ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/openbsd-packet-filter-ddos-koruma-ozellikleri/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Openbsd%20Packet%20Filter%20Ddos%20Koruma%20%C3%96zellikleri.pdf

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

1)

OpenBSD işletim sistemi *BSD ailesinin güvenliğe önem veren asi üyesidir. Firewall, IPS, VPN, Load Balancer, DDOS Engelleme amacıyla rahatlıkla kullanılabilir.

(Page 2)

2)

OpenBSD Packet Filter Firewall anormal paketleri (örn; port tarama, işletim sistemi versiyonu saptama, traceroute kullanma gibi paketleri) engeller.

(Page 4)

3)

Firewall bir paketi engellediğinde iki tür aksiyon alabilir:

- Paketi engelle ve geriye cevap dön
- Paket engelle ve geriye cevap dönme

DDOS saldırılarında kesinlikle geriye cevap dönmemelidir. Bu sistem kaynaklarını boşa israfa yol açar.

(Page 11)

4)

HTTP Get/Post flood saldırılarında IP spoofing yapılamaz.

(Page 18)

5)

Rate Limiting Çalışma Örnekleri

- IP başına gelen maximum bağlantı sayısını 100 ile limitle.
- IP başına saniyede gelecek paket sayısını 10 ile limitle.

Yukarıdaki gibi kurallara uymayan IP adresleri ddos tablosuna eklenir.

(Page 22)