SynFlood DDOS Saldırıları

SynFlood saldırıları ve korunma yolları

Huzeyfe ÖNAL
huzeyfe@lifeoverip.net
http://www.lifeoverip.net

1/16/2010

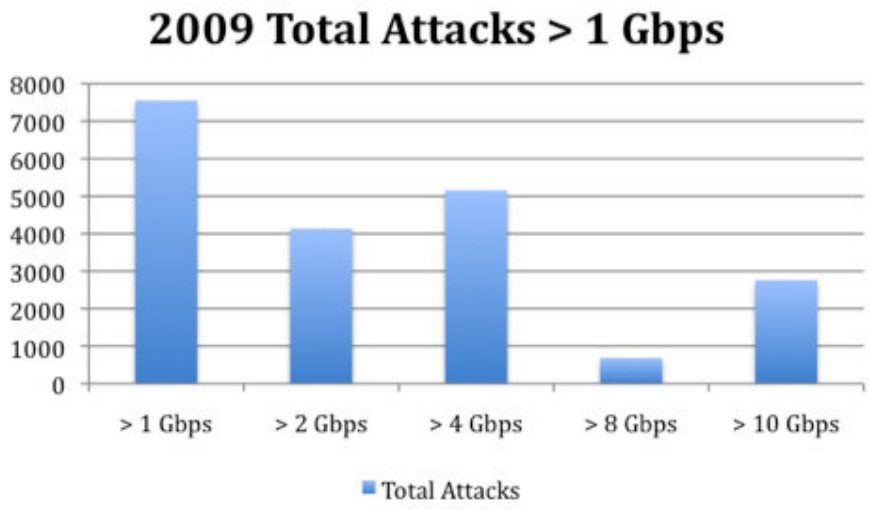
[Bu yazı internet ortamında sık karşılaşılan ve genelde çözümsüz kalan DDOS saldırı tiplerinden SYNFlood saldırıları ve bu saldırıların detayını teknik analiz etme amaçlı yazılmıştır.]

İçerik

Giriş

DDOS saldırıları günümüz ve gelecek internet dünyasının en temel problemlerinden biridir. İnternete bağlı bilgisayar sayısı arttıkça bu tehdit de katlanarak artmaya devam edecektir. Günümüz şirketleri henüz bu konuda önlemler almaya başlamamıştır, önlem alanlar da mutlaka bir iki DDOS saldırısına maruz kalıp maddi/manevi zarara uğradıktan sonra harekete geçmişlerdir. Oysa DDOS konusu tam da sık konuşulan ve önem verilen "iş sürekliliği" projelerinde ilk alınması gereken önlemlerden biridir.

Aşağıdaki grafik Arbor Networks'un çeşitli Telekom firmalarından aldığı verilerden oluşturduğu 2009 yılı DDOS istatistikleri raporundan alınmıştır. Kaynaklar kısmından detayına ulaşılacak bu rapora göre 2009 yılında her 26 dakikada bir 1Gbps üzerinde DDOS saldırısı yaşanmıştır ki bu saldırıların %99'unun başarılı olduğunu tahmin edebiliriz.



DDOS saldırı çeşitleri arasında en kolay gerçekleştirileni SynFlood saldırılarıdır. Bu yazıda SYNFlood saldırılarının nasıl gerçekleştirildiği, neden bu kadar etkili olabildiği ve çözüm yolları teknik detay verilerek anlatılacaktır. Konuyla ilgili daha fazla bilgi edinmek, DDOS saldırılarını uygulamalı olarak görmek ve alınabilecek önlemleri denemek için www.guvenlikegitimleri.com adresindeki DDOS Saldırıları ve Korunmya Yolları eğitimi incelenebilir

Yazıya başlamadan DDOS saldırılarıyla ilgili olarak bilinmesi gereken iki temel hususu hatırlatalım:

DDOS saldırıları eğer sizin sahip olduğunuz bandwithden fazla değilse teorik olarak engellenebilir, gelen saldırı sizin sahip olduğunuz trafik miktarından fazlaysa bunu ancak ve ancak hizmet aldığınız telekom firması engelleyebilir.

DDOS saldırılarının engellemesi teknik ve teorik olarak mümkündür aynı zamanda engellenemez DDOS saldırısı gerçekleştirmek de teknik ve teorik olarak mümkündür. Bu konuda bilgili ve tecübeli bir saldırgan amacına ulaşmada kararlıysa bir şekilde alınacak tüm engelleri aşacaktır. Burada biz güvenlik uzmanlarının yapacağı riski tamamen ortadan kaldırmak değil olabildiğince azaltmak için çeşitli önlemler almaktır.

SynFlood DDOS Saldırıları

Nedir?

Syn Flood servis engelleme saldırılarından(DOS) en bilineni ve sık karşılaşılanıdır. Amaç: hedef sisteme kapasitesinden fazla SYN bayraklı TCP paket gönderip sistem kaynaklarını hizmet veremez hale getirmektir. Günümüzde genellikle WEB sunuculara yönelik yapılmakta ve sonuç olarak web sayfalarının çalışamaz hale gelmektedir.

Syn Flood saldırıları ilk olarak 1994 yılında teorik olarak "*Firewalls And Internet Security*" kitabında bahsi geçmiş ve 1996 yılında Phrack dergisinde exploit aracının çıkmasıyla yaygınlaşmaya başlamıştır.

Syn flood saldırılarını anlayabilmek ve gerekli önlemleri alabilmek için TCP/IP ailesinin en sık kullanılan bileşeni TCP(RFC 793)'nin yapısı ve çalışma mantığının iyi bilinmesi şarttır. SynFlood saldırısını gerçekleştirenin bilmesi gereken ise sadece hedef ip hedef port ve kullanacağı ddos programının ismidir.

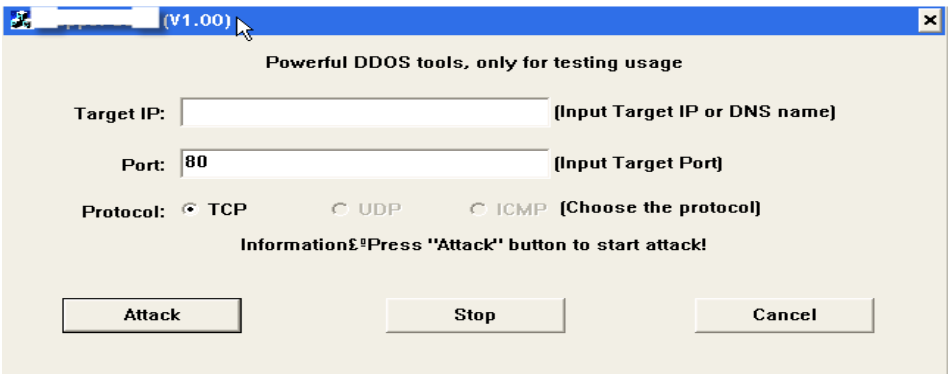
Neden Kaynaklanır?

SynFlood saldırısının temel sebebi bağlanan istemcilerin herhangi bir doğrulama(bağlantı yapanın gerçekten ilgili ipadresine sahip olduğu bilgisi) mekanizmasından geçmemesidir. Bu aslında Ipv4 'e ait bir eksiklik olmakla birlikte Ipv6'a geçiş yapıldığında kısmen ortadan kalkacaktır.

Kim Yapar?

Internette arama yapabilen her bilgisayar kullanıcı bu saldırı tipini gerçekleştirebilir. Hem Windows hem de Linux/UNIX sistemler icin onlarca ddos aracı bulunmaktadır.

Saldırının etkili olabilmesi için sahip olunması gereken trafik miktarı belli bir değerin üzerinde olmalıdır(>50Mbps gibi) . Saldırıyı kimin yaptığını bulmak teoride mümkün gibi gözükse de günümüz internet dünyasının yapısı düşünüldüğünde spoof edilmiş ip adresleri üzerinden yapılan SynFlood saldırısının gerçek kaynağını bulmak imkansızdır.



Temel TCP bilgisi

OSI katmanına göre 4. Katta yer alan TCP günümüz internet dünyasında en sık kullanılan protokoldür. Aynı katta yer alan komşu protokol UDP'e göre oldukça karışık bir yapıya sahiptir.

Http,smtp, pop3, https gibi protokoller altyapı olarak TCP kullanırlar.

TCP bağlantılarında bayraklar

TCP bağlantıları bayraklarla(flags) yürütülür. Bayraklar TCP bağlantılarında durum belirleme konumuna sahiptir. Yani bağlantının başlaması, veri transferi, onay mekanizması ve bağlantının sonlandırılması işlemleri tamamen bayraklar aracılığı ile gerçekleşir.(SYN, ACK, FIN, PUSH, RST, URG bayrak çeşitleridir)

UDP'de ise böyle bir mekanizma yoktur. UDP'de güvenilirliliğin(paketlerin onay mekanizmasi) sağlanması üst katmanlarda çalışan uygulamalar yazılarak halledilebilir. DNS protokolü UDP aracılığı ile nasıl güvenilir iletişim kurulacağı konusunda detay bilgi verecektir.

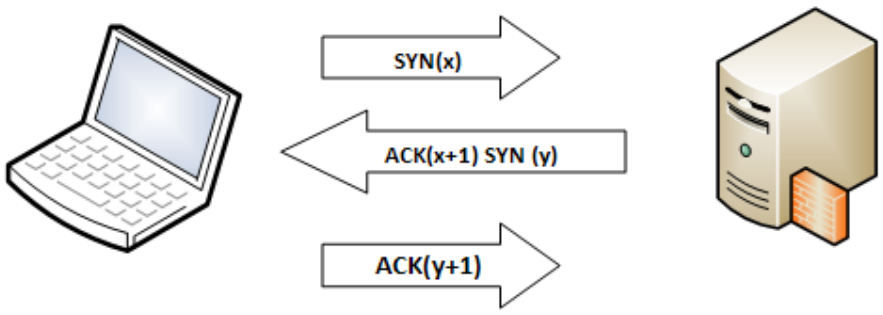
UNIX/Windows sistemlerde bağlantılara ait en detaylı bilgi netstat (Network statistics) komutu ile elde edilir. Netstat kullanarak TCP, UDP hatta UNIX domain socketlere ait tüm bilgileri edinebiliriz.

TCP'de bağlantıya ait oldukça fazla durum vardır. TCP bağlantılarında netstat aracılığı ile görülebilecek çeşitli durumlar:

CLOSE_WAIT, CLOSED, ESTABLISHED, FIN_WAIT_1, FIN_WAIT_2, LAST_ACK, LISTEN, SYN_RECEIVED, SYN_SEND ve TIME_WAIT

TCP Oturum başlatma

Web sayfalarını gezmek için kullanılan http üzerinden örnek vermek gerekirse bir web sayfasına ulaşıp içeriğini görebilmemiz için öncelikle TCP oturumunun kurulması(3 lü el sıkışma) gerekir. Bu adım tamamlandıktan sonra web sayfasının içeriğini görüntüleyecek komutlar sisteme gönderilir.



Hizmet veren bir TCP portu açıksa kendisine gelen SYN paketine karşılık olarak ACK+SYN paketi döner. Dönen paketlerden ACK(onay paketi), SYN ise hizmet veren tarafın istek başlatma paketidir.

Port kapalıysa RST döner, SYNflood saldırısının başarılı olabilmesi için portun açık ve dinlemede (LISTEN mod)olması gerekir.

Oturum başlangıcında portun alabileceği durumlar

SYN_SEND : Hedef sistemle TCP bağlantısı oluşturma adımının ilkidir. Kısaca SYN bayraklı paket gönderilip buna karşılık cevap bekleme zamanında portun alacağı durum.

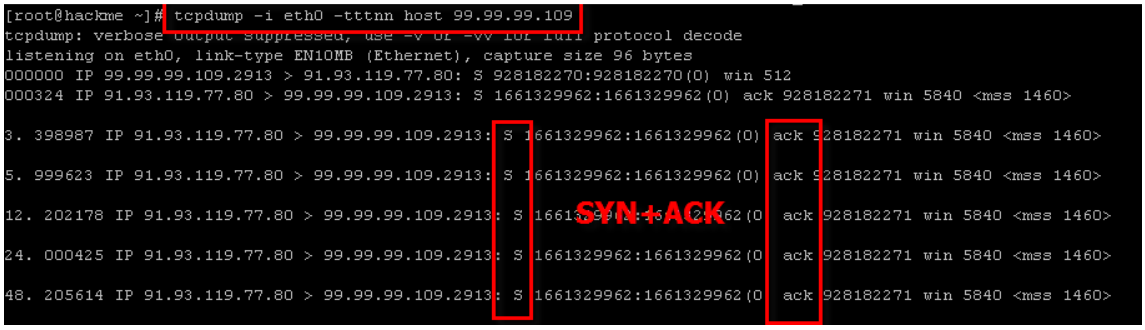
SYN_RECEIVED: Hedef sistem portu bağlantı kurulması için gerekli ilk adım olan SYN paketini almıştır ve cevap olarak SYN+ACK dönmüştür, karşı taraftan son ACK paketi gelene kadar bu pozisyonda bekler.

ESTABLISHED: son ACK paketi de gelmiş ve 3 lü el sıkışma tamamlanmış artık taraflar veri transferi yapabilir durumdadır.

LISTEN: O portun bağlantı kabul eder olduğunu belirtir.

Gelen bir SYN paketine kaç kere SYN+ACK döner ve dönen her cevap kaç byte'dir?

Ortalama bir TCP başlığı 60 Byte, buna dönen SYN+ACK cevabı da 60 Byte civarı olacaktır ve yapılandırılışına göre SYN paketini alan sistem son ACK paketini alana kadar 5-6 kere SYN+ACK paketini tekrar gönderir ki bu da ortalama 3 dakika tutar.



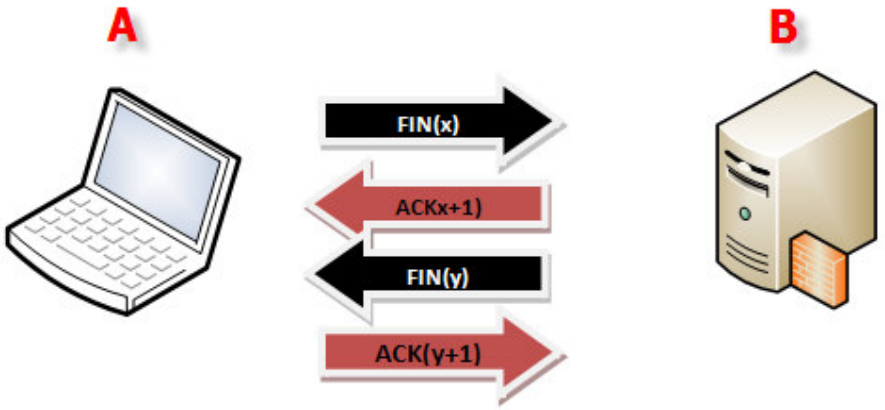
LISTEN durumunda olan bir TCP portuna SYN paketi geldiğinde SYN_RECEIVED durumuna geçer ve son ACK paketi gelene kadar verileri bir veriyapısında tutar. Bu veriyapısı TCB(Transmission Control Block) olarak adlandırılır. İşletim sistemlerine göre TCB değeri değişkenlik gösterse de ortalama olarak sistemden 280-1300 byte arası bellek kullanır (Üçlü el sıkışma tamamlanana kadar bir SYN paketininin sistemden kullandığı bellek miktarı)

İşletim sistemleri gelecek fazla isteklerden kaynaklanacak bellek yetmezliğini önleme amaçlı TCB'lerin tutacağı max bellek miktarını sınırlandırırlar.

TCP oturum sonlandırma

Oturum sonlandırma her iki tarafında anlaşması sonucu tamamlanır. Taraflardan birinin ilgili bayraklı paketi göndermemesi, geç göndermesi bağlantının sağlıklı olarak sonlanmasına engel olur.

Bağlantı sonlandırma aşamalarında çeşitli durumlar oluşur. Bu durumlara geçmeden bir TCP bağlantısının nasıl kapatıldığını inceleyelim.



görüleceği üzere A ve B sistemleri arasındaki bağlantıyı kapatmak için 4 paket transferi oluyor. Bu paketleri Wireshark ya da tcpdump ile rahatlıkla görebilirsiniz.

tcpdump çıktısı

2007-08-13 21:38:57.239126 IP 80.93.212.86.3306 > 88.233.216.57.2175: **F 75:75(0)** ack 1 win 65535
2007-08-13 21:38:57.292806 IP 88.233.216.57.2175 > 80.93.212.86.3306: **. ack 76** win 17446
2007-08-13 21:38:57.295927 IP 88.233.216.57.2175 > 80.93.212.86.3306: **F 1:1(0)** ack 76 win 17446
2007-08-13 21:38:57.295941 IP 80.93.212.86.3306 > 88.233.216.57.2175: **. ack 2** win 65534

Bağlantı sonlanması esnasında oluşan durumlar:

FIN_WAIT_1:

Bağlantı sonlandırmak için işlem başlatan taraf(A) hedef sisteme FIN bayraklı TCP paketi gönderir. Ardından karşı taraftan(B) ayrı ayrı ACK ve FIN bayraklı paketleri bekler . Bu arada durumunu FIN_WAIT_1 olarak ayarlar.

FIN_WAIT_2:

Bağlantı sonlandırma isteğini(FIN bayraklı ilk paket) alan taraf(B) bu pakete karşılık olarak ACK(onay) bayraklı TCP paketi hazırlar ve gönderir ve durumunu CLOSE_WAIT'e alır. Ilk FIN bayraklı paketi gönderen taraf(A) ACK paketini aldığında durumunu FIN_WAIT_2 olarak ayarlar.

Böylece bağlantı sonlandırma işleminin ilk yarısı tamamlanmıştır. Diğer yarısıda sağlıklı tamamlandıktan sonra bağlantı tamamen sonlanmış olacaktır.

LAST_ACK:

B tarafı ACK bayraklı paket gönderdikten sonra , kendisinin de bağlantıyı sonlandırmak istediğini bildiren FIN bayraklı paket oluşturarak A sistemine gönderir ve durumunu LAST_ACK olarak ayarlar.

TIME_WAIT

: A sistemi FIN bayraklı paketi aldıktan sonra buna cevaben ACK bayraklı bir paket oluşturarak B'ye gönderir ve durumunu TIME_WAIT olarak belirler.

A sistemi TIME_WAIT durumunda son gönderilen ACK bayraklı paketin hedef sisteme(B) ulaştığını garantilemek için bir müddet bekler. Bu müddet eğer gereğinden fazla(eski tip UNIX sistemlerde 4 dakikaya kadar çıkabiliyor.) ise sisteminizde netstat -an çalıştırdığınızda oldukca fazla TIME_WAIT satırı görebilirsiniz.

Bu da sistemi gereğinden fazla meşgul edeceği için performans problemleri yaşanması kaçınılmaz olacaktır.

Örnek bir sistem üzerinde inceleme:

TCP/80 portuna yapılan bir istek ve isteğin sonlanması sırasında netstat ile alınan durum çıktıları. Sadece sunucu tarafını gösterdiği için bazı durumlar gözükmemektedir. İsteği yapan taraf da incelenecek olursa eksik kalan kısımlar tamamlanır.

tcp4 0 0 80.93.212.86.80 88.233.216.57.2348 SYN_RECEIVED

tcp4 0 0 80.93.212.86.80 88.233.216.57.2348 ESTABLISHED

tcp4 0 0 80.93.212.86.80 88.233.216.57.2348 FIN_WAIT_2

tcp4 0 0 80.93.212.86.80 88.233.216.57.2348 TIME_WAIT

SynFlood Nasıl Gerçekleşir?

Syn Flood saldırısı basitce açık bir porta hedef sistemin kapasitesinden fazla gönderilecek SYN paketleriyle gerçekleştirilir. Buradaki “kapasite” tanımı önemlidir. Teknik olarak bu kapasiteye Backlog Queue denilmektedir.

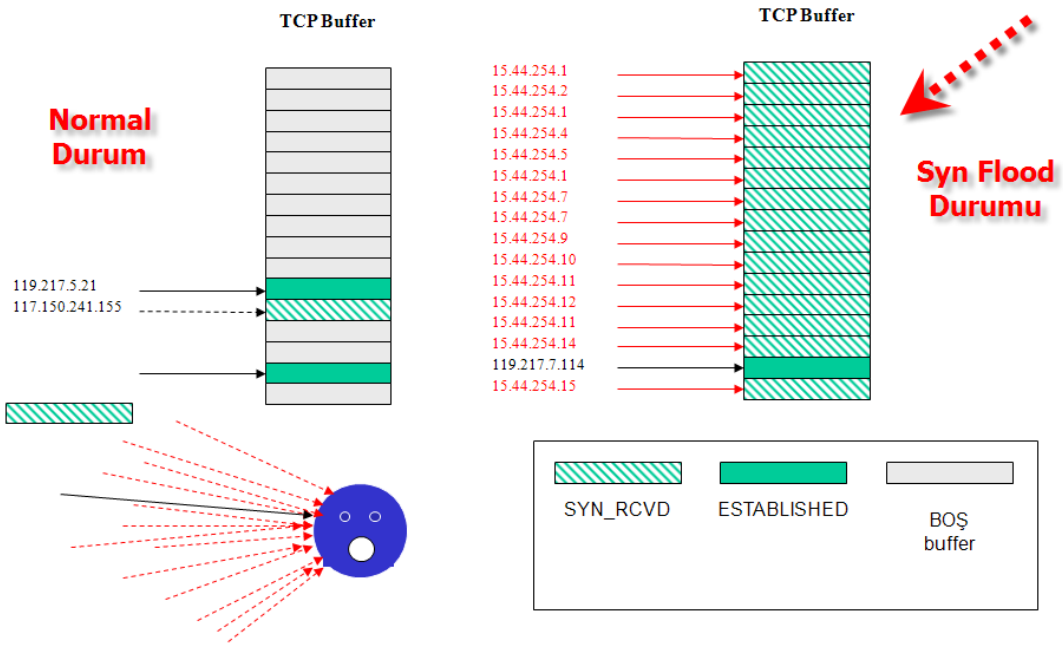
Backlog queue kavramı

İşletim sistemleri aldığı her SYN paketine karşılık üçlü el sıkışmanın tamamlanacağı ana kadar bellekten bir alan kullanırlar, bu alan TCB olarak adlandırılır ve bu alanların toplamı backlog queue olarak adlandırılır.

Başka bir ifadeyle işletim sisteminin half-open olarak ne kadar bağlantı tutabileceğini backlog queue veriyapısı belirler. Bu değer her işletim sisteminde vardır ve ön tanımlı olarak düşük bir değerdir(256 gibi). SYNFlood saldırılarında bu değer arttırılarak saldırıya karşı ek önlem alınabilir.

Synflood saldırılarında tüm mesele backlog queue’nin dolması ve yeni gelen bağlantıların reddedilmesidir. Backlog queue değerinin büyük olması demek daha fazla half-open(SYN paketi) bağlantı kabul edebilmek demektir.

Backlog queue dolmasıyla birlikte işletim sistemi yeni bağlantı kabul edemez ve bu esnada sunucuya bağlanmaya çalışanlar bağlanamazlar ki bu da SYN Flood saldırısına denk gelir.



Synflood matematik hesabı

Günümüzde yeterli önlem alınmamış sistemlerin Synflood'a karşı ne kadar dayanıksız olduğunu göstermek için basit bir matematik hesabı yapalım:

Backlog queue değeri 1000 olan sisteme 1000 adet SYN paketi göndererek servis veremez duruma getirilebilir.

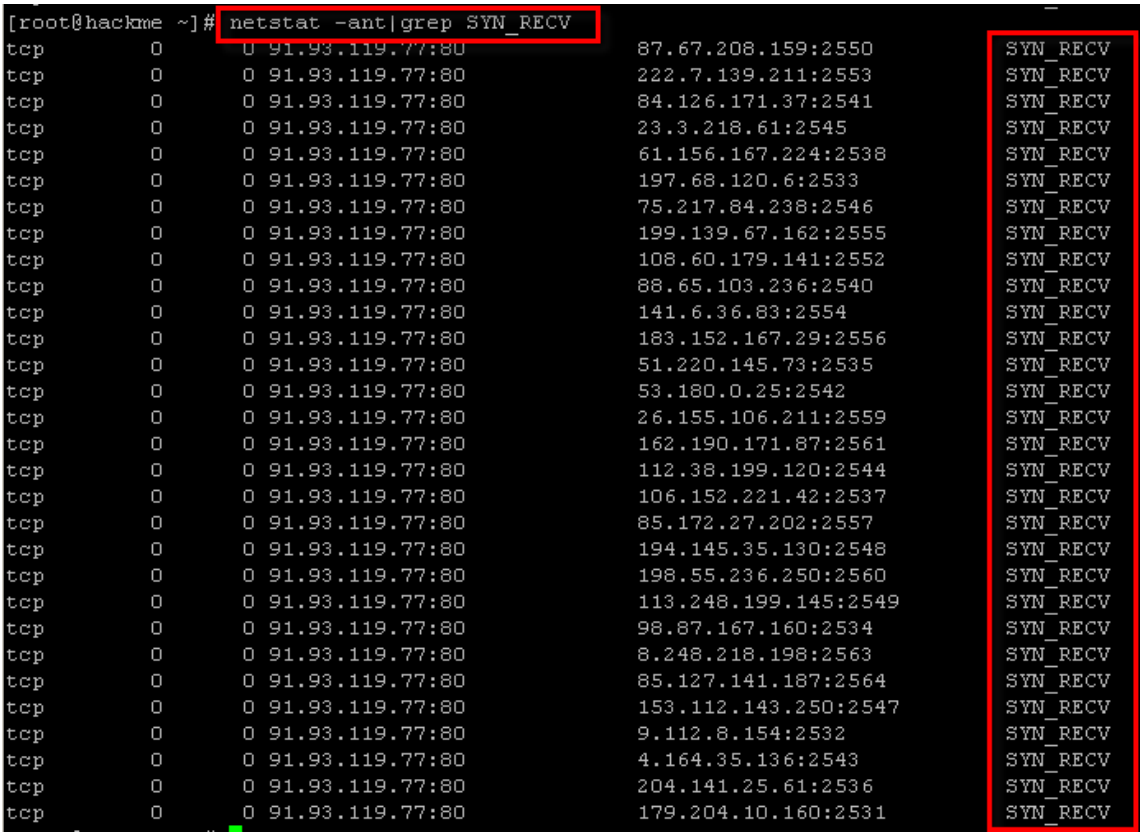
1000 adet SYN paketi=1000*60byte=60.000 byte=468Kpbs olacaktır ki bu değer günümüzde çoğu ADSL kullanıcısının sahip olduğu hat kapasitesine yakındır.

Servis verememe durumu ilgili porta gelen paketlerin timeout değeriyle doğru orantılıdır. Her 60 saniye de bir bu kadar paket gönderilmesi durumunda sistem tamamen erişilmez olabilir.

Not: Bir porta SYN paketi geldiğinde cevap olarak ACK +SYN döneceği için iki kat malzeme harcanır. Bu durum özellikle güvenlik cihazlarındaki PPS(Saniyede işleyebileceği paket sayısı) değerlerini ölçerken göz ardı edilir. Bir cihaz 100.000 pps diyorsa aslında bu saniyede 50.000 SYN paketi kabul edebilir demektir.

SynFlood DDOS saldırısını nasıl anlarız?

UNIX/Linux ve Windows işletim sistemlerinde netstat komutuna uygun parametre vererek SYN Flood saldırıları anlaşılabilir. Güvenlik cihazlarında ise state(durum) tablosuna bakarak ya da connection tablosuna bakarak Syn Flood saldırıları anlaşılabilir.



Ya da basit olarak aşağıdaki komutu çalıştırılır

 # netstat -ant|grep SYN_RECV|grep ":80"|wc -l

1002

Bu komutun çıktısı belli bir değerin üzerindeyse sisteme SYNFlood saldırısı yapılıyor olabilir. (Yukardaki komut sadece 80. Porta gelen syn paketlerini saydırmak için kullanılır, tüm sisteme gelen syn paketlerini görmek için grep “:80” kolonu kaldırılabilir.

Ek olarak Linux altında SYNFlood’a uğrayan bir sistem messages dosyasına aşağıdaki gibi bir log atar.

possible SYN flooding on port 80. Sending cookies.

SynFlood Saldırı Testleri

Syn Flood saldırıları sizi bulmadan önce kendi sistemlerinizi bu tip saldırılara karşı yapılandırmanız ve test yapmanız bir saldırı karşısında hangi durumlara düşebileceğiniz konusunda fikir verecektir. Aşağıda bazı araç isimleri ve kullanımları verilmiştir, bunlar tamamen kendi sistemlerinizi test etme amaçlı kullanılmalıdır.

İnternet üzerinde bu tip atakları yapanlar daha basit ve etkili araçlar kullanmaktadır. (bkz: botnet yönetim konsolları)

Scapy ile basit Synflood aracı

Scapy, istenilen türde TCP/IP paketleri üretmeye ve bu paketler üzerinde çeşitli işlemler yapmaya izin veren bir çatıdır. Python ile yazıldığından Python destekleyen sistemlerde(Tüm işletim sistemleri) çalışmaktadır.

Scapy kullanarak aşağıdaki gibi istenilen aralıkta spoofed ip üreten SYNFlood saldırısı denenebilir.

```
>>> send(IP(src=RandIP('78.0.0.0/16'), dst='www.example.com')/TCP(sport=RandShort(),
    dport=80), loop=1)
```

Hping ile SYNflood testleri

Hping TCP/IP paket üretim aracıdır. Hping'in –flood ve rand-source özellikleri kullanılarak yüksek miktarlarda SYN Flood saldırıları simulasyonu yapılabilir.

Hping ile spoof edilmiş ip adreslerinden Syn Flood saldırısı

#hping --rand-source -p 80 -S www.hedefsistem1.com --flood

Benzeri araçlar kullanarak sahip olduğunuz trafik miktarına göre oldukça yüksek sayılarda SYN paketi üretip gönderebilirsiniz. SYN paketinin 60 byte civarında olduğunu düşünürsek 50Mb hat ile saniyede 100.000 SYN paketi üretip gönderilebilir ki bu değer birçok güvenlik duvarının sahip olduğu bağlantı limiti sayısını kısa sürede aşırır.(günümüz güvenlik duvarlarında en yüksek bağlantı limitleri 400-500k civarındadır). Bağlantı limit sayısı 500.000 olan(eş zamanlı 500.000 bağlantı tutabilen) bir sistemi 50Mb hat ile 5 saniyede işlevsiz bırakılabilir.

Not: Burada güvenlik duvarları üzerinde syncookie, synproxy gibi özelliklerin aktif olmadığını düşünüyoruz.

SynFlood saldırılarında kaynak ip adresleri eğer internette açık olan ip adreslerinden seçilirse etkisi düşük olur. Zira açık olan bir ip adresini spoof ederek gönderilecek SYN paketine sunucu SYN+ACK cevabı dönecektir ve bu cevap spoof edilen makineye gelecektir, makine de daha önce böyle bir paket göndermediği için RST paketi gönderip bağlantının hızlıca kapanmasını sağlayacaktır.

SYNFlood saldırısı esnasında yapılacaklar

ilk olarak gelen giden tüm paketleri görebilecek bir sistem üzerinde(Port mirroring, TAP cihazı vs yi dinleyen Linux/UNIX makine)n saldırıyı analiz etmek için paket kaydı yapılmalıdır. Bunun için tcpdump kullanılabilir.

#tcpdump -ttttnn -s0 tcp -w SYNFLOOD.pcap &

Tcpdump ile sadece SYN bayraklı TCP paketlerini görmek için verilecek komut:

tcpdump 'tcp[13] & 2 != 0' -i eth0 -nnn

Saldırı esnasında paketleri incelemek bazı basit saldırılarda faydalı olabilmektedir. Mesela Synflood için çok sık tercih edilen Juno aracı öntanımlı olarak kaynak port numarasını 1024/3072 yapmaktadır. Eğer saldırgan Juno.c'nin kaynak kodunu inceleyip kaynak port numaralarını random hale getirmemişse bu saldırı router üzerinden yazılacak basit bir ACL(erişim listesi) ile engellenebilir.

Sistemleriniz güvenlik duvarı, IPS vs ile korunuyorsa bu sistemlerindeki Syncookie, Synproxy özellikleri aktif edilmeli. (Eğer saldırının boyutu yüksekse bu tip engellemelerin kısa sürede devre dışı kalacağı da bilinmelidir) .

Bu gibi durumlarda alternatif yöntemler denenerek sistemlerin ulaşılabilir olması sağlanabilir. Dns kayıtlarının TTL değerlerinin düşürülerek farklı ip adresine geçilmesi gibi.

Ülkeye göre IP bloklama

SynFlood esnasında syncookie vs işe yaramadıysa portu dünyaya kapatıp sadece Türkiye IP bloklarına açabiliriz, eğer SYNFLood yapan tamamen random ip üretiyorsa bu tip bir önlem saldırıyı %70-%90 oranında etkisiz hale getirecektir.

Peki spoof edilmiş ip adresleri arasında Türkiye ip adresleri de olursa? Bunlar için de çözüm doğrudan Türkiye ip aralığından paket kabul etmek yerine bu ip aralığından gelecek istekleri SYNProxy'e devredip bu ip aralığından gelebilecek muhtemel saldırı paketlerini de elemiş oluruz.

Sık kullanılan SYNflood araçları kaynak ip adresini isteğe göre oluşturma özelliğine sahip değildir, genelde kaynak ip adresi random üretilir. Fakat bu yöntem bu konuda tecrübeli saldırganlar için

sadece bir engeldir, ilgili programın kaynak kodunda yapılacak basit değişikliklerle isteğe göre kaynak ip adresi üretilebilir.

78.*.*.* bloğundan random ip üret gibi.

Türkiye IP blokları nereden edinebiliriz?

İnternet üzerinde ülkerelere ait ip bloklarını ücretsiz dağıtan çeşitli servisler vardır. Google üzerinden yapılacak "country ip blocks" araması yeterli sonuç verecektir. Buradan alınacak ip blokları ciddi saldırılar esnasında işe yarayacaktır.

Synflood saldırılarına karşı geliştirilen önlemler

SynFlood saldırılarına karşı çeşitli önlemler geliştirilmiştir. Bunlar arasında günümüzde teoriden pratiğe geçiş yapabilmiş üç temel yöntem bulunmaktadır.

- Syncookie
- syncache(FreeBSD default)
- SynProxy

Syncookie Nasıl çalışır?

Normal TCP bağlantılarında gelen SYN bayraklı pakete karşılık ACK paketi ve SYN paketi gönderilir. Gönderilen ikinci(sunucunun gönderdiği) SYN paketinde ISN değeri random olarak atanır ve son gelecek ACK paketindeki sıra numarasının bizim gönderdiğimizden bir fazla olması beklenir, son paket gelene kadar da sistemden bu bağlantı için bir kaynak ayrılır(backlog queue). Eğer bizim gönderdiğimiz SYN paketine dönen ACK cevabı bizim ISN+1 değilse paket kabul edilmez.

Syncookie aktif edilmiş bir sistemde gelen SYN paketi için sistemden bir kaynak ayrılmaz, bunun aksine SYN paketine dönecek cevaptaki ISN numarası özel olarak hesaplanır (kaynak.ip+kaynak.port+.hedef.ip+hedef.port+x değeri) ve hedefe gönderilir, hedef son paket olan ACK'i gönderdiğinde ISN hesaplama işlemi tekrarlanır ve eğer ISN numarası uygunsa bağlantı kurulur, değilse bağlantı kurulmaz. Böylece spoof edilmiş binlerce ip adresinden gelen SYN paketleri için sistemde bellek tüketilmemiş olacaktır ki bu da sistemin SYNflood saldırıları esnasında daha dayanıklı olmasını sağlar.

Syncookie mekanizması backlogqueue kullanmadığı için sistem kaynaklarını daha az tüketir. Syncookie aktif iken hazırlanan özel ISN numarası cookie olarak adlandırılır.

İstemci tarafı syncookie özelliği İnverse syn cookie (Scanrand aracı) araçları kullanılarak syncookie engellemesi aşılabilir. Bu durumda da bir ip adresinden gelecek max bağlantı sayısı limitlenerek saldırı engellenmiş olur.

Syn cookie dezavantajları

Syncookie'de özel hazırlanacak ISN'ler için üretilen random değerler sistemde matematiksel işlem gücü gerektirdiği için CPU harcar, ve eğer saldırının boyutu yüksekse CPU performans problemlerinden dolayı sistem yine darboğaz yaşar. DDOS Engelleme ürünleri(bazı IPS'ler de) bu darboğazı aşmak için sistemde Syncookie özelliğini farklı özel bir CPU'ya devredeler. Böylece Syncookie işlemleri için farklı, sistemin işleyişi için farklı CPU'lar kullanılır.

Syncookie özelliği sadece belirli bir sistem için açılamaz. Ya açıktır ya kapalı, bu özellik çeşitli IPS sistemlerinde probleme sebep olabilir.

Syncookie uygulamalarından bazıları TCP seçeneklerini tutmadığı için bazı bağlantılarda sorun yaşatabilir.

SynCache nasıl çalışır?

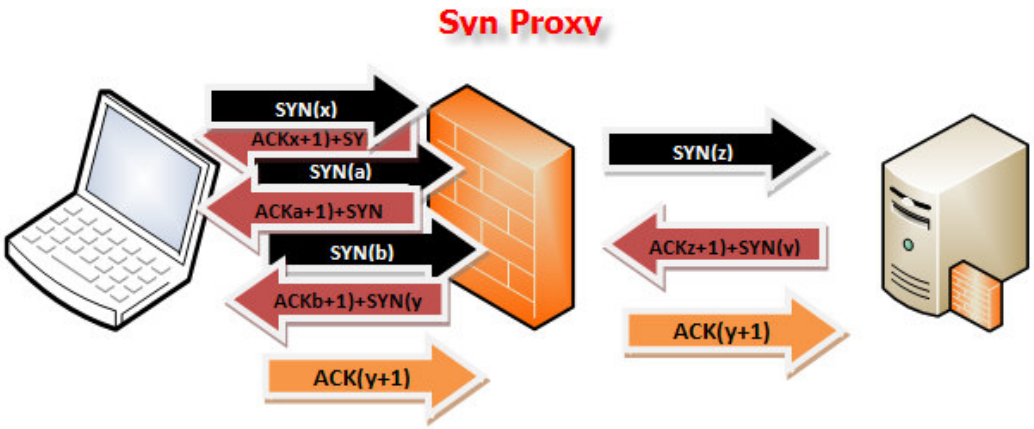
LISTEN modundanki bir portun gelen SYN paketlerinde bellekten bir alan ayırdığını ve bu alanın belirli boyutlarda olduğundan bahsetmiştik. SynCache özelliği FreeBSD sistemlerde gelen SYN paketleri için TCB değerinden daha az yer kaplayan başka bir veri yapısı kullanmayı önerir. Böylece sisteme gelen SYN paketlerinde faha az bellek alanı harcanır(Normalde 700 Byte civarı, 160 Byte Syncache kullanıldığında). Fakat yoğun bir saldırı da bu özellik kısa sürede işe yaramaz hale gelecektir.

Bu sebepledir ki Syncache tek başına synflood saldırılarına karşı efektif bir koruma sağlamaz. Syncookie'i tetikleyici olarak kullanılır. Yani sistemde ön tanımlı olarak syncookie aktif edilmez, syncache aktif edilir. Syncache belli bir değerin üzerinde SYN paketi almaya başladığında SYNCookie'ei tetikler ve sistem koruma moduna geçer.

Syn Proxy nasıl çalışır?

SynProxy, adından da anlaşılacağı üzere SYN paketlerine karşı proxylik yapmaya yarayan bir özelliktir. Güvenlik duvarlarında ve Syncookie'nin kullanımının sıkıntılı olduğu durumlarda rahatlıkla kullanılabilir.

Syncookie gibi arkasında korumaya aldığı sistemlere gelecek tüm SYN paketlerini karşılar ve üçlü el sıkışma tamamlandıktan sonra paketleri koruduğu sistemlere yönlendirir.



Synproxy yapan sistem kendisi de SYNFlood'a dayanıklı olmalıdır.

Ağınızdan SYN Flood yapılmasını Engelleme

SYNFlood saldırıları genelde iki şekilde yapılır:

-BotNet kullanarak gerçek makinelerden

-Bw'i yüksek sistemler üzerinde spoof edilmiş ip adreslerinden

Günümüz SynFlood saldırıları genellikle spoof edilmiş ip adresleri kullanılır. Diğer türlü saldırı çok efektif olmayacaktır.

Eğer firmalar, özellikle de telekom firmaları Spoof edilmiş ip adreslerinden trafik çıkışına izin vermeyecek yapılar kursa ip adres spoofing işlemi yapılamayacağı için Syn flood saldırıları büyük oranda engellenebilecektir. Günümüz internet dünyasında şirketler spoofed ipleri engellese de internetin çoğunluğunu oluşturan masaüstü kullanıcılarına hizmet veren Telekom firmaları bu özelliği kullanmamaktadı(Ya da kullanamamaktadır)

Kullandığınız network/güvenlik sistemlerinde URFP (Unicast Reverse Path Forwarding) özelliği varsa kullanarak ağınızdan dışarı çıkacak spoof edilmiş paketleri engelleyebilirsiniz.

OpenBSD PF ile URPF kullanımı?

URPF kullanilarak eger paket uygun arabirimden gelmiyorsa paketin spoofed olduguna karar verilir ve PF ile bu tip paketler yasaklanir. Anlasilir olmasi icin bir ornekleyelim.

Guvenlik duvarimizda iki ag arabirimi olsun. Biri ic aga bakan(fxp0) ve ip adresi 192.168.0.1, digeri de dis aga (Modem/router vs) baksin(xl0) ve ip adresi 172.16.10.2

```
#netstat -rn -f inet
Routing tables

Internet:
```

Destination Gateway Flags Refs Use Mtu Interface

default 172.16.10.1 UGS 2 20010970 – xl0
192.168.0/24 link#2 UC 1 0 – fxp0
172.16.10/24 link#1 UC 2 0 – xl0

Normal durumlarda fxp0 arabirimine sadece 192.168.0/24 networkune ait ip adresli makinelerden paket gelmesi gerekir. Bunun harici ip adreslerinden paket geliyorsa ya ağın içerisinde başka alt ağlar kurulmuş ya da birileri ip adreslerini spoof etmeye çalışyor demektir.

OpenBSD PF'e urpf kurali girerek istenen ağ arabirimi uzerinde geriye doğru yönlendirme yapılamayacak ip adreslerinden gelen isteklerin bloklanması sağlanabilir.

urpf icin OpenBSD PF kurali.

block in quick on $int_if from urpf-failed

Not-I: urfp kullanirken dikkatli olmak lazim, zira gunumuz aglari artik alt aglardan olusuyor . URPF kullanmadan once yonlendirme tablosu detaylica incelenip karar verilmeli.

Snort Kullanarak SYNFlood saldırılarının Belirlenmesi

Snort saldırı testpit ve engelleme sistemidir. Spoof edilmiş ip adreslerinden yapılacak SYNFLood saldırıları karşısında herhangi bir engelleme özelliği olmamakla beraber, synflood saldırısının yapıldığını belirleyebilir.

alert tcp any any -> $WEB_SUNUCU 80 (msg:"Syn Flood Saldirisi"; flow: stateless; flags:S,12; threshold: type threshold, track by_src, count 100, seconds 1; classtype:attempted-recon; sid:10009;rev2;)

İşletim Sistemlerinde SYNFlood Koruması

Her işletim sistemi Synflood saldırılarına karşı benzer çözüm önermektedir.

1. Açılabilecek maksimum half-open sayısının arttırılması(SAYN_RECEIVED durumu)
2. Half-open bağlantılarda bekleme süresini kısaltma
3. TCP paketleri için zamanaşımı sürelerini düşürme

Backlog Queue değerini arttırma

Backlog queue değeri doğrudan sistemde varolan fiziksel bellekle alakalıdır. Bu değeri arttırırken sistemdeki bellekği de gözönüne almak gerekir.

Linux için backlog queue değerini arttırma

Öntanımlı değeri:

cat /proc/sys/net/ipv4/tcp_max_syn_backlog

1024

Arrtırmak için

echo 4096 > /proc/sys/net/ipv4/tcp_max_syn_backlog

bu değerin kalıcı olabilmesi için /etc/sysct.conf dosyasına yazılması gerekir.

FreeBSD backlog queue değeri arttırma

 # sysctl kern.ipc.somaxconn=4096

kern.ipc.somaxconn: 128 -> 4096

Zaman aşımı(Timeout) değerlerini düşürme

İşletim sistemleri SYN paketi aldığında buna SYN+ACK cevabı döner ve ACK cevabı bekler. Eğer ACK cevabı gelmezse belirli bir süre SYN+ACK cevabını tekrarlar. Bir Synflood saldırısı esnasında kaynak ipler spoof edilmiş olacağından gereksiz yere binlerce ip adresine defalarca SYN+ACK cevabi dönülecek ve kaynak tüketilecektir.

Backlog queude bekleme zamanını değiştirerek spoof edilmiş ip adreslerinden gelen syn paketlerinin çabucak paketlerin drop edilmesini sağlayabiliriz.

Linux altında gelen SYN paketine karşılık kaç kere ACK+SYN dönüleceği tcp_synack_retries değerinde saklanır.

cat /proc/sys/net/ipv4/tcp_synack_retries

5

Bu değerin 5 olması demek aşağı yukarı bağlantının üç dakika asılı kalması ve backlog queue'i şişirmesi demektir. Bu değeri iki ya da üç yaparak bağlantıların çok daha kısa sürelerde düşürülmesini sağlayabiliriz.

Syncookie aktivasyonu

Linux için;

sysctl net.ipv4.tcp_syncookies = 1

FreeBSD için

sysctl net.ipv4.tcp_syncookies = 1

ayarların kalıcı olabilmesi için /etc/sysctl.conf dosyasına yukardaki formatta yazılmış olması gerekir.

Sonuç

Syn Flood DDOS saldırıları oldukça basit , basit olduğu kadar da etkili bir saldırı yöntemidir. Teknik olarak saldırının altyapısı ve ağ yapısı bilinirse daha kolay önlem alınabilir. DDOS konusunda akıldan çıkarılmaması gereken husus bu tip saldırıların tak çalıştır cihazlarla engellenemeyeceğidir. Alınacak DDOS koruma ürünleri mutlaka kullanılacak ağın trafik yapısına göre ayarlanmalı ve özellikleri iyi bilinmelidir. Tak ve çalıştır tipi cihazlar komplike saldırılara karşı etkisiz kalacaktır.

DDOS saldırıları ve korunma yöntemleri konusunu uygulamalı olarak öğrenmek isterseniz http://www.guvenlikegitimleri.com/new/egitimler/ddos-saldiri-tipleri adresindeki eğitim yardımcı olacaktır.

KAYNAKLAR:

[1] http://www.lifeoverip.net/doddos/
[2] Syncookies implementation for the Linux kernel
(http://tomoyo.sourceforge.jp/cgi-bin/lxr/source/net/ipv4/syncookies.c)
[3] http://cr.yp.to/syncookies.html
[4] http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html
[5] http://asert.arbornetworks.com/2010/01/fire-or-ddos-which-is-more-probable/
[6] Web Sunuculara Yönelik DOS/DDOS Saldırıları