ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/syn-flood-ddos-saldirilari/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Syn%20Flood%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)

SYN Flood DDOS Saldırısı TCP'ye özel bir saldırıdır. Internet dünyasında en sık gerçekleştirilen DDOS saldırısı tipidir. Oldukça kolaydır. Eğer gerekli önlemler alınmamışsa 2Mb'lık hat ile 100 Mb'lık hatta sahip sistemler devre dışı bırakılabilir. Saldırıyı yapması kadar korunması da kolaydır.

(Page 2)

2)

Syn Flood saldırısı basitçe hedef sistemin açık bir portuna sistemin kapasitesinin üzerinde SYN paketi göndererek yapılır. Saldırı yapan kendini gizlemek için gerçek IP adresi kullanmaz.

(Page 11)

3)

İşletim sistemleri aldığı her SYN paketine karşılık üçlü el sıkışmanın tamamlanacağı ana kadar belleklerinden bir alan tahsisi yapar. İşletim sistemlerinin bu şekilde half-open olarak ne kadar bağlantı tutabileceğini Backlog Queue veri yapısı belirler.

(Page 12)

4)

Backlog Queue değeri 1000 olan sisteme 1000 adet SYN paketi gönderilerek hedef sistemi servis veremez duruma getirebiliriz.

(page 14)

5)

SYN Flood saldırılarında sahte IP kullanılırsa saldırı yapılan sistemden geriye doğru binlerce SYN+ACK paketi dönecektir. Bu da belirtilen IP'ye sahip makinaya ayrı bir saldırı olarak değerlendirilir. Buna SynFlood Backscatter denir.

(Page 15)

6)

SYN Flood Araçları

- Hping
- Netstress
- Juno
- Windows Tabanlı Araçlar
- Botnet Yönetim Sistemleri

(Page 16)

7)

Syn Flood Saldırısı Örneği

> hping3 -S --flood -p 80 192.168.1.1

(Page 18)

8)

Random sahte IP adresi kullanarak SYN Flood saldırı örneği

> hping3 -S --flood -p 80 192.168.1.1 --rand-source

(Page 20)

9)

Syn Flood saldırılarını gerçekleştirmek kolay olduğu gibi engellemek de çok kolaydır. Dünyada Syn Flood saldırılarını engellemek için iki temel çözüm kullanılır:

- Syn Cookie
- Syn Proxy

(Page 25)

10)

Syn Cookie Aktifken TCP Bağlantısı
Syn Cookie aktif edilmiş bir sistemde gelen SYN paketleri için sistem kendi içinde bir kaynak ayırmaz. Böylece gelen SYN paketleri için sistemde bellek tüketilmemiş olacaktır.

NOT: Syn Cookie aktifken tcp iletişimini tedarik eden TCP Sequence numaraları (ISN'ler) Syn Cookie'ye has formüllerle hazırlanır ve bunlar cookie olarak adlandırılır.

(Page 27)

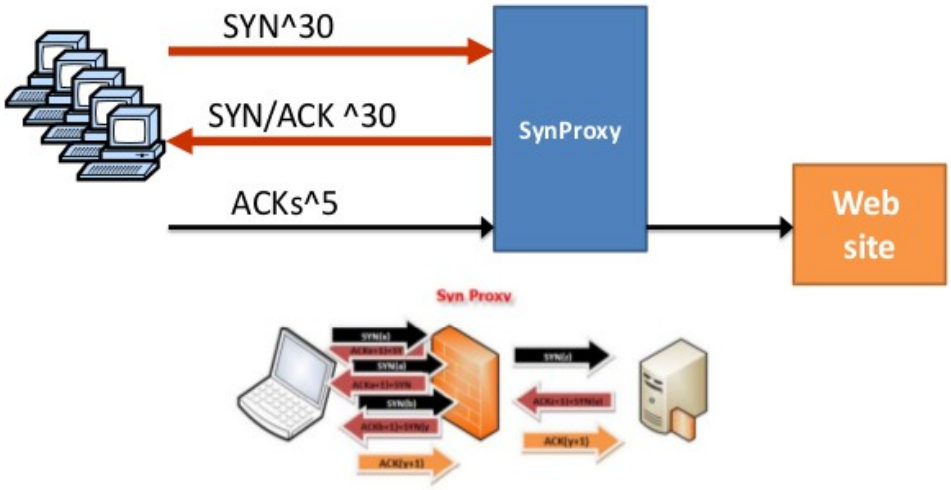
11)

Syn Proxy
Syn Proxy adından da anlaşılabileceği üzere SYN paketlerine karşı proxy'lik yapmaya yarayan bir özelliktir.

(Page 34)

12)

Syn Proxy Mantığı
Syn Proxy sadece 3'lü el sıkışmanın olduğu TCP bağlantılarını sunucuya geçirir.



NOT: Syn Proxy'de proxy'lik yapan makina state bilgisi tutacağından yoğun saldırılarda state tablosu şişebilir.

(Page 35-36)

13)

FIN Flood Saldırı Örneği

> hping3 -F --flood -p 80 192.168.1.1

(Page 49)

14)

ACK Flood Saldırısı Örneği

> hping3 -A --flood -p 80 192.168.1.1

(Page 50)