SALDIRI TESPİT SİSTEMLERİ

Ankara Üniversitesi

Bölüm Tanıtımı

- Bu bölümde
  - **Saldırı tespit sistemeleri tanımı**
  - **Saldırı tespit sistemleri ilkeleri**
  - **Saldırı tespit sistemleri özellikleri**
  - **Saldırı tespit metodolojileri**
  - **Saldırı tespit yöntemleri**

  ayrıntılı olarak ele alınmıştır.

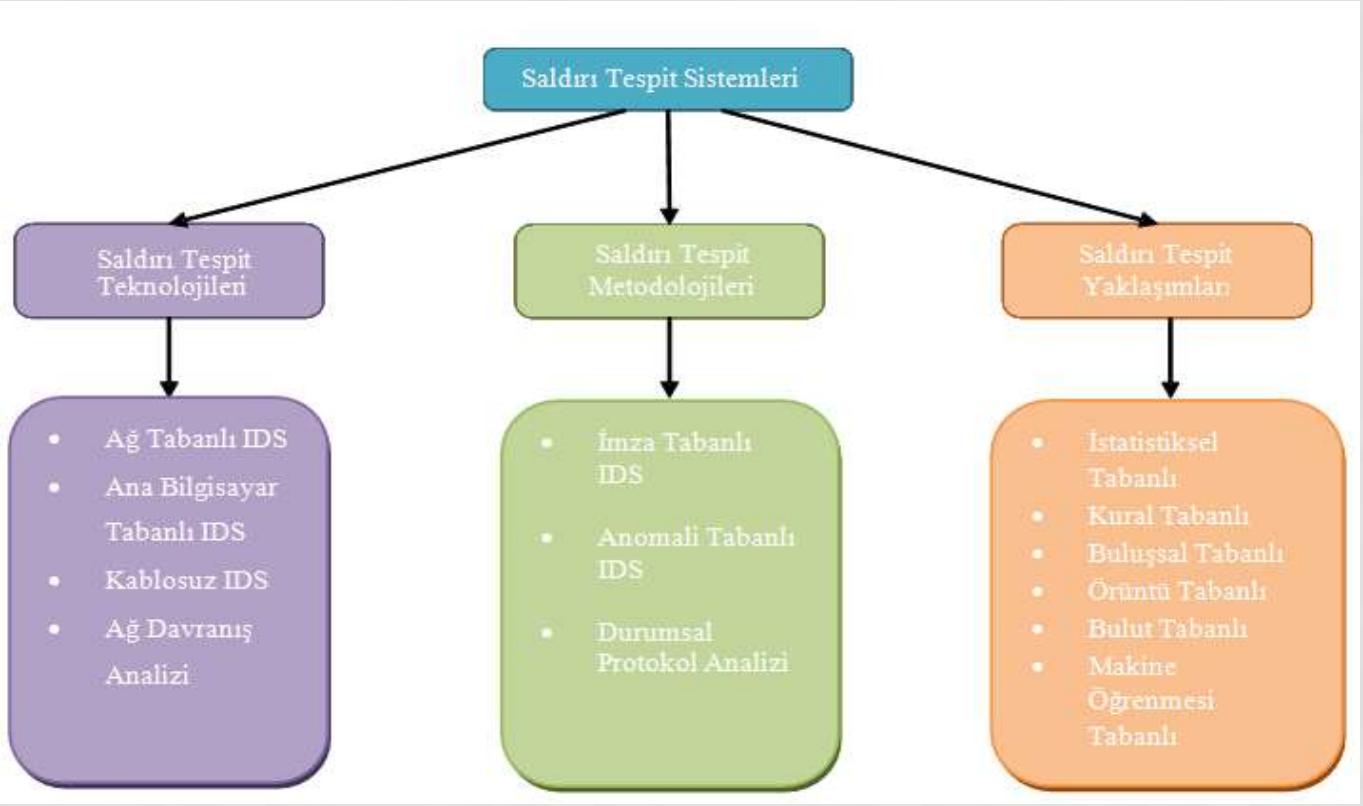
Giriş

- Saldırı tespiti, bir bilgisayar sisteminde veya ağında meydana gelen olayları izleme ve bu olayları güvenlik uygulamalarının ihlalleri veya yakın tehditleri gibi olası durumları analiz etme ve uyarma işlemidir.

- Saldırı tespit sistemleri (IDS) öncelikle olası olayları belirlemeye, onlar hakkında bilgi kaydetmeye ve kullanıcılara bildirmeye odaklanır. Ayrıca, kuruluşlar IDS'leri güvenlik politikalarıyla ilgili problemleri tespit etmek, mevcut tehditleri belgelemek ve kişileri güvenlik politikalarını ihlal etmekten alıkoymak gibi amaçlar için de kullanırlar.

Saldırı Tespit Sistemleri

- IDS teknolojilerinin türleri, temel olarak izledikleri olay türleri ve dağıtım şekilleri ile sınıflandırılır. Şekil'de saldırı tespit sistemlerinin sınıflandırılması verilmiştir.



Saldırı Tespit Sistemleri

- Genel olarak, verimli bir IDS için dikkate alınması gereken bazı önemli kurallar vardır ve bu kurallar aşağıda sıralanmıştır.
  - **IDS bileşenleri uygun şekilde güvence altına alınmalıdır.**

  IDS bileşenlerinin güvenliğini sağlamak çok önemlidir çünkü bu bileşenler, sistemlerin saldırıları tespit etmesini engellemek veya hassas bilgilere erişmek isteyen saldırganlar tarafından doğrudan hedef alınır.
  - **Saldırıların kapsamlı ve yüksek doğrulukta tespiti için birden fazla IDS teknolojisini kullanmak gerekebilir.**

  Her bir teknoloji, belirli olayları daha verimli bir şekilde tespit etme veya daha yüksek doğrulukla tespit etme gibi avantajlar sunar. Örneğin, verimli bir çözüm sağlamak için ana bilgisayar tabanlı ve ağ tabanlı IDS'ler entegre edilebilir
  - **IDS'leri değerlendirmeden önce, karşılaması gereken gereksinimler net olarak tanımlanmalıdır.**

  Bilgi toplama, kaydetme ve tespit etme dahil olmak üzere güvenlik yetenekleri, kapasite ve performans özellikleri gibi özellikleri göz önünde bulundurulmalıdır.

Saldırı Tespit Sistemleri

- **Saldırı Tespit İlkeleri**

IDS teknolojilerini uygularken etkili bir saldırı çözümü için bazı önemli faktörler vardır. Saldırıların yüksek doğruluk ve zamanında tespiti için aşağıda belirtilen özellikleri sağlamalıdır.

- Sistem dayanıklılığı/güvenilirliği;
- Hızlı tespit;
- Minimum yanlış pozitif;
- Maksimum doğruluk oranı;
- Minimum yazılım/donanım kullanımı;
- İzinsiz girişin yerini doğru bir şekilde tespit etme yeteneği;
- Diğer teknolojilerle çalışabilme.

Saldırı Tespit Sistemlerinin Temel İşlevleri

İstenmeyen olayları tespit etmek için olayları gözlemleme ve analiz etme yeteneğine ek olarak, tüm IDS türleri aşağıda belirtilen işlevleri sağlamalıdır.

- ✓ **Bilgilerin kaydedilmesi**: Bilgiler genellikle karşılaştırma için veya normal olarak ayarlanmış profiller oluşturmak için yerel olarak kaydedilir. Ayrıca kaydedilen bilgiler, merkezi kayıt sunucularına, bilgi güvenliği çözümlerine ve yönetim sistemlerine ayrı ayrı gönderilir.
- ✓ **Önemli olayların tespit edilmesi:** Düzenli olarak kayıt altına alınan ve normal olarak görülen bilgilerin dışında oluşan bir durumun hızlı ve doğru bir şekilde tespit edilmesi gerekmektedir.
- ✓ **Tespit edilen önemli olayların bildirilmesi:** Uyarı adı verilen bu bildirimler, sistemin kullanıcı arayüzünde e-posta, mesaj gibi çeşitli yöntemlerle gerçekleştirilir. Bir mesaj genellikle meydana gelen şüpheli olaylarla ilgili temel bilgileri içerir. Sistem kullanıcılarının daha fazla bilgi edinmek için IDS'ye erişmesi gerekir.
- ✓ **Rapor oluşturma:** Oluşturulan sistem raporları, gözlemlenen olayları özetler veya dikkate değer olaylar hakkında ayrıntılı bilgi sağlar. Örneğin, oturumda şüpheli etkinlik tespit edilirse, IDS daha ayrıntılı bilgi toplayabilir. Ayrıca, bir tehdit algılandıktan sonra uyarıların ne zaman verilmesi gerektiği gibi ayarları değiştirebilir.

Saldırı Tespit Sistemlerindeki Eksiklikler

- IDS'ler, diğer güvenlik ürünleriyle birlikte kullanıldığında katmanlı bir güvenlik mimarisi olarak kullanılabilir.
- WLAN için güvenlik standartları hala net olarak ortaya koyulamamıştır ve WLAN'lara özgü bir saldırı tespit sistemi bulunmamaktadır.
- Evrensel veri kümeleri üretmek için bu alanda birçok çalışma yapılmış olmasına rağmen, teorik olarak tüm normal davranışları modellemesi gereken veri kümelerinde hala eksiklikler bulunmaktadır.
- Yeni çalışmalarla bilinen saldırıların yanı sıra bilinmeyen saldırıları da bir ölçüde tespit edebilirken, normal davranışları da saldırı olarak tanımlanabilmektedir.
- İmza tabanlı sistemler ise imzaları ile saldırıları doğrudan tespit edebilir, ancak bilinmeyen saldırıları tespit edemezler.

Saldırı Tespit Teknolojileri

- **1. Kablosuz IDS**

Kablosuz IDS'ler çeşitli güvenlik özellikleri sunar. Kablosuz IDS nispeten yeni bir IDS türü olduğundan, özellikleri şu anda ürünler arasında büyük ölçüde farklılık göstermektedir. Temel olarak üç kategoriye ayrılan ortak güvenlik yetenekleri tanımlanmaktadır: bilgi toplama, kaydetme ve tespit etme.

Bilgi Toplama

- Kablosuz IDS'lerin çoğu kablosuz cihazlar hakkında bilgi toplayabilir. Bu bilgi toplama yeteneklerinin örnekleri aşağıdaki gibidir:
  - **Cihazları Tanımlama**
  - **Kablosuz Ağları Tanımlama**

Saldırı Tespit Teknolojileri

- **1. Kablosuz IDS**

Kaydetme Özelliği

Kablosuz IDS'ler tarafından yaygın olarak kaydedilen veri alanları aşağıdakileri gibidir:

- Zaman damgası (genellikle tarih ve saat)
- Etkinlik veya uyarı türü
- Öncelik veya önem derecesi
- Kaynak MAC adresi
- Kanal numarası
- Olayı gözlemleyen sensörün kimliği

Saldırı Tespit Özelliği

Kablosuz IDS'ler iletişimleri daha yüksek seviyelerde incelemez (IP adresleri, uygulama yükleri vb.). Bazı ürünler yalnızca basit imza tabanlı tespit gerçekleştirirken, diğerleri imza tabanlı tespit, anomali tabanlı tespit ve durumsal protokol analizi tekniklerinin bir kombinasyonunu kullanır

Saldırı Tespit Teknolojileri

- **1. Kablosuz IDS**

  Kablosuz IDS'ler tarafından en sık tespit edilebilen olay türleri aşağıdaki gibidir:

  - Yetkisiz WLAN ve cihazları
  - Olağandışı kullanımlar
  - Kablosuz ağ tarayıcılarının kullanımı
  - Hizmet reddi (DoS) saldırıları ve koşulları
  - Kimliğe bürünme ve ortadaki adam saldırıları

Saldırı Tespit Teknolojileri

- **2. Ağ Tabanlı IDS**

Ağ tabanlı IDS ürünleri çok çeşitli güvenlik yetenekleri sunar. Genel olarak üç kategoriye ayrılan ortak güvenlik özellikleri aşağıda tanımlanmaktadır: bilgi toplama, kaydetme ve tespit.

Bilgi Toplama

- Bazı ağ tabanlı IDS'ler sınırlı bilgi toplama özellikleri sunar; ana bilgisayarlar ve ana bilgisayarları içeren ağ etkinliği hakkında bilgi toplayabilirler. Bilgi toplama özelliklerine örnekler aşağıdaki gibidir:
  - **Ana Bilgisayarları Belirleme**
  - **İşletim Sistemlerini Belirleme**
  - **Uygulamaları Tanımlama**
  - **Ağ Özelliklerinin Belirlenmesi**

Saldırı Tespit Teknolojileri

- **2. Ağ Tabanlı IDS**

Kaydetme Özelliği

Ağ tabanlı IDS'ler tarafından yaygın olarak kaydedilen veri alanları şu şekildedir:

- Zaman damgası (genellikle tarih ve saat)
- Bağlantı veya oturum kimliği
- Etkinlik veya uyarı türü
- Derecelendirme (öncelik, önem, etki, güven)
- Ağ, iletim ve uygulama katmanı protokolleri
- Kaynak ve hedef IP adresleri
- Kaynak ve hedef TCP veya UDP bağlantı noktaları veya ICMP türleri ve kodları
- Bağlantı üzerinden iletilen bayt sayısı
- Uygulama istekleri ve yanıtları gibi veriler

Saldırı Tespit Özelliği

Çoğu ürün, ortak protokollerin derinlemesine analizini gerçekleştirmek için imza tabanlı algılama, anomali tabanlı algılama ve durumsal protokol analizi tekniklerinin bir kombinasyonunu kullanır.

Saldırı Tespit Teknolojileri

- **2. Ağ Tabanlı IDS**

  Ağ tabanlı IDS'ler tarafından en sık tespit edilebilen olay türleri aşağıdaki gibidir:

  - Uygulama katmanı keşif ve saldırıları:
  - İletim katmanı keşif ve saldırıları:
  - Ağ katmanı keşif ve saldırıları:
  - Beklenmeyen uygulama hizmetleri:
  - Politika ihlalleri

Saldırı Tespit Teknolojileri

- **3. Ağ davranış analizi sistemi**

NBA ürünleri çeşitli güvenlik yetenekleri sunar. Bunlar sırasıyla bilgi toplama, kaydetme ve tespittir

Bilgi Toplama

- NBA sistemleri saldırıların tespiti için aşağıdaki bilgileri elde etmektedir:
  - IP adresi
  - İşletim sistemi
  - IP protokolleri ve TCP/UDP bağlantı noktaları
  - İletişim kurduğu diğer ana bilgisayarlar ve hangi hizmetlerin kullanıldığı
- NBA sensörleri, bu bilgilerdeki değişiklikler için ağ etkinliğini sürekli izler. Her sunucunun akışına ilişkin ek bilgiler de sürekli olarak toplanır.

Saldırı Tespit Teknolojileri

- **3. Ağ davranış analizi sistemi**

Kaydetme Özelliği

NBA sistemleri tarafından yaygın olarak kaydedilen veri alanları şu şekildedir:

- Zaman damgası (genellikle tarih ve saat)
- Etkinlik veya uyarı türü
- Derecelendirme (örneğin, öncelik, önem, etki, güven)
- Ağ, taşıma ve uygulama katmanı protokolleri
- Kaynak ve hedef IP adresleri
- Kaynak ve hedef TCP veya UDP bağlantı noktaları veya ICMP türleri ve kodları
- Ek paket başlık alanları
- Bağlantı için kaynak ve hedef ana bilgisayarlar tarafından gönderilen bayt ve paket sayısı

Saldırı Tespit Özelliği

Çoğu ürün, ağ akışlarını analiz etmek için bazı durumsal protokol analizi teknikleriyle birlikte, öncelikle anomali tabanlı algılama kullanır.

Saldırı Tespit Teknolojileri

- **3. Ağ davranış analizi sistemi**

  NBA sistemleri tarafından en sık tespit edilen olay türleri aşağıdakileri içerir:

  - Hizmet reddi (DoS) saldırıları
  - Tarama
  - Solucanlar
  - Beklenmeyen uygulama hizmetleri
  - Politika ihlalleri

Saldırı Tespit Teknolojileri

- **4. Ana bilgisayar tabanlı IDS**

Ana bilgisayar tabanlı IDS'ler çeşitli güvenlik yetenekleri sunar. Bunlar günlüğe kaydetme ve tespit özellikleridir.

Günlüğe Kaydetme

- Genel olarak ana bilgisayar tabanlı IDS'ler tarafından kaydedilen veri alanları şunlardır:
  - Zaman damgası (genellikle tarih ve saat)
  - Etkinlik veya uyarı türü
  - Derecelendirme (öncelik, önem, etki, güven)
  - IP adresi ve bağlantı noktası bilgileri, uygulama bilgileri, dosya adları/yolları ve kullanıcı kimlikleri
  - Önleme işlemi (varsa)

Saldırı Tespit Özelliği

Bilinen saldırıları tanımlamak için sıklıkla imza tabanlı algılama tekniklerinin bir kombinasyonunu ve önceden bilinmeyen saldırıları tanımlamak için politika veya kural setleriyle anomali tabanlı tespit tekniklerinin bir kombinasyonunu kullanırlar

Saldırı Tespit Teknolojileri

- **4. Ana bilgisayar tabanlı IDS**

  Ana bilgisayar tabanlı IDS'lerde yaygın olarak kullanılan spesifik teknikler aşağıdaki gibidir

  - Kod Analizi
  - Ağ Trafiği Analizi
  - Ağ Trafiği Filtreleme
  - Dosya Sistemi İzleme
  - Günlük Analizi
  - Ağ Yapılandırması İzleme

Teknolojilerin Değerlendirilmesi

Kablosuz IDS'ler

- Kablosuz IDS'ler, WLAN protokolü düzeyindeki saldırıları, yanlış yapılandırmaları ve ilke ihlallerini tespit edebilir.
- Ayrıca, hizmet reddi saldırılarına ve fiziksel saldırılara karşı hassastırlar.
- Bazı kablosuz IDS ürünleri yalnızca imza tabanlı algılama gerçekleştirirken, diğerleri imza tabanlı algılama, anormallik tabanlı algılama ve durumsal protokol analizi tekniklerinin bir entegrasyonunu kullanır.
- Diğer IDS biçimleriyle karşılaştırıldığında, kablosuz IDS'ler daha yüksek izinsiz giriş algılama doğruluğuna sahiptir.
- Kablosuz IDS'ler güçlü algılama yetenekleri sunsalar da bazı sınırlamaları vardır: Pasif izleme ve kablosuz trafiğin çevrimdışı işlenmesini içeren saldırılar gibi kablosuz ağlara yönelik saldırı türlerini algılayamazlar.

Teknolojilerin Değerlendirilmesi

Kablosuz IDS'ler

- Kablosuz IDS'ler, WLAN protokolü düzeyindeki saldırıları, yanlış yapılandırmaları ve ilke ihlallerini tespit edebilir.
- Ayrıca, hizmet reddi saldırılarına ve fiziksel saldırılara karşı hassastırlar.
- Bazı kablosuz IDS ürünleri yalnızca imza tabanlı algılama gerçekleştirirken, diğerleri imza tabanlı algılama, anormallik tabanlı algılama ve durumsal protokol analizi tekniklerinin bir entegrasyonunu kullanır.
- Diğer IDS biçimleriyle karşılaştırıldığında, kablosuz IDS'ler daha yüksek izinsiz giriş algılama doğruluğuna sahiptir.
- Kablosuz IDS'ler güçlü algılama yetenekleri sunsalar da bazı sınırlamaları vardır: Pasif izleme ve kablosuz trafiğin çevrimdışı işlenmesini içeren saldırılar gibi kablosuz ağlara yönelik saldırı türlerini algılayamazlar.

Teknolojilerin Değerlendirilmesi

Ağ Tabanlı IDS'ler

- İlk teknolojilerin çoğu, yalnızca göreceli olarak basit bilinen tehditleri tespit etmek için doğru olan, imza temelli tespiti temel almaktadır.
- Daha yeni teknolojiler, doğruluğu ve tespit genişliğini arttırmak için tespit metotlarının bir kombinasyonunu kullanır ve genel olarak yanlış pozitiflerin ve yanlış negatiflerin oranları azalır.
- Ağa dayalı IDS'lerin doğruluğuyla ilgili diğer bir yaygın sorun, izlenen ortamın özelliklerini dikkate almak için genellikle önemli miktarda ayarlama ve özelleştirme gerektirmeleridir.
- Ağ tabanlı IDS'ler kapsamlı algılama yetenekleri sunsa da, bazı önemli sınırlamaları vardır. En önemlileri, şifreli ağ trafiğini analiz etmek, yoğun trafik yüklerini ele almak ve IDS'lerin kendilerine yönelik saldırılara dayanmaktır.
- Ağ tabanlı IDS'ler, sanal özel ağ (VPN) bağlantıları, SSL üzerinden HTTP ve SSH oturumları dahil olmak üzere şifreli ağ trafiğindeki saldırıları algılayamazlar ve çeşitli saldırı tiplerine karşı hassastırlar.

Teknolojilerin Değerlendirilmesi

Ağ Davranış Analizi Sistemleri

- NBA sistemleri küçük çaplı saldırıları tespit etmede hassastır, özellikle yavaş uygulanırsa ve yönetici tarafından belirlenen politikaları ihlal etmiyorlarsa algılama doğruluğu da zamanla değişir.
- NBA teknolojileri anomaliye dayalı algılama yöntemleri kullandığından, etkinliklerinin beklenenden önemli ölçüde farklı olduğu bir noktaya ulaşana kadar birçok saldırıyı tespit edemezler.
- Sensörleri anormal aktiviteye daha duyarlı olacak şekilde yapılandırarak, saldırılar meydana geldiğinde daha hızlı uyarılar üretilecektir, ancak daha fazla yanlış pozitifin de oluşması muhtemeldir.
- Tersine, eğer sensörler anormal aktiviteye karşı daha az hassas olacak şekilde yapılandırılmışsa, daha az yanlış pozitif olacaktır, ancak daha uzun süre boyunca saldırıların gerçekleşmesine izin veren uyarılar daha yavaş üretilecektir.

Teknolojilerin Değerlendirilmesi

Ana bilgisayar tabanlı IDS'ler

- Ana bilgisayar tabanlı IDS'ler tarafından algılanan saldırı türleri, sistemde kullanılan algılama tekniklerine bağlı olarak değişiklik gösterir.
- Diğer IDS teknolojilerinde olduğu gibi, ana bilgisayar tabanlı IDS'ler de sıklıkla yanlış pozitiflere ve negatiflere neden olur.
- Tespitin doğruluğu, ana bilgisayar tabanlı IDS'ler için daha zor olabilir. Çünkü çoğu IDS, günlük analizi ve dosya sistemi izleme gibi algılanan olayların gerçekleştiği bağlamı bilmez.
- Birkaç algılama tekniğinin bir kombinasyonunu kullanan ana bilgisayar tabanlı IDS'ler, genellikle tek bir teknik kullananlardan daha doğru bir algılama oranı sağlayabilir.
- Her teknik, sunucunun farklı yönlerini izleyebildiğinden, daha fazla teknik kullanmak, gerçekleşen faaliyetler hakkında daha fazla bilgi toplamayı sağlar. Bu, olayların daha eksiksiz bir profilini sağlar ve ayrıca olayların amacının değerlendirilmesine yardımcı olacak ek bilgiler sağlayabilir.