ÖN BİLGİ

Bu belge

- https://www.slideshare.net/bgasecurity/web-ddos

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Web%20Sunucular%C4%B1na%20Y%C3%B6nelik%20DDOS%20Sald%C4%B1r%C4%B1lar%C4%B1.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Bu yazıda Web’in ve HTTP’nin DOS saldırıları karşısındaki durumunu inceleyeceğiz.

(Page 1)

2)

HTTP (Hypertext Transfer Protocol) OSI modelinin uygulama katmanında yer alan iletişim protokolüdür.

(page 1)

3)

Http Nasıl Çalışır?

Bir HTTP isteği yapılacağı zaman önce TCP 3 yollu el sıkışma yapılır ve ondan sonra istek gönderilir. İsteğe karşılık yanıt alındıktan sonra istemci tekrar HTTP isteğinde bulunacaksa tekrar TCP 3 yollu el sıkışma yapılır. Çünkü gönderilen her bir istek birbirinden bağımsızdır. Sonuç olarak her HTTP isteği için bir TCP 3 yollu el sıkışma prosedürü uygulanır.

(Page 1)

4)

Web’in çalışma mantığı istek ve cevaplardan ibarettir.

(Page 2)

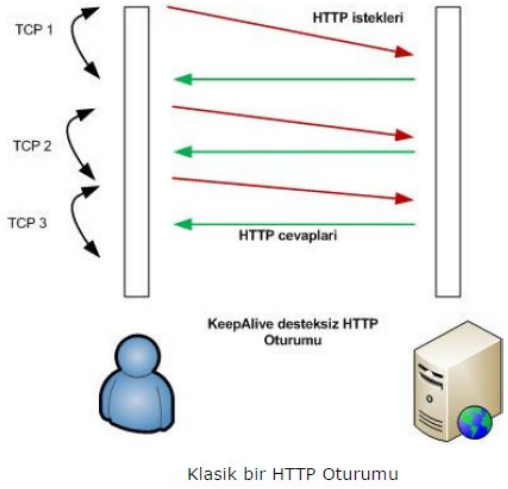
5)

HTTP ve TCP İlişkisi

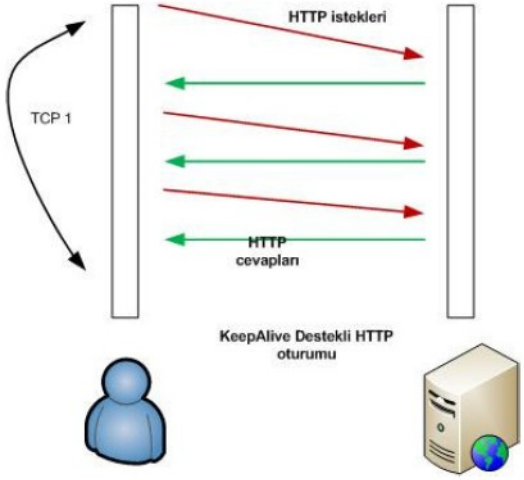
HTTP TCP kullanan bir protokoldür. Günümüzde örneğin bir haber portalının yüklenmesi için ortalama 40-50 HTTP GET isteği gönderilmektedir. E haliyle 50 HTTP GET isteğinin her biri için TCP üç yollu el sıkışma yapıldığından dolayı 50 x 3 = 150 TCP paketinin gidip gelmesi gerekir ki bu değer oldukça fazladır (HATIRLA: TCP 3 yollu el sıkışmada 3 paket kullanılır: SYN, SYN/ACK, ACK).

HTTP’de bu performans sorununu aşabilmek için çeşitli yöntemler geliştirilmiştir. Bunların başında HTTP KeepAlive (persistent connection) özelliği gelmektedir. HTTP Keep Alive özelliği her HTTP isteği için ayrı bir TCP 3 yollu el sıkışma yerine bir adet

TCP 3 yollu el sıkışma kullanır ve bu kurulan bağlantı içerisinden birden fazla HTTP isteğinin aktarılabilmesini sağlar.



KLASİK HTTP OTURUMU



KEEPALIVE DESTEKLİ HTTP OTURUMU

Yukarıdaki KeepAlive destekli HTTP oturumu resminden de görülebileceği gibi bir TCP bağlantısıyla 3 tane HTTP talebi gönderilebilmiş ve yanıtları alınabilmiştir.

(Page 2-4)

6)

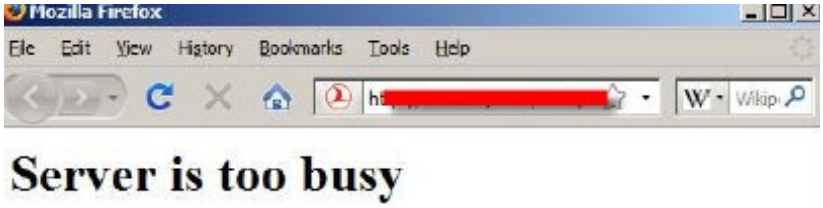
HTTP Pipelining

Pipelining HTTP isteklerinin peşisıra gönderilmesi işlemine verilen addır. Genellikle KeepAlive kavramıyla karıştırılır, fakat bunlar birbirlerinden farklı kavramlardır. Klasik http bağlantılarında önce istek gönderilir ve cevap beklenir. Cevap alındıktan sonra tekrar istek gönderilir ve cevap beklenilir. Pipelining kullanıldığında ise cevapların gelmesi beklenmeksizin birden fazla HTTP isteğinde bulunulur. Bu arada istenirse KeepAlive özelliği kullanılarak her istek için ek bir TCP bağlantısı açılmaz.

(Page 4)

7)

DOS/DDOS'a maruz kalan web sunucularında çalışan web sayfalarında genellikle aşağıdakine benzer bir hata ile karşılaşılır:



Eğer saldırı yoğunluğu yüksekse sayfa hiç gelmeye de bilir.

(Page 4-5)

8)

Web Sunucularına Yönelik DOS Saldırıları

Web sunuculara karşı yapılacak DOS saldırıları temelde iki türdür:

- Kaba Kuvvet Saldırıları (Flood)
- Tasarımsal/yazılımsal eksikliklerden kaynaklanan zafiyetler

Kaba Kuvvet DOS/DDOS Saldırıları

Sunucunun kapasitesinin gönderilen binlerce isteklerle zorlanmasına denir. Literatürde adı GET Flood ya da POST Flood olarak geçen bu saldırılar iki şekilde yapılabilir. Birincisi bir kişi ya da anlaşan birden fazla kişi hedefe yüzlerce, binlerce istek gönderir. Orta ölçekli çoğu şirket bu isteklere uzun süre dayanamazlar. Fakat bu saldırı güvenlik duvarıyla, IPS'lerin Rate Limiting özelliğiyle kolaylıkla bertaraf edilebilir. Kaba Kuvvet DOS saldırılarının ikinci şekline gelecek olursak bu DOS saldırısında zombie bilgisayarlar kullanılır. Böylelikle farklı farklı IP ve subnet'lerden gelen yüzlerce, binlerce istek güvenlik duvarıyla ya da IPS'in Rate Limiting özelliğiyle engellenemeyeceği için hedef sistemi erişime kapatabilir.

Yazılımsal ya da Tasarımsal Eksikliklerden Kaynaklanan DOS/DDOS Saldırıları

Tasarımsal zafiyetler protokol daha en başta tasarlanırken detaylı düşünülmemiş ya da kolaylık olsun diye esnek bırakılmış bazı özelliklerin kötüye kullanılmasıdır. Tasarımsal zafiyetlerden kaynaklanan DOS saldırılarına en iyi örnek geçtiğimiz aylarda yayınlanan Slowloris aracıdır. Bu araçla tek bir sistem Apache kullanan sunucuları rahatlıkla devre dışı bırakabilir. Benzeri şekilde Captcha kullanılmayan

formlarda da ciddi DOS saldırılarına yol açabilir. Mesela form üzerinden alınan bilgiler sunucu tarafındaki bir mail sunucu aracılığıyla belirtilen eposta adresine gönderiliyorsa saldırgan otomatize araçlarla binlerce kez aynı formu submit'leyebilir ve bu talep yoğunluğuna dayanamayan mail sunucu kilitlenebilir.

(Page 5-6)

9)

PHP'nin Apache'nin vs... yazılımsal zafiyetlerine karşı klasik sınır koruma araçları işe yaramaz. Çünkü bu bu zafiyetler koruma araçlarıyla kapatılamayacak kadar karmaşıktır. Dolayısıyla çözüm yazılımları daima güncel tutma ve yapılandırma dosyalarını iyi bilmek, yani gerektiğinde manipule edebilmektir.

(Page 6)

10)

HTTP Dos yapan başlıca yazılımlar şunlardır: Ab, Siege, slowloris, Http_Load, hping3 ve curl.

(Page 7)

11)

DOS ve DDOS Saldırılarından Korunma Yöntemleri

Bu tip saldırılardan korunma konusunda bilinmesi gereken en temel kanun yapılan saldırının şiddeti, yani gelen trafiğin ihtiyaç duyduğu bandwidth sunucununkinden fazla ise hiçbir şeyin yapılamayacağıdır.

Web sunucularına yapılan DOS/DDOS saldırılarından korunmak diğer DOS/DDOS saldırılarına göre oldukça zordur. Yani HTTP DOS/DDOS'dan korunmak diğer DOS/DDOS saldırıları olan Syn Flood, UDP Flood, Smurf'e,... göre daha zordur. Syn Flood, UDP Flood ve Smurf belirli oranda engellenebilir, çünkü bu saldırılar Layer 4'te gerçekleşir. Layer 4'te gerçekleşen saldırılar Router, Firewall ve IPS'lerle belirli oranda engellenebilmektedir.

NOT: Syn Flood, UDP Flood ve Smurf saldırıları Layer 4'te gerçekleşir dendi. Çünkü bunlar adlarından da belli olabileceği gibi sırasıyla TCP, UDP ve ICMP protokollerini kullanmaktadırlar. Fark ettiysen bu protokollerden sorumlu katman Layer 4'tür, yani Transport Layer'dır.

HTTP üzerinden yapılan DDOS saldırıları tıpkı normal kullanıcı kitlesinden geliyormuş gibi göründüğünden ağ güvenlik cihazları bunun bir saldırı mı yoksa saldırgan olmayan bir kitlenin rağbeti mi olduğunu anlayamamaktadırlar. İşte bu yüzden HTTP DOS/DDOS saldırısını önlemek diğer DOS/DDOS saldırılarına göre daha zordur. Yine de web sunucularının önüne koyulacak ağ güvenlik cihazları iyi yapılandırılabilirlerse bu tip saldırılardan büyük oranda korunulabilir. Bunun için şu adımlar izlenebilir:

- İstekleri daha rahat karşılayacak ve gerektiğinde belleğe alarak ana sunucunun yükünü hafifletecek sistemler kullanılmalıdır. Mesela Load Balancer, ReverProxy gibi…
- Firewall/IPS ile belirli bir kaynaktan gelebilecek maksimum istek sayısı sınırlandırılmalıdır (Rate Limiting ile bu yapılabilir)
- Saldırı anında log'lar incelenerek saldırıya has bir veri deseni belirlenebilirse (User Agent, refererer gibi) IPS üzerinden özel imzalar yazılarak bu veri desenine sahip paketler engellenebilir. Fakat bunun normal kullanıcıları etkilemeyeceğinden emin olunması gerekir.
- Web sunucu yazılımının desteklediği DOS koruma modülleri kullanılabilir. Mesela Apache'nin Mod_DOSEvasive'si gibi…

NOT: Apache'nin modülü gibi modüller kullanıldığında DOS yaptığı kanısına varılan kullanıcılara HTTP 403 cevabı döndürtmek yerine IPTables'tan bloklama şeklinde modülü yapılandırmak sunucuyu gereksiz bir yükten kurtaracaktır.

(Page 7)

12)

Siber dünyada gün geçtikçe Web'in önemi artaracak ve HTPP'ye yönelik DOS/DDOS saldırıları ciddi artışlar gösterecektir. DOS/DDOS saldırılarını engellemeye yönelik atılacak en sağlıklı adım kullanılan sistemleri iyi bilmek ve DOS/DDOS saldırısına maruz kalmadan sistemlerinizi test ettirmektir. Bu konuda hazır çözüm sunan ticari ürünlerin onu yapılandıran kadar işlevsel olacağı da unutulmamalıdır.

(page 8)