ERİŞİM ENGELLEME DOS VE DDOS:

DoS nedir?

Denial of service türkçesi erişim engelleme saldırısı olarak anlaşılmaktadır. Hedef bilgisayar ağının kaynaklarını kullanamayacak şekilde erişilmez kılınmasını amaçlayan saldırı türüdür.

Bir DoS atağı nasıl gerçekleştirilir?

Saldırgan hedef sistemi sahte syn istekleri ve udp istekleriyle cevap veremeyecek duruma getirerek erişilemez kılmayı amaçlar. Saldırının başarılı olması için web sunucusunun veya saldırılan hedefin alabileceğinden fazla istek alması ve cevap veremez durumda overload olması gerekmektedir.

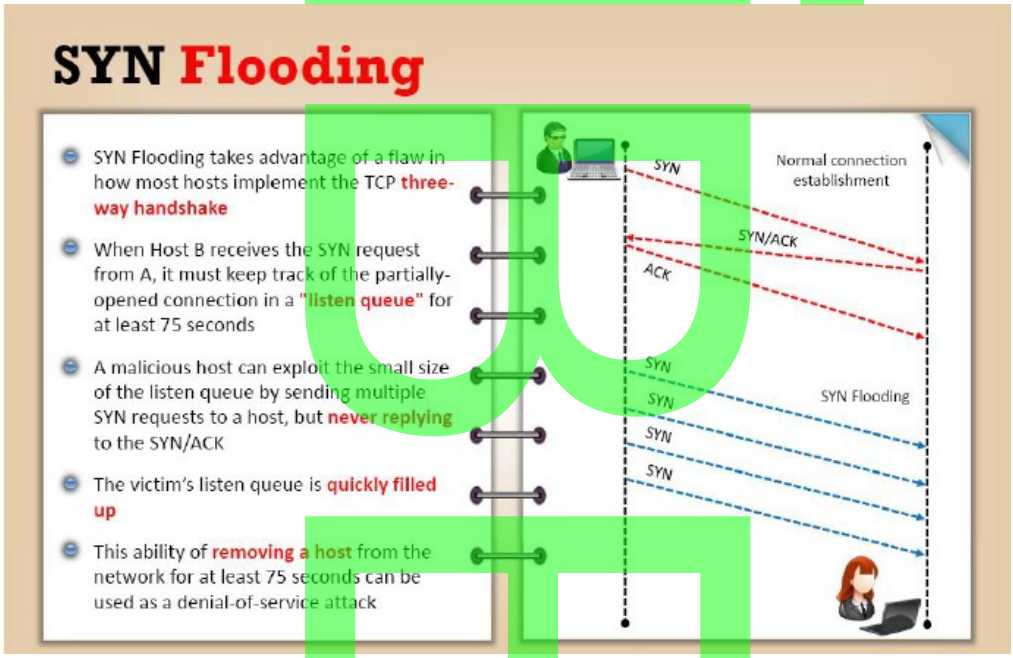
DDoS nedir?

Distributed Denial of Servis Saldırısı türkçesiyle Dağıtık Erişim engelleme saldırı olarak anlaşılmaktadır. Saldırı genellikle botnet olarak adlandırılan ele geçirilmiş zombi olarak adlandırılan bilgisayarlar vasıtası ile gerçekleştirilmektedir. Ele geçirilmiş gerçek istek gönderen binlerce bazen milyon adet bilgisayar hedefi sayısız istek göndererek ulaşılamaz hale getirmektedir.

DdoS Atak Çeşitleri:

Service Request Saldırıları

Syn Flood Saldırıları:



Saldırgan hedefe sahte syn paketi gönderir.
Saldırılan hedef syn-ack cevabı döner.
Saldırgan fazla sayıda syn paketi göndererek sunucunun cevap veremez hale gelmesini sağlar.
Hedef cevap alamaz çünkü paketin kaynağı sahtedir.

Örnek komut:

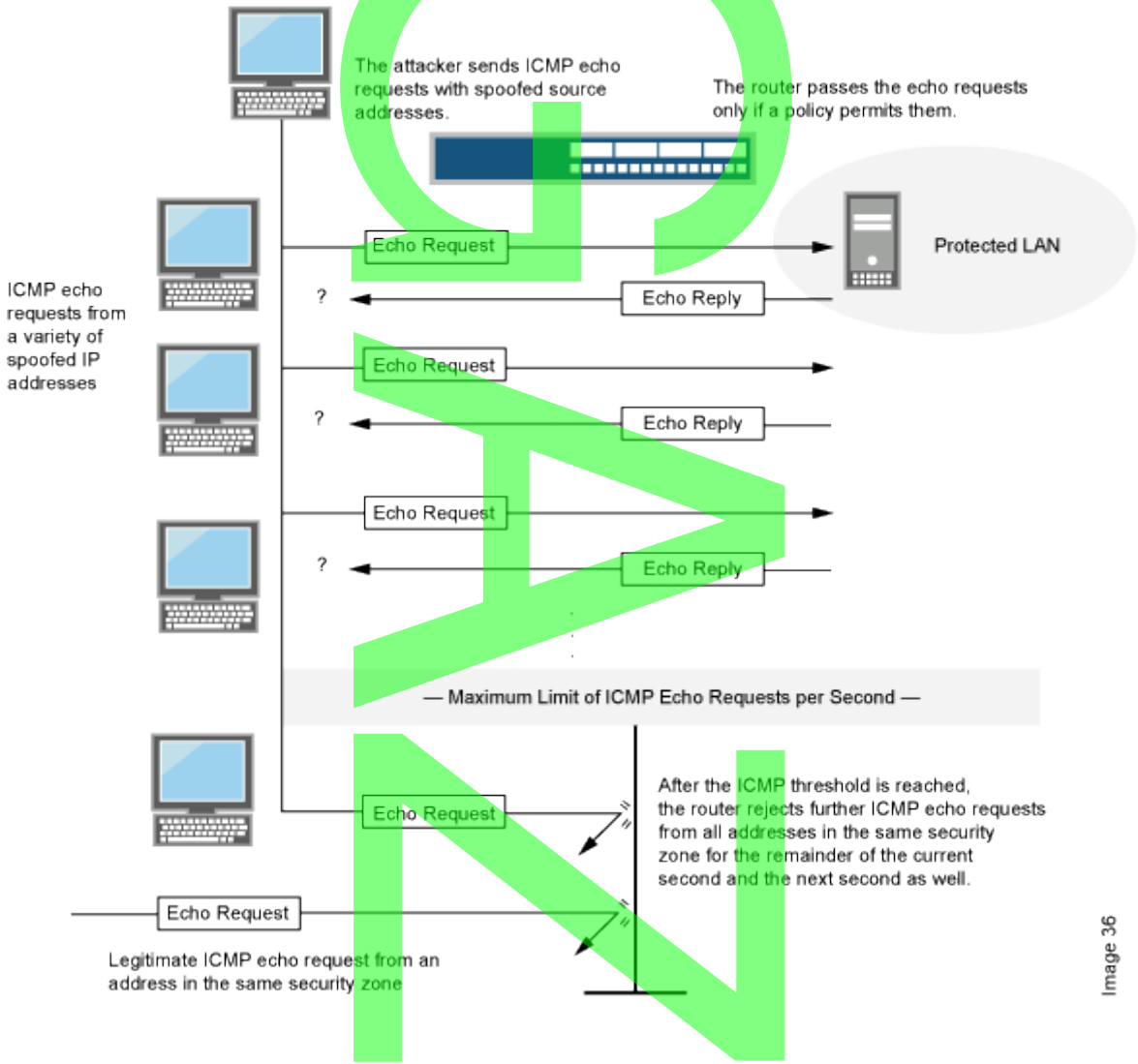
hping3 -S test.com -p 80 –rand-source

Söz konusu komut test.com sitesinin 80 portuna rastgele sahte adreslerden Syn flood atağı gerçekleştirir.

Söz konusu atağı izlemek için:

tcpdump dst host test.com and dst port 80

ICMP Flood Saldırıları:



Saldırgan sahte icmp echo istekleri gönderir. Sahte sayıda ve ardı ardına gönderilen icmp echo isteklerine hedef echo reply döner. Sahte isteklere cevap dönme süresi giderek yavaşlar ve hedef cevap veremez hale gelir.

ICMP Flood sahte kaynaklı adreslerden fazla sayıda paket göndererek hedefin cevap veremeyecek şekilde crash olmasına sebep olur.

Örnek komut:

hping3 -1 192.168.2.3 –rand-source

Söz konusu komut hedefe sahte kaynaktan icmp echo isteği gönderir

Application Level DoS Saldırıları:

Üç çeşittir:

Flood:

Web uygulamasındaki zaafı kullanarak kullanıcıların erişimine kapatmak.Exploiting

Disrupt:Defalarca login denemesi yaparak kullanıcının engellenmesini sağlamak.

Jam:Birden fazla sql query'si göndererek hedefi erişilemez hale getirmek.

HTTP GET FLOOD:

Hyper Text Transfer Protokolü üzerinden get veya post şeklinde çeşitlendirebileceğimiz saldırı çeşidi.

HTTP GET FLOOD siteye GET istekleri gönderilerek yapılan saldırı çeşididir.Bunu kullanıcıların bir web sitesini ziyaret etmesine benzetebiliriz.Binlerce kullanıcının sayfaya istek gönderdiği bir senaryoda sayfa gönderilen GET isteklerini karşılayamaz ve cevap veremez duruma gelir.Bu saldırıyı önlemek için gelen ip'ye göre sınırlanama getirirsek saldırıdan korunmuş oluruz.

HTTP POST FLOOD ise form ve benzeri web sayfalarına captcha koruması yoksa sınırsız sayıda istek göndererek sitenin yoğun şekilde post isteği almasına neden olarak cevap vermemesine neden olmaktır.Önlem almak için CAPTCHA kullanılmalıdır.

Örnek program:slowloris

UDP FLOOD:

UDP connectionless bir protokoldür.

DNS Protokolü udp flood saldırısı ile çalışamaz hale getirilebilir.

Üçlü el sıkışma gereği olmadığı için doğası gereği spoof edilebilir.

Örnek komut:

hping3 --udp test.com -p 53 -a google.com -d 15—rand-source

DDOS Önlem:

İnternet servis sağlayacısından destek alınmalı.

Firewall konfigürasyonu doğru yapılandırılmalı.

IDS/IPS yapılandırması düzgün olmalı.(Tehdit önleme sistemi)(Intrusion Detection System)

IPS(Tehdit Engelleme Sistemi(Intrusion Prevention System)

Ip'ler tespit edilerek blacklist oluşturulmalı bu şekilde get flood ve zombi saldırılarının önüne geçilebilir.

LoadBalancer kullanılarak sunucu dengelemesi yapılmalı.Web sunuusu,mail sunucusu,dns sunucusuveritabanı sunucusu farklı makinelerde tutulmalıdır.

SYN Flood koruması:

SynCookie Koruması:

Linux'da:

```
sysctl -n net.ipv4.tcp_syncookies
```

Windows'da:

Windows Vista ve sonrası işletim sistemlerinde Syn Attack koruması varsayılan olarak etkin ve devre dışı bırakılamıyor.