ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/guvenlik-muhendisligi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

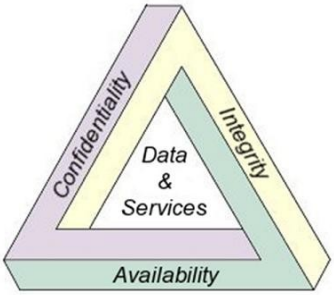
- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/G%C3%BCvenlik%20M%C3%BChendisli%C4%9Fi.pdf

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

1)

Güvenlik Üçgeni

- Bütünlük
- Gizlilik
- Erişilebilirlik



(Page 3)

2)

Eskiden bilişim güvenliği tek başına ele alınan bir olguydu. Zamanla bu olgu kendi içerisinde alt dallara ayrıldı:

- Ağ Güvenliği
- Web Uygulama Güvenliği
- İşletim Sistemi Güvenliği
- Unix/Linux Sistem Güvenliği
- Windows Sistem Güvenliği
- Veritabanı Güvenliği

(Page 5)

3)

Ağ Güvenliği Bileşenleri

- Router
- Firewall
- IDS/IPS
- Anormallik Tespit Sistemleri (ADS)
- Kablosuz Ağ Cihazları
- WAF (Web Application Firewall)
- Tüm bu sistemleri yönetecek mühendis

(Page 8)

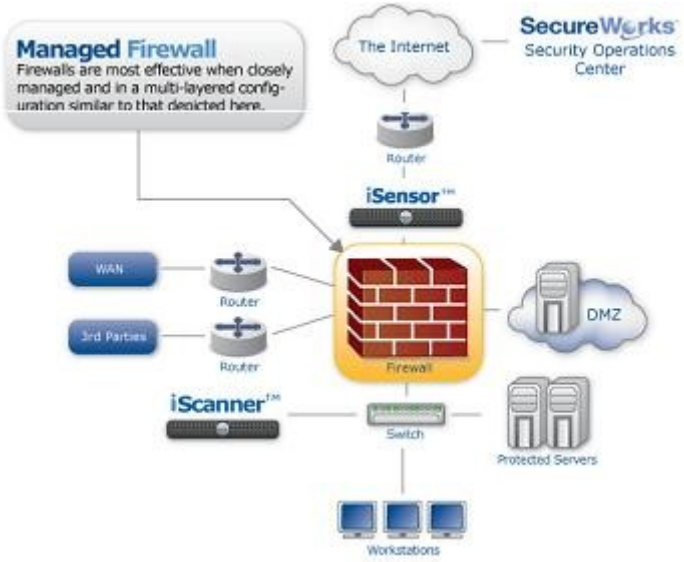
4)

Router
En temel ağ bileşenidir. Amacı ağlar arası paket yönlendirme yapmaktır. Paket filtreleme işlemleri de gerçekleştirebilmektedir. Örneğin IP ve port bazında filtreleme yapabilir. Katmanlı güvenlik anlayışının ilk bileşenini teşkil etmektedir.

(Page 9)

5)

Firewall
Firewall IP'ye, port'a, tcp bayraklarına göre filtreleme, ayrıca anormal bağlantıları sonlandırma yeteneğine sahiptir. Router ile Firewall benzer işlevleri yerine getirseler de temelde her ikisinin geliştirilme amacı farklıdır. Router yerel network'ümüzle internet arasındaki veri alışverişinden sorumlu bir cihazken, firewall bu veri alışverişinde gidip gelen paketlere filtreleme uygulayan bir cihazdır. Fakat zaman içerisinde firewall konumu gereği Router'ın kasasına dahil edilmiştir. Böylece 2 in 1 bir cihaz elde edilmiştir.



Firewall ile router'ın ayrı olduğu network'lerde router veri alışverişinden sorumluyken firewall ise bu veri alışverişini gözetlemekten ve denetlemekten sorumludur. Ayrıca bu iki cihazın ayrı olduğu network'lerde firewall cihazı router'ın hemen arkasına koyulur, çünkü internet'ten (router'dan) gelen her paketin network'e girmeden önce gözlemlenmesi ve denetlenmesi gerekmektedir.

(Page 10-11)

6)

Unix/Linux tabanlı Firewall
Modern software firewall'lar ile yarışabilir düzeydedir. Ücretsizdir. Evdeki iki bilgisayarı koruyabildiği gibi 5000 kullanıcılı bir şirketi dahi koruyabilir. Güvenlik duvarının çalışma şeklini ve arkasında yatan mantığı kavramak için kurcalanması gereken bir firewall'dur.

7)

Iptables
Iptables, linux işletim sistemlerinin varsayılan firewall'udur (güvenlik duvarıdır).

(http://www.ismailsaygili.com.tr/2012/10/iptables-nedir-ne-degildir.html)

8)

IPTables
iptables bir firewall'dur, fakat tıpkı linux'taki diğer programlar gibi bir komut satırı tool'udur ve komut satırından kumanda edilir. Iptables firewall'una argüman olarak verilecek kurallar doğrultusunda sistemde herhangi bir bağlantı başlatılmaya çalışıldığında iptables kendisine verilmiş kurallara göre bağlantıyı bir süzgeçten geçirir. Eğer bağlantı iptables'a verilmiş kurallara takılmazsa salıverilir, eğer kurallara takılırsa iptables kendisine verilen kuralda ne deniyorsa onu yapar. Örn;

```
> sudo apt-get install iptables
```

ile iptables kurulur. Kurallara örnek olarak aşağıdakiler verilebilir:

```
# Gelen trafiğe izin ver.
> iptables --policy INPUT ACCEPT

# Giden trafiğe izin ver.
> iptables --policy OUTPUT ACCEPT

# Gelen ve giden paketlerin akışına izin ver.
> iptables --policy FORWARD ACCEPT

> iptables --policy INPUT DROP
> iptables --policy OUTPUT DROP
> iptables --policy FORWARD DROP
```

Mevcut kurallar -L parametresi ile ekrana basılır.

```
> sudo iptables -L
```

Output:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
```

Chain **FORWARD** (policy **ACCEPT**)
target prot opt source destination

Chain **OUTPUT** (policy **ACCEPT**)
target prot opt source destination

(http://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/)

8)

IPFilter (IPF)
ipf açık kaynak kodlu Unix benzeri işletim sistemleri için NAT yapan ve firewall servisleri sunan, ayrıca adı üzere ip filtrelemesi yapabilen bir yazılımdır. Bu yazılımın geliştiricisi yazılımını IPv4 ve IPv6 protokollerini destekler şekilde tasarlamıştır.

NOT: Sanırım yukarıdaki tanıma göre IPFilter yazılımının Router cihazları üzerinde koştuğunu söyleyebilirim.

(https://en.wikipedia.org/wiki/IPFilter)

9)

IDS/IPS
Eskiden saldırılar daha çok network cihazlarına yönelik olurdu. Network cihazları üzerinden hedef makine hack'lenirdi. Fakat firewall ve router'ın varlığıyla beraber siyah şapkalı hacker'lar sistem hack'lemek için yönteme değişikliğine gittiler. Yeni yöntemleri uygulama yönelimli açık bulma olmuştur. Örneğin 25. portta çalışan Sendmail uygulamasının X bileşenini etkileyen bir saldırı ile hacker'lar sistemi exploit edebildikleri gibi payload ile de sistemi al aşağı edebilirler. Bu örnekte güvenlik gereği 25. portu kapatmak bir yoldur. Fakat bu portta çalışan servisin doğası gereği portun açık kalması zorunludur. Bu nedenle o portta çalışan ve ilgili uygulamadan anlayan, paketlerin içeriğine bakabilen bir sisteme ihtiyaç vardır. O sisteme IDS ve IPS denmektedir.

Firewall'ların paket içeriğine ilişememesi ve daha başka sebeplerden ötürü yetersizliği ortaya çıktığından IDS kavramı ortaya atılmıştır. IDS sistemine göre gelen saldırı sistemin alarmlarını tetiklemektedir. Fakat gelen saldırıyı engellememektedir. Engellemek için de IPS denilen sisteme gereksinim duyulmuştur. Böylece IDS alarmları çalarken IPS saldırıyı bloklamakla uğraşarak güvenliği üst düzeye çıkarmış olacaktır.

Açık kaynak kodlu IDS'e örnek olarak Snort verilebilir.

(Page 14-16)

10)

Paket analizini öğrenmeden IDS kullanmaya kalkılmamalıdır. Yoksa ezbere ortalıkta bir şeyler döner ve derinliğine vakıf olunamadığından yenilikçi bir saldırı sezilemeyebilir. Dolayısıyla kötü sonuçlar doğabilir.

(Page 21)