ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/guvenlik-sistemlerini-atlatma-ve-alinacak-dersler/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/G%C3%BCvenlik%20Sistemlerini%20Atlatma.pdf

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

1)

Bilgi güvenliği dinamik bir alandır ve tak-çalıştır şeklinde hazır sunulan çözümlerin gerçek manada güvenliğimizi arttırmadığı bir gerçektir.

(Page 3)

2)

Güvenlik Sistemleri Çeşitleri

a. Firewall
b. IPS
c. WAF // Web Application Firewall
d. DoS Engelleme
e. N-DLP // Network Data Loss Prevention

(page 4)

3)

N-DLP

Data loss prevention (DLP) software products use business rules to classify and protect confidential and critical information so that unauthorized end users cannot accidentally or maliciously share data whose disclosure could put the organization at risk.

DLP is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.

(http://whatis.techtarget.com/definition/data-loss-prevention-DLP)

4)

Kısaca N-DLP kritik bilgileri tanımlayan ve dışa sızdırmayan bir güvenlik sistemidir.

(Benim notum)

5)

TCP/IP bilmeden Firewall/IPS yönetmek son derece yanlıştır ve sakat bir iştir.

(page 5)

6)

Firewalls (Güvenlik Duvarları)

● Güvenlik duvarları genelde iki tip engelleme yöntemi kullanırlar:

- DROP
- REJECT

DROP gelen veya giden paketi hattan düşür işini yapar. Bu işlem sonrası herhangi bir geri bildirim mesajı yollamaz.

REJECT gelen veya giden paketi hattan düşür işini yapar. DROP'un aksine bu işlemi gerçekleştrdikten sonra TCP RST veya UDP Port Unreachable gibi bir mesaj döner.

● Güvenlik duvarları paketlerin içeriğine bakmazlar (L7 firewal'lar hariç).

(Page 8)

7)

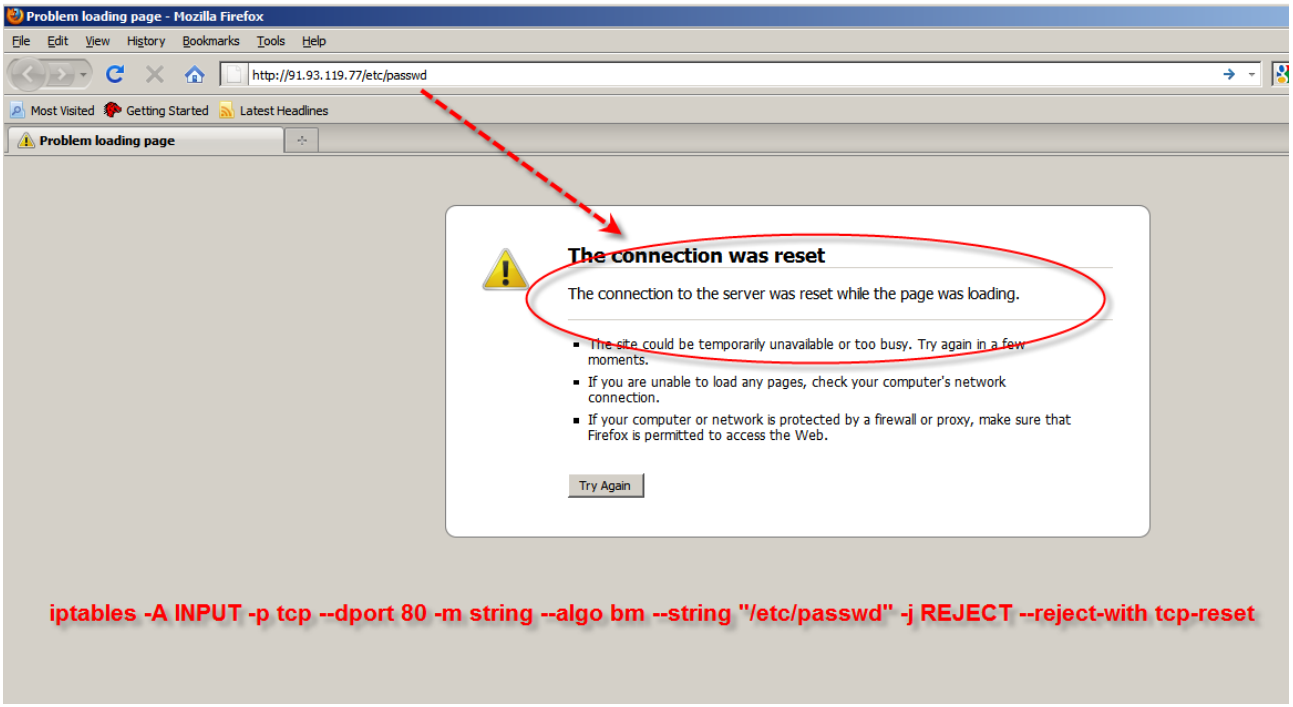
L7 Firewall
Uygulama katmanında işlem yapan Firewall'lara denir. Paketlerin sadece IP ve port bileşenlerine değil içeriğine de bakar. Örneğin bir L7 firewall'ı gidecek paketin içerisinde /etc/passwd geçiyorsa engelleyebilir. Böylece web uygulaması istediği kadar açık verse de firewall'dan /etc/passwd geçemeyeceği için saldırgan amacına ulaşamayacaktır. Firewall'a bu kuralı vermek için aşağıdaki sistem komutu kullanılabilir:

> iptables -A INPUT -p tcp -dport 80 -m string --algo bm --string "/etc/passwd" -j REJECT

Eğer aşağıdaki rule kullanılırsa;

> iptables -A INPUT -p tcp -dport 80 -m string --algo bm --string "/etc/passwd" -j REJECT **--reject-with tcp-reset**

ve hedef sitenin /etc/passwd dosyasını okuma teşebbüsünde bulunulursa ekrana aşağıdaki uyarı gelir ve saldırgan hedefine ulaşamaz.



(page 23)

8)

L7 Firewall Atlatma

1) Çeşitli IP parçalama teknikleri kullanılarak L7 Firewall'ları atlatılabilir.
2) Çeşitli encoding teknikleri kullanılarak L7 firewall'ları atlatılabilir.

(Page 24)

9)

Hping ile dilediğimiz şekilde paket üretip hedef sisteme göndererek DoS saldırısında bulunabiliriz. Yani hping kişiselleştirilmiş paket oluşturma kabiliyetine sahip olduğu gibi bu üretilen paketleri DoS amacıyla gönderim kabiliyetine de sahiptir. Örneğin bir saniyede 100 paket göndermek gibi ayarlamalara müsaittir.

(page 37)