ÖN BİLGİ

Bu belgenin resmi adresi bulunamamıştır. Alternatif adreste yedeklenmiştir. Bu belge

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Sald%C4%B1r%C4%B1%20Tespit%20Sistemleri%20-%20Giri%C5%9F.pdf

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

1)

Saldırı Tespit Sistemi Nedir (IDS Nedir) ?
Saldırı tespit sistemleri internet veya yerel ağdan gelebilecek ve sistemlere zarar verebilecek paketlerden oluşan saldırıları fark etmek üzere tasarlanmış sistemlerdir. Temel amaçları belirlenen kurallar çerçevesinde bu saldırıları tespit ederek SMS, SNMP, Mail gibi araçlarla haber vermektir.

(Page 1)

2)

Saldırı Tipleri
Saldırganlar bir sisteme saldıracakları zaman iki genel yoldan birini benimserler. İlk yol acemi saldırganların tercih ettiği otomatize araçlarla yapılan saldırılardır. İkinci yol ise uzman seviyesindeki saldırganların hedefe göre değişebilen çeşitli yöntemleri uygulaması sonucu oluşan saldırılardır. İlk tip saldırıları önlemek ikinci tip saldırıları önlemeye göre daha kolaydır.

Yerel ağı korumak amacıyla icat edilen Firewall ve Antivirus gibi sistemler sadece ilk tip saldırganları engelleme imkanı sunmaktadır.

(Page 1)

3)

Saldırı tespit sistemleri savundukları ağ için düzenli olarak log tutarlar. Bu log'ların incelenmesiyle ağa sızan biri var mı, sızmışsa neler yapmış gibi bilgilere ulaşılabilir.

(Page 1)

4)

Saldırı Tespit Sistemlerinin İçerik Olarak Çalışma Şekilleri
IDS'ler içerik olarak iki ayrı prensipte çalışırlar. İlk yapıda Antivirus sistemlerinde olduğu gibi oluşturulmuş çeşitli imzalar ile paketleri incelerler ve eşleşme olduğunda saldırıyı tespit ederler. İkinci yapıda ise savundukları sistemlerin ve ağın normal işleyişini ortaya koyarlar ve bu normal işleyişin dışına çıkan hareketler saldırının tanımlanmasını sağlar.

İlk tür saldırı tespit sistemleri günümüzde yaygın olarak kullanılmaktadır. Belirlenen çeşitli kurallar çerçevesinde gelen paketleri inceleme şeklinde çalıştıkları için her saldırı izinin tanımlanmış olması gerekir. Bunu elle tek tek yapmak pek realistik olmadığı için bu iş adına saldırı imzaları yayınlayan sitelerden imzalar kullanılabilir. Bu tip imzalar dağıtan sitelerden bazısı şunlardır:

http://www.whitehats.com
http://www.snort.org

İkinci tür saldırı tespit sistemleri savundukları sistemleri düzenli olarak takip ederler ve bu öğrenme süreci sonrası karşılaştıkları olağan dışı hareketleri saldırı olarak raporlarlar. Bu tür saldırı tespit sistemlerinde iş pek kolay değildir. Çünkü IDS'e normal olarak nitelendirilebilecek hareketleri öğretmek oldukça fazla zaman almaktadır. Ayrıca bu hareketlerin zaman içerisinde değişebilirliği işi daha da güçleştirmektedir.

(Page 2)

5)

IDS'lerin Yerleşim Yerlerine Göre Sınıflandırılması
IDS'ler yerleşim yerine göre iki sınıfa ayrılmaktadır. Birincisi ağı koruyan IDS'lerdir, ikincisi ise spesifik bir sunucuyu koruyan IDS'lerdir.

Ağ tabanlı IDS'ler ağa gelen tüm paketleri incelerler ve ona göre raporla bildirimde bulunurlar. Sunucu tabanlı IDS'ler ise önce sunucuya yüklenirler. Böylece sunucudaki konfigurasyon dosyalarını, log'ları, sistemin bütünlüğünde meydana gelebilecek değişiklikleri izlemeye alırlar ve sisteme yönelik kötü niyetli hareketleri raporlarlar.

(Page 2)

6)

IDS'ler Firewall ve router gibi pasif güvenlik araçları değildirler. Aktif olarak raporlama, engelleme ve öğrenme gibi avantajlara sahiptirler.

(Page 2)

7)

Bir IDS kuralı yazarken, yani bir saldırı paketini tanımlarken paketin tüm özellikleri (paketin boyu, hedefi, içeriği, kaynağı, protokolü, hedef ve kaynak portu) tam olarak tanımlanmalıdır.

(Page 3)

8)

Saldırı tespit Sistemlerinin Zafıylıkları

1. Öncelikle IDS'lerin ortak problemlerine bakılırsa çok fazla hatalı kayıt ürettikleri görülmektedir. Henüz tam gerçel ve güvenilir kayıtlar üretememektedirler. Üretilen kayıtlardan büyük bölümü bir saldırıya ait değildir. Yani yanlış alarm vermektedirler.

2. IDS'ler tarafından üretilen log'lar henüz yasal delil olarak kullanılamamaktadırlar. Halen IDS'lerin bu yönü üzerinde çalışılmaktadır.

3. IDS'ler şifrelenmiş veri trafiği konusunda çözümsüz durumdadırlar. Örneğin ssl ile kurulmuş bir oturum içerisindeki paketleri fark edememeleri IDS'lerin ciddi zayıflıklardan biridir.

4. Ağa eklenecek yeni bir sunucu, sunulacak yeni bir hizmet gibi durumlar IDS'leri tekrar öğrenme sürecine sokacağı için bu süreç boyunca sürekli yanlış alarmlar üretilecektir.

(Page 3)

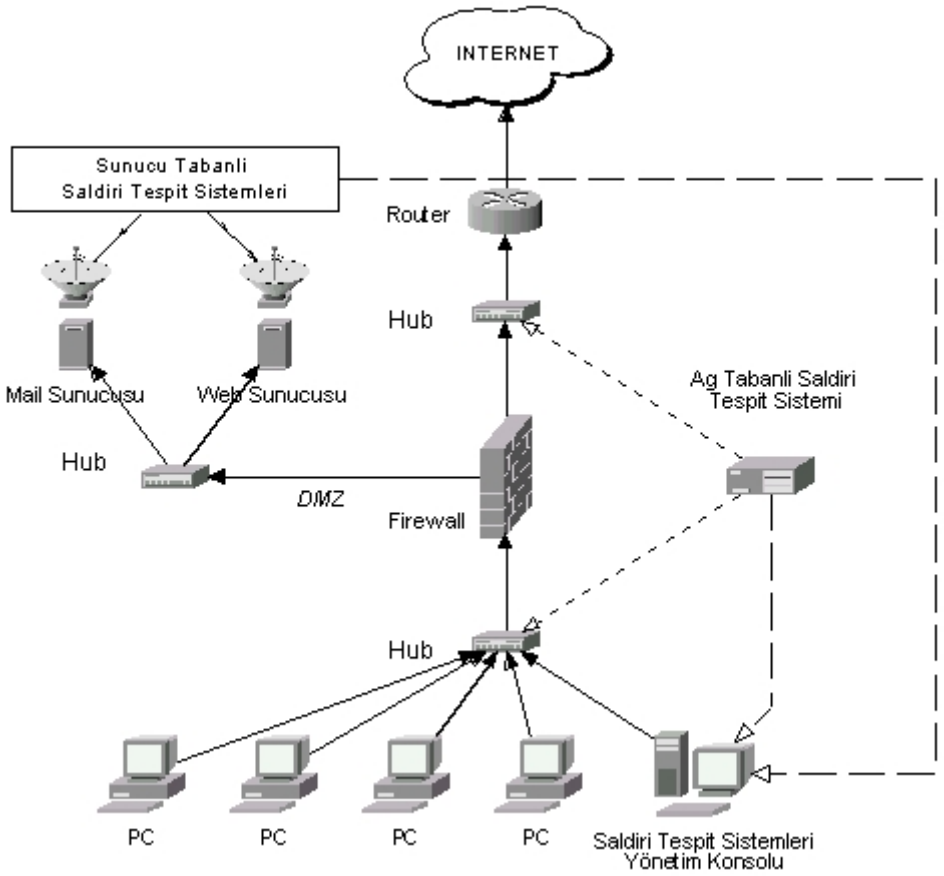
9)

IDS'leri atlatmanın bir yolu onların paket yakalama hızlarını istismar etmektir. Örneğin günümüzdeki IDS'lerin en iyisi bile ancak 60 Mbit'lik trafiği inceleyebiliyor. Daha hızlı bir trafik akıyorsa maalesef akan trafikteki paketlerin çoğunu inceleyemeden kaçırıveriyorlar. Saldırganlar böylesi bir trafik hızında saldırı paketlerini parçalayarak gönderdikleri takdirde IDS'ler paketlerden bir kısmını yakalayabilirken bir kısmını yakalayamayacaktır. Birleştirilemeyen paket dolayısıyla imzalar doğrulanamayacağı için saldırı paketleri IDS'i atlatmış olacaktır ve saldırı paketleri hedefte birleşeceğinden saldırı gerçekleşecek ve tüm bu olanlar IDS'in log'unda görünemeyecektir.

(Page 3)

10)

Aşağıdaki şekilde normalde saldırı tespit sistemlerinin nasıl yerleştirilmesi gerektiğine dair bir örnek verilmiştir.



Yukarıda basitçe bir ağ tasvir edilmiştir. Bu ağda DMZ bölgesinde Web sunucusu ve Mail sunucu yer almaktadır. Firewall ile router arasındaki hub ve yerel ağ ile Firewall arasındaki hub'a ağ tabanlı saldırı tespit sisteminde yer alan iki ethernet kartı da bağlı olmalıdır. Böylece ağ tabanlı bu saldırı tespit sistemi sniffer gibi çalışarak trafiği dinleyebilecektir. Ancak hub yerine switch kullanılırsa bu durumda switch'in portlarını ağ tabanlı saldırı tespit sisteminin portuna aynalamak gerekmektedir.

(Page 4-5)

11)

Saldırı Tespit Ürünleri

Firma	IDS Ürün Adı	
Axent	NetProwler	// Ağ tabanlı IDS
Axent	Intruder Alert	// Sunucu tabanlı IDS
Cisco	Cisco Net Ranger	// Ağ tabanlı IDS
NAI	CyberCOP Monitor	// Sunucu tabanlı IDS
ISS	Real Secure Host	// Sunucu tabanlı IDS
Cisco	Snort	// Ağ tabanlı (Açık Kaynak Kodlu)

(page 6)

12)

Sistemleri sürekli olarak izleyebilmeyi ve saldırıları kısa süre içerisinde fark edebilmeyi sağlayan IDS'ler güvenlik sektörünün vazgeçilmez ürünleri arasındadır. Henüz olgunlaşmamış olsalar bile yapılan saldırıları fark edebilme açısından ciddi bir alternatiftir.

Sunucu tabanlı sistemlerde kurulacak port tarama saptayıcıları, dosya bütünlüğü kontrol edicileri gibi yazılımlar ile güvenlik arttırılabileceği gibi Snort, Firestorm, Pakemon gibi ağ tabanlı saldırı tespit sistemleri kurarak da belirli seviyede bir güvenlik elde edilebilir.

(page 6)