymous'un Türkiye'de yürürlüğe girecek filtre uygulamasını protesto için yapacağını açıkladığı ilk siber saldırı, dün akşam saatlerinde gerçekleşti ve ilk olarak Telekomünikasyon ve İletişim Başkanlığı'nın sitesini hedef aldı.

Başkanlığın yedek sunucular da dahil 8 ayrı önlemine rağmen, siteye 18:00'den itibaren yaklaşık 20 dakika erişilemedi.



AnonOps is currently under heavy DDoS attack. The website will be back up ASAP.



DOS/DDoS Saldırıları

- Neden DDoS saldırıları yoğun olarak kullanılmaya başlandı?
  - En basit saldırı tipi!
  - Bir adet 100 Mb sunucu+ekmek+yağ+un+su...

Başlamadan Önce...

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

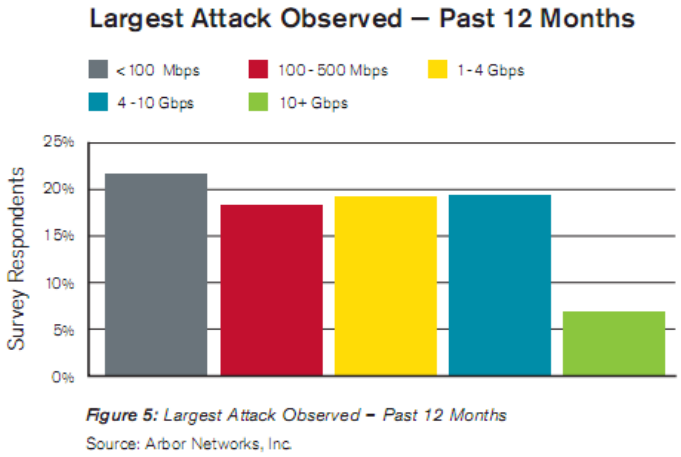


Figure 5: Largest Attack Observed – Past 12 Months

Source: Arbor Networks, Inc.

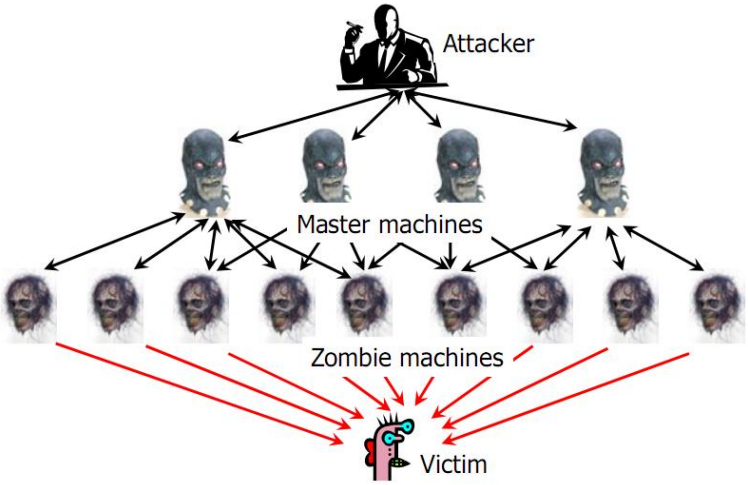
Gürcistan DDOS saldırısı 200-800 Mbps arası

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

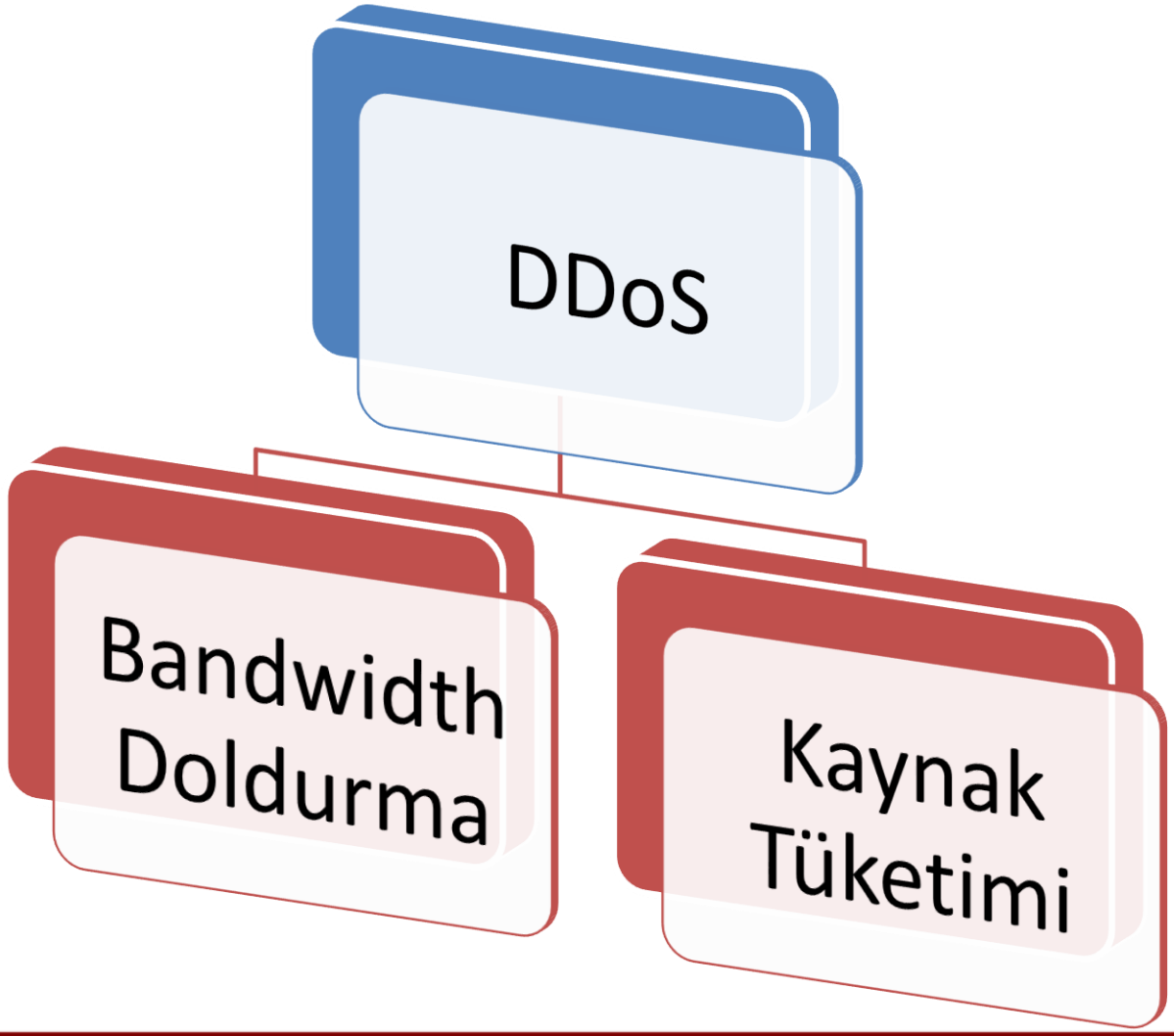
- DDOS(Distrubuted Denial of Service) =Dağıtık Servis Engelleme
- Binlerce, yüzbinlerce sistem kullanılarak gerçekleştirilir.
- Genellikle sahte IP adresleri kullanılır
- BotNet'ler kullanılır
- Saldırgan kendini gizler
- Engellemesi zordur!



DDoS Hacking Yöntemi midir?

- Değildir ”.”

DDoS Çeşitleri



TCP ve UDP Protokollerinde IP Spoofing

TCP

- TCP'de sadece bağlantı başlangıç paketleri spoof edilebilir.
- Veri taşıyan TCP paketleri spoof edilemez
  - Veri taşıma öncesi kurulması gereken üçlü el sıkışma aşaması vardır
- HTTP, HTTPS, SMTP, POP3 gibi uygulama katmanı protokollerde ip spoofing teoride mümkündür!

UDP

- Mümkündür
- Her tür UDP paketi spoof edilmiş ip adreslerinden gönderilebilir.
- DNS istekleri sahte ip adreslerinden gönderilebilir
- UDP kullanan servisler (DNS vs) ip spoofingi engellemek için ek yöntemler geliştirmiştir.

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 Ne 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

DDOS-I:Bandwidth Doldurma

- Önlemenin yolu yoktur
  - Sürahi bardak ilişkisi
- ISP seviyesinde engellenebilir...
- L7 protokolleri kullanılarak yapılan DDOS'larda saldırı trafiği çeşitli yöntemlerle ~6'da birine düşürülebilir
  - HTTP GET flood 400 Byte
  - IP Engelleme sonrası sadece syn paketi gelir(60 byte)

DDOS-II:Ağ/güvenlik Cihazlarını Yorma

- Amaç ağ-güvenlik sistemlerinin kapasitesini zorlama ve kaldıramayacakları kadar yük bindirme
- Session bilgisi tutan ağ/güvenlik

cihazlarının kapasitesi sınırlıdır

Max session 10.000.000

Sık Gerçekleştirilen DDoS Saldırıları

SYN Flood

HTTP Flood

UDP Flood

DNS Flood

SynFlood

- Hedef sisteme kapasitesinin üzerinde SYN paketi göndererek yeni paket alamamasını sağlamaktır
- En sık yapılan DDoS saldırı tipidir
- İlk olarak 1994 yılında “Firewalls and Internet Security “ kitabından teorik olarak bahsi geçmiştir
- İlk Synflood DDoS saldırısı 1996 yılında gerçekleştirilmiştir

Nasıl Gerçekleştirilir?

- Syn Flood saldırısı basitce açık bir porta hedef sistemin kapasitesinden fazla gönderilecek SYN paketleriyle gerçekleştirilir.
- Buradaki “kapasite” tanımı önemlidir. Teknik olarak bu kapasiteye Backlog Queue denilmektedir.
- Saldırıyı yapan kendini gizlemek için gerçek IP adresi kullanmaz

Backlog Queue Kavramı(Kapasite)

- İşletim sistemleri aldığı her SYN paketine karşılık üçlü el sıkışmanın tamamlanacağı ana kadar bellekten bir alan kullanırlar, bu alan TCB olarak adlandırılır
- Bu alanların toplamı backlog queue olarak adlandırılır.
- Başka bir ifadeyle işletim sisteminin half-open olarak ne kadar bağlantı tutabileceğini backlog queue veriyapısı belirler.

Problem|Uygulama

SynFlood Saldırılarını Engelleme

- Syn Flood Saldırısı gerçekleştirme çok kolaydır
- Syn flood saldırılarını engellemek çok kolaydır
- Syn flood saldırıları için tüm dünya iki(+1) temel çözümü kullanır
  - Syn cookie
  - Syn proxy
- Bunun haricinde sık tercih edilmeyen iki yöntem daha vardır
  - DFAS(Drop First Accept Second)*
  - Anormallik tespiti

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

Uygulama|Syn Flood Analizi

HTTP Flood

- HTTP Protokolü kullanılarak gerçekleştirilen DoS/DDoS saldırı tipi
- Neden HTTP?
- %99,999 firma/kurum dışarı HTTP servisini açmış durumdadır.
- HTTP en kolay hedeftir!
- Literatürde GET Flood, POST Flood olarak geçer.

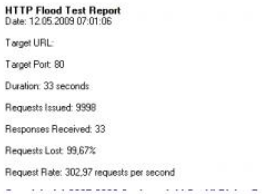
GET/POST Flood Saldırıları

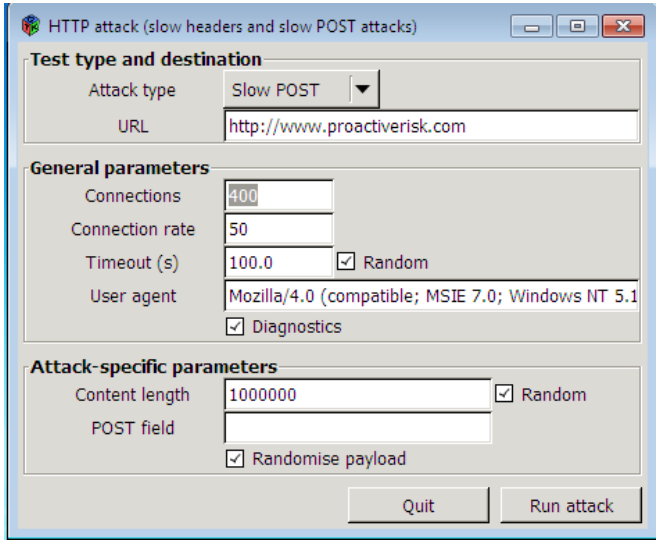
- Synflood için önlem alınan yerlere karşı denenir
- Daha çok web sunucunun limitlerini zorlayarak sayfanın ulaşılamaz olmasını sağlar
- Önlemesi Synflood'a göre daha kolaydır
  - HTTP için IP spoofing "pratik olarak" imkansızdır.
- #ab –n 100000 –c 5000 http://www.google.com/

HTTP Flood Test Araçları

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

Basit bir adsl hattından yapılan deneme ve sonuçları





HTTP Flood Engelleme

- HTTP Flood saldırılarını normal HTTP isteklerinden ayırt etmek oldukça güçtür.
- Genel HTTP Flood belirleme yöntemleri:
  - Bir ip belirli sayıdan fazla GET/POST isteği göndermektedir (f5 tuşu?)
    - Proxy arkasından yüzlerce sistem bağlanıyor olabilir
  - Gelen saldırıda HTTP başlık bilgileri tam değildir
    - Referrer bilgisi eksik, User-agent eksik, Protokol bilgisi eksik, URL olarak sadece ana sayfa defalarca isteniyor...
- Rate limiting ya da başlık bilgisi kullanılarak engellenebilir
  - False positive riski ...

Uygulama|HTTP Flood Analizi

UDP Flood

- UDP paketleri kullanılarak gerçekleştirilir
- Hedef sistemde açık (Firewall'dan) Udp portu varsa bu porta yönelik gönderilecek her udp paket oturum tablosunda yer edinecektir
  - Bir udp paketi için timeout suresi ortalama 60 sn.
  - UDP paketleri küçüktür.
  - 100 Mb ile 300.000 UDP paketi gönderilebilir.

UDP Flood Engelleme

- Kesin bir yöntem yoktur!
  - IP spoofing her durumda mümkündür, engellenemez!
- Genel engelleme yöntemleri
  - Gereksiz udp portlarının kapatılması!
  - Açık portlarda “protokol” kontrolü
    - Gelen paket DNS mi? Boş udp paketi mi?
  - Rate limiting
    - Belirli sayıdan fazla udp paketi gönderenleri karantinaya al
- False positive durumu...

Uygulama|UDP Flood Analizi

DNS Flood

- 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 Sunucuya boş dns paketleri gönderme(session sayısı doldurma amaçlı)

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
- İlk isteği reddet aynı istek ikinci kere gelirse kabul et!

Uygulama|DNS Flood Analizi

Türkiye'den Güncel Örnek

- Güncel saldırı
- DNS Flood
- Kaynak IP Adresleri →
- Saldırgan gerçek DNS sunucu ip

Adreslerini spoof ederek gönderiyor paketleri

- Nasıl engellenecek?
  - IP engelleme?
  - Rate limiting?

195.175.39.3
195.175.39.5
195.175.39.7
195.175.39.9
195.175.39.11
195.175.39.13
195.175.39.15
195.175.39.17
195.175.39.75
195.175.39.76
195.175.39.77
195.175.39.81
195.175.39.136
195.175.39.137
195.175.39.138
195.175.39.229

Sonuç

- DDoS klasik bir saldırı tipi değildir, klasik yöntem ve araçlarla engellenemez!
- DDoS bir altyapı problemidir! Altyapınızı ne kadar güçlü tutarsanız (Altyapı!= fiziksel altyapı) o kadar korunaklı olursunuz.
- DDoS saldırılarında en önemli bileşen TCP/IP bilgisidir.

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