DoS/DDoS Saldırıları ve Koruma

Ozan Berk Aktaş

İÇİNDEKİLER

DoS Nedir ? 3
DDoS Nedir ? 3
Zombi PC Nedir? 3
BOTNET Nedir ? 3
PROTOKOLLER 3
IP (Internet Protocol address) 3
TCP (Transmission Control Protocol) 3
TCP BAĞLANTISI NASIL KURULUR ? 3
ACK 3
SYN 4
FIN 4
RST 4
URG 4
PSJ 4
UDP (User Datagram Protocol) 4
TCP-UDP FARKLARI 4
ICMP (INTERNET CONTROL MESSAGE PROTOCOL) 4
NTP (Network Time Protocol) 4
HTTP/HTTPS & DNS 4
HTTP (HyperText Transfer Protocol) 4
HTTPS (HyperText Transfer Protocol Secure) 4
DNS (Domain Name System) 5
DDoS Saldırı Çeşitleri 5
Volumetrik Saldırılar (Ağ) 5
UDF FLOOD 5
ÖNLEMLER 5
ICMP FLOOD 6
ÖNLEMLER 6
Reflection Amplification (Yansıma Yükseltme) 6
ÖNLEMLER 6
SYN FLOOD SALDIRILARI 7
ÖNLEMLER 7
SLOWLORİS SALDIRILARI 7
ÖNLEMLER 7

DoS Nedir ?

DOS (Denial Of Service) , sistemleri aksatmak ya da durdurmak için yapılan saldırı türü

DDoS Nedir ?

DDOS (Distrubuted Denial of Service) **DOS** saldırısının yüzlerce, binlerce **farklı** sistemden saldırısının yüzlerce, binlerce **farklı** sistemden yapılması. Genellikle spoof edilmiş ip adresleri ve zombiler kullanılır.

Zombi PC Nedir?

Sahibinin haberi olmadan , virüs ile ele geçirilmiş ve çeşitli amaçlar için kullanılan bilgisayarladır.

BOTNET Nedir ?

Zombi Bilgisayarlar tarafından oluşturulmuş bir ordu. Bu ordu tek bir saldırgan tarafından kontrol edilerek hedef sunuculara karşı koordineli saldırılar başlatmak için kullanılır.

PROTOKOLLER

IP (Internet Protocol address)

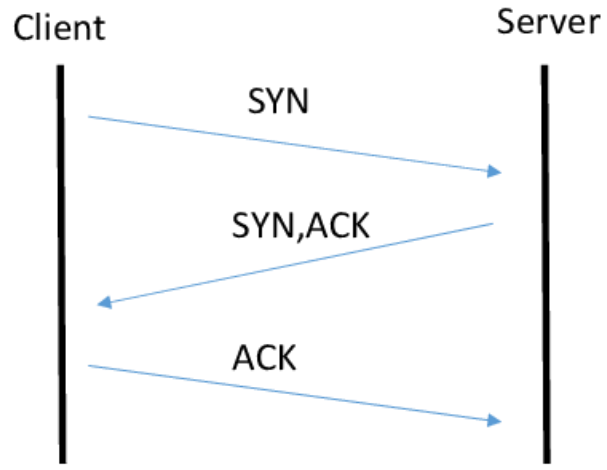
interneti ya da TCP/IP protokolünü kullanan diğer paket anahtarlamalı ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adres.

İnternet'e bağlanan her cihaza, İnternet Servis Sağlayıcısı tarafından bir IP adresi atanır ve internetteki diğer cihazlar bu cihazlara verilen IP adresleri ile ulaşırlar. IP adresine sahip iki farklı cihaz aynı ağda olmasa dahi, yönlendiriciler (router) vasıtası ile birbirleri ile iletişim kurabilirler.

TCP (Transmission Control Protocol)

Bilgisayarlar arasındaki iletişimin kayıpsız olarak ve küçük paketler hâlinde gerçekleştirilmesine yarayan bir protokoldür. Aslında veriyi alırken ya da karşı tarafa gönderirken verinin bütünlüğünü sağlaması ve kimlik doğrulaması yapması **TCP** protokolünün en önemli özelliğidir.

TCP BAĞLANTISI NASIL KURULUR ?



ACK: VERİLERİN KARŞI TARAFA SORUNSUZCA ULAŞTIĞINI BELİRTİR.

SYN: TCP BAĞLANTISININ KURULUCAĞINI BELİRTİR.

FIN: TCP OTURUMUNUN SONLANDIRILMASINI SAĞLAR.

RST: BAĞLANTIDA HATA OLDUĞUNU BAĞLANTIYI KESMESİNİ SAĞLAR

URG: GELEN VERİ PARÇALARININ ÖNCELLİKLİ OLARAK İŞLEME ALINMASINI SAĞLAR.

PSJ: VERİ PARÇALARI ARASINDA ÖNCELLİK BELİRTMEK İÇİN KULLANILIR.

UDP (User Datagram Protocol)

UDP'nin temel işlevi verilerin gönderimini bağlantı kurulmaksızın gerçekleştirmektir. UDP protokolü yeni nesil bilgisayar ağlarında datagram modu oluşturabilmek için geliştirilmiştir. Böylelikle bilgisayarlarda paket anahtarlı bilgisayar iletişimi mümkün olabilmektedir.

UDP, WAN ağlarında veri aktarımında kullanılır. Ses ve görüntüler eş zamanlı aktarımını gerçekleştirebilir. UDP diğer protokollerin aksine kurulum ve akış kontrolü gerektirmediği için veri iletim hızı yüksektir.

UDP , güvenilir olmayan protokol olarak nitelendirilmektedir. Kullanılan ağ üzerinden veriyi gönderdikten sonra gidip gitmediğinin bilgisine ulaşamazsınız. Bu durumda ise daha güvenli bir şekilde veri aktarımı gerçekleştirmek isteyen firmalar bunu kendi yöntemleri ile gerçekleştirmektedirler. TCP protokolü ile aktarım yaptığınızda verileriniz sıralı bir şekilde giderken UDP'de sıralı bir şekilde gitmez.

TCP-UDP FARKLARI

- **TCP**: **UDP** 'den daha yavaştır, çünkü verinin karşı tarafa ulaşıp ulaşmadığını kontrol eder.
- **UDP**: Ses ve video gönderiminde kullanılır. **TCP**'ye göre daha hızlıdır fakat güvenli değildir. Veri ismine datagram denilir.

ICMP (INTERNET CONTROL MESSAGE PROTOCOL)

TCP/IP İşlenmesini sağlar. Hata durumunda host tarafından geri bilgilendirmeyi sağlar. ICMP, aAğ hakkında bazı bilgileri toplamak amacı ile de kullanılır. **Traceroute** ve **Ping** ICMP Kullanır.

NTP (Network Time Protocol)

NTP Network Time Protocol'ün kısaltmasıdır. Türkçesi Ağ Zaman Protokolü'dür. NTP, değişken gecikmeye sahip paket anahtarlamalı ağlar üzerindeki bilgisayarların saatlerinin eş zamanlanmasının sağlanması için kullanılan bir protokoldür.

HTTP/HTTPS & DNS

HTTP (HyperText Transfer Protocol)

Aslında en basit haliyle söylersek web sayfalarının görüntülenmesini sağlayan protokoldür. HTTP, kullanıcının bilgisayarı ve sunucu(server) arasındaki veri alışverişinin kurallarını belirler. Bu protokolü kullanmak için tarayıcı kullanılır. Google Chrome, Mozilla Firefox, Internet Explorer bu web tarayıcılarından bazılarıdır. Bu tarayıcılar yardımı ile herhangi bir internet sitesine girmek için adres çubuğuna sitenin adresini yazdığınız vakit HTTP ile sunucuya bir istek gönderilir ve sunucu bu isteğe cevap verdiği vakit internet sitesinin verileri size gelir.

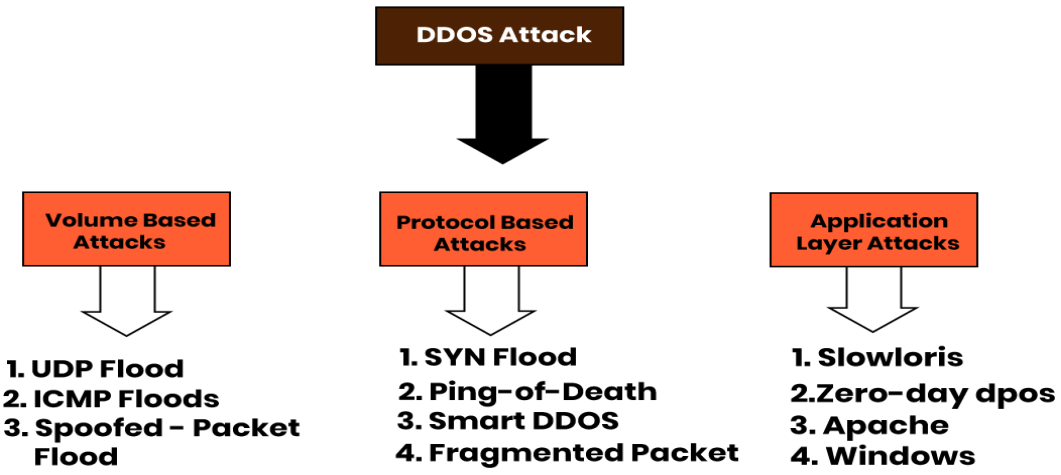
HTTPS (HyperText Transfer Protocol Secure)

HTTP ile aynı özelliği taşır fakat bu yapıda kendi içerisinde TSL/SSL barındırdığı için 2 taraf arasındaki iletişim güvenlidir.

DNS (Domain Name System)

İnternet ağını oluşturan her birim sadece kendine ait bir IP adresine sahiptir. Bu IP adresleri kullanıcıların kullanımı için www.site_ismi.com gibi kolay hatırlanır adreslere karşılık düşürülür. DNS sunucuları, internet adreslerinin IP adresi karşılığını kayıtlı tutmaktadır.

DDoS Saldırı Çeşitleri



Volumetrik Saldırılar (Ağ)

Saldırganlar tarafından en sık kullanılan atak çeşidi olup hedef organizasyonların kullanmakta olduğu internet bant genişliğini tüketmeyi hedeflemektedir. Bu şekilde gerek organizasyona gelen ağ trafiği gerek organizasyondan dışarı çıkan ağ trafiği etkilenecek ve meşru isteklere cevap veremeyerek servis dışı kalacaktır.

Volümetrik saldırılara örnek olarak; TCP/UDP Flood, DNS/NTP/Mamcached Amplifikasyonu saldırıları verilebilir.

UDP FLOOD

Güvenlik Duvarının oturum tablosunu doldurarak erişilmez hale getirir. Hedef sistemin rastgele

Portlarına çok fazla sayıda UDP Paketi gönderilmesi prensibine dayanır.

Çok fazla UDP Paketi geldiğinde sistem ICMP Paketi ile karşılık verir. Bu döngü sonucunda ise çok sayıda UDP Paketine , çok sayıda ICMP Paketi ile karşılık verildiği için hedef sistem erişilmez duruma gelir.

ÖNLEMLER

- Güçlü güvenlik duvarları
- Belirli ip adreslerinden gelecek istekler sınırlandırılmalı
- Timeout değerlerini düşürme
- Timeout ile UDP Sessionların kapatılması sağlanabilir.
- Rate Limiting özelliği ile bir ip adresinden 500'den fazla istek geldiyse engellenecek listesine alınabilir ve ip adresine ait oturum tablosu temizlenebilir.

ICMP FLOOD

Hedef sisteme yönelik aşırı yük oluşturmak için kullanılır. Gelen ve giden bant genişliğine aşırı Yük bindirerek sistemi çalışılmaz hale getirmek için kullanılır.

ÖNLEMLER

- Gelen paketlere boyut sınırlandırılması getirilebilir.
- Süre aralığı verilip gelen paketlerin sayısı ve boyutu kısıtlanabilir.
- ICMP Hata mesajlarının dışarı çıkışına izin verilebilir.
- İnternetten iç ağa ICMP trafiği engellenebilir.
-

Reflection Amplification (Yansıma Yükseltme)

Bir yansıma saldırısı, bir saldırganın, bir hedefin IP adresini yanıltması ve öncelikle Kullanıcı Datagram Protokolü'nü (UDP) veya bazı durumlarda İletim Kontrol Protokolü'nü (TCP) kullanarak bilgi talebi göndermesini içerir. Sunucu daha sonra isteğe yanıt vererek hedefin IP adresine bir yanıt gönderir. Her iki yönde de aynı protokolü kullanan bu "yansıma", yansıma saldırısı olarak adlandırılmasının nedenidir. UDP veya TCP tabanlı hizmetleri çalıştıran herhangi bir sunucu yansıtıcı olarak hedeflenebilir.

Amplifikasyon saldırıları, aracıyı uyarmadan hedef web sitesini bunaltmak için kullanılan yüksek hacimli paketler üretir. Bu, güvenlik açığı bulunan bir hizmetin, saldırgan isteğini gönderdiğinde, genellikle "tetikleme paketi" olarak adlandırılan büyük bir yanıtla yanıt verdiğinde ortaya çıkar. Saldırgan, hazır araçları kullanarak bu isteklerin binlercesini savunmasız hizmetlere gönderebilir, böylece orijinal istekten önemli ölçüde daha büyük yanıtlara neden olur ve hedefe verilen boyut ve bant genişliğini önemli ölçüde artırır.

Yansıma büyütme saldırısı, saldırganların hem oluşturabilecekleri kötü amaçlı trafik miktarını büyütmelerine hem de saldırı trafiğinin kaynaklarını gizlemelerine olanak tanıyan bir tekniktir. Bu tür dağıtılmış hizmet reddi (DDoS) saldırısı , hedefi bunaltarak sistemlerin ve hizmetlerin kesintiye uğramasına veya kesintiye uğramasına neden olur.

Bu saldırıların en yaygın biçimleri, milyonlarca açıkta kalan DNS, NTP, SNMP, SSDP ve diğer UDP/TCP tabanlı hizmetlere dayanır.

ÖNLEMLER

Yansıma yükseltme saldırılarına karşı birincil savunma, sahte kaynak paketlerini engellemektir. Saldırılar, DNS ve NTP gibi güvenilir hizmetleri kullanan meşru kaynaklardan geldiğinden, gerçek kullanıcı iş yükleri ile saldırganlar tarafından oluşturulan yansıtılan trafik arasındaki farkı söylemek zorlaşır. Zorluklara ek olarak, bir hizmet saldırıya uğradığında, hizmetteki yavaşlama nedeniyle meşru kullanıcı trafiği yanıtları yeniden denemek zorunda kalabilir ve bu yeniden denemelerin kendi ayinlerinde yanlışlıkla DDoS saldırıları olarak tanımlanmasına neden olabilir.

Kuruluşlar, yansıma büyütme saldırılarını azaltmak için aşağıdaki adımları atabilir:

- Genel bir DDoS azaltma stratejisi, sistemlerin aşırı yüklenmesini önlemek için hedeflere
- veya kaynaklara uygulanabilen hız sınırlaması kullanmaktır. Hedef hız sınırlaması, yasal trafiği istemeden etkileyebilir, bu da bunu daha az arzu edilen bir yaklaşım haline getirir. Kaynağı

sınırlayan hız daha etkili kabul edilir. Bu yaklaşım, kaynakları önceden oluşturulmuş bir erişim politikasından sapmaya dayalı olarak kısıtlar.

- Gerekli olmayan bağlantı noktalarının engellenmesi, saldırılara karşı güvenlik açığını azaltabilir. Ancak bu, hem yasal hem de saldırgan trafiği tarafından kullanılan bağlantı noktalarına yönelik saldırıları engellemez.
- Trafik imza filtreleri, bir saldırının göstergesi olan tekrarlayan yapıları tanımlamak için kullanılabilir. Bu tür filtrelemenin dezavantajı, performans üzerindeki etkisi olabilir. Her paketi incelemek, nihayetinde savunmaları bunaltabilir.
- Tehdit istihbaratı hizmetleri, kuruluşların savunmasız sunucuları tanımlamasına yardımcı olabilir ve bu savunmasız sunucuların IP adreslerini engellemelerine olanak tanır. Bu proaktif yaklaşım, daha kesin azaltma sağlayabilir. Netscout/Arbor, DDoS Reflektörleri olarak aktif olarak kullanılan savunmasız sunucular hakkında güncel bilgileri içeren bir dizi AIF filtre listesini düzenli olarak yayınlar.

SYN FLOOD SALDIRILARI

En çok kullanılan DDoS saldıır tipi. Mevcut sunucu kaynaklarını tüketmeyi amaçlar. SYN Paketlerini

Tekrar tekrar göndererek , hedef makinadaki tüm kullanılabilir bağlantı noktalarını doldurabilir ve

Hedeflenen aygıtın trafiğe yavaş bir şekilde yanıt vermesini veya hiç yanıt vermemesini neden olabilir. Sahte ip adresleri ile hedefe çok yüksek hacimde SYN Paketleri gönderir, sunucu bu paketlere yanıt verdikçe açık oluşur.

ÖNLEMLER

- Server bağlantı isteğinin kapasitesini artıra bilirisiniz.
- En eskiden başlayak ACK Paketlerini sonlandırabilirsiniz.
- Timeout süresini azaltabilirsiniz.
- SYN Çerezlerini kullanabilirsiniz.

SLOWLORİS SALDIRILARI

Robert 'RSnake' Hansen tarafından oluşturulmuş DDoS saldırımı yazılımıdır. Bu yazılım diğer DDoS attack türlerinden farklı olarak tek bir makinenin ağ kaynaklarını minimum bant genişliği kullanarak hedef makinenin web sunucusunu çökertmeye yönelik yavaşlatma saldırısı yapan bir DDoS Attack türüdür.

ÖNLEMLER

- İp adresi bağlantısını sınırlamak
- Bir istemcinin bağlı kalmasına izin verilen süreyi kısıtlamak