SALDIRI TESPİT SİSTEMLERİ-II

Ankara Üniversitesi

Bölüm Tanıtımı

- Bu bölümde
  - **Saldırı tespit metodolojileri**
  - **Saldırı tespit yöntemleri**

  ayrıntılı olarak ele alınmıştır.

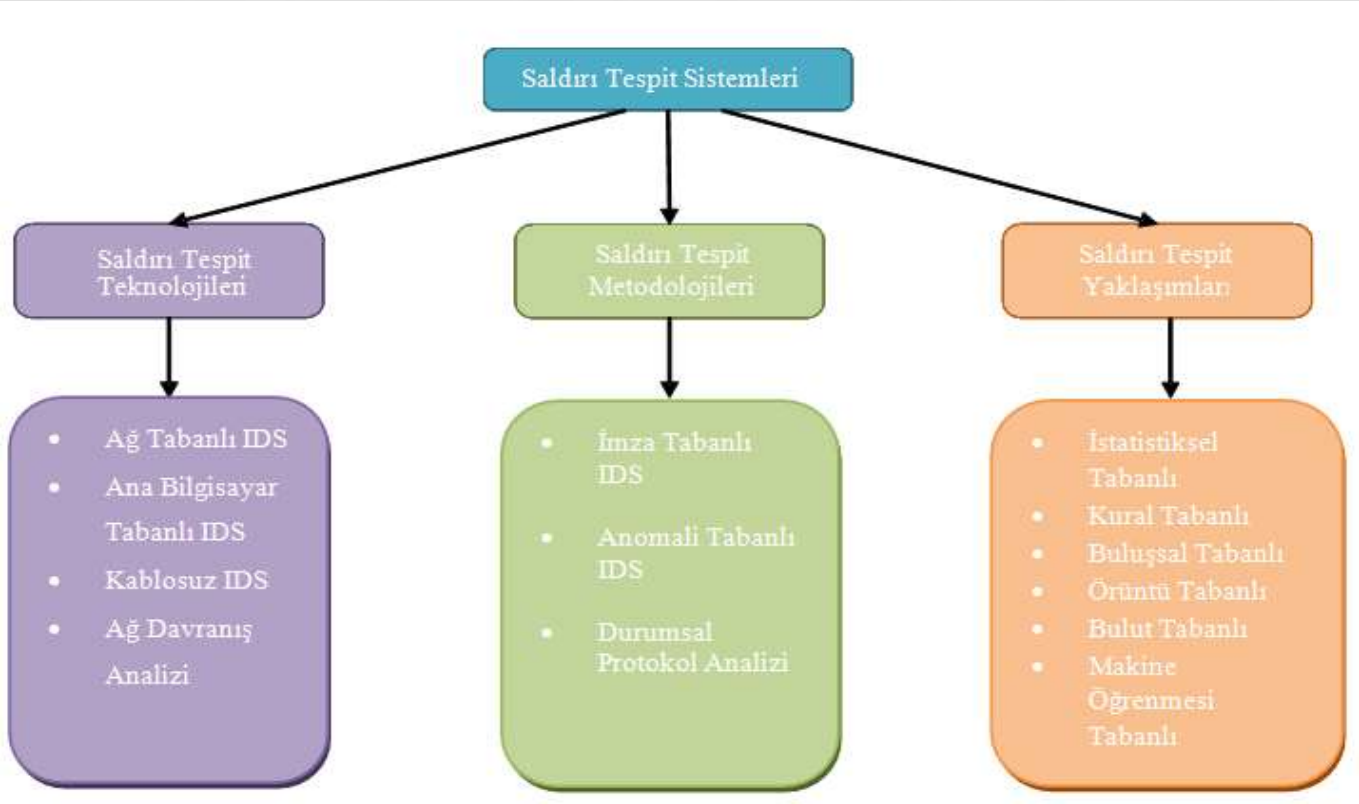
Giriş

- 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 Metodolojileri

1. İmza Tabanlı (Signature-Based) Model

- ✓ İmza, bilinen bir saldırıya karşılık gelen bir kalıptır.
- ✓ Bazı imza örnekleri şunlardır: Ağın güvenliğini tehdit eden "root" kullanıcı adıyla saldırı girişimi veya bilinen ve yaygın kötü amaçlı yazılımların ortak özelliği olan "Ücretsiz programlar" konulu bir e-posta.
- ✓ İmza tabanlı algılama, en basit algılama yöntemidir, çünkü karşılaştırma işlemi kullanılarak bir imza listesine göre kontrol edilir.
- ✓ İmza tabanlı IDS'ler bilinen tehditleri tespit etmede çok etkilidir, ancak bilinmeyen tehditleri veya bilinen tehditlerin türevlerini tespit etmede büyük ölçüde etkisizdir.

Saldırı Tespit Metodolojileri

2. Anomali Tabanlı (Anomaly-Based) Model

- ✓ Anomali tabanlı tespit, anormal olayları tanımlamak için gözlemlenen aktiviteleri normal kabul edilen tanımlarla karşılaştırma sürecidir.
- ✓ Anomali tabanlı algılama sistemi kullanan bir IDS, kullanıcıların, normal davranışını temsil eden kurallara sahiptir.
- ✓ Örneğin, iş günü saatlerinde web etkinliğinin ortalama kullanım süresidir bir kuraldır.
- ✓ Mevcut etkinliğin özelliklerini kurallarla karşılaştırırken uyarılar oluşturmak için istatistiksel yöntemler kullanır.
- ✓ Anomali tabanlı tespit yöntemlerinin en önemli avantajı, önceden bilinmeyen saldırı tiplerini tespit etmede etkili olmalarıdır.

Saldırı Tespit Metodolojileri

2. Anomali Tabanlı (Anomaly-Based) Model

- ✓ Anomali tabanlı tespit için oluşturulan kurallar iki türdür: statik ve dinamik.
- ✓ Bir kez oluşturulduktan sonra, IDS yeni bir kural oluşturmaya yönlendirilmedikçe statik kural listesi değişmez.
- ✓ Dinamik liste ise ek olaylar gözlemlendikçe sürekli olarak güncellenir.
- ✓ Kuralın bir parçası olarak kötü niyetli etkinliklerin yanlışlıkla dahil edilmesi, anomali tabanlı IDS ürünlerinde yaygın bir sorundur.
- ✓ Anormali tabanlı IDS'lerle ilgili bir diğer sorun, bazı durumlarda kuralları doğru belirlemenin zor olabilmesidir.
- ✓ Örneğin, büyük dosya aktarımları gerçekleştiren bir olay ayda yalnızca bir kez meydana gelmesi.

Saldırı Tespit Metodolojileri

3. Durumsal Protokol Analizi

- ✓ Durumsal protokol analizi, her bir protokol durumu için genel kabul görmüş normal (benign) protokol aktivite tanımlarının, önceden belirlenmiş profillerden sapmalarını tanımlamak için gözlenen olaylarla karşılaştırılmasıdır.
- ✓ Anomali tabanlı tespitin aksine, belirli protokollerin nasıl kullanılması ve kullanılmaması gerektiğini belirten, sağlayıcı tarafından geliştirilen evrensel profillere dayanır.
- ✓ Durumsal protokol analizi yöntemleriyle gerçekleştirilen "protokol analizi" genellikle bağımsız komutlar için minimum ve maksimum uzunluklar gibi denetimler içerir.
- ✓ Örneğin, bir komutun tipik olarak bir kullanıcı adı argümanı varsa ve kullanıcı isimleri maksimum 20 karakter uzunluğundaysa, 100 karakter uzunluğunda bir argüman şüphelidir.

Saldırı Tespit Metodolojileri

3. Durumsal Protokol Analizi

- ✓ Durumsal protokol analiz yöntemlerinin bir dezavantajı, birçok oturumun aynı anda izlenmesi nedeniyle analiz sürecinin karmaşık ve kaynak kullanımının yüksek olmasıdır.
- ✓ Diğer bir sorun, protokol davranışının özelliklerini ihlal etmeyen saldırı türlerinin tespit edilememesidir.
- ✓ Ayrıca, özel protokoller için, protokoller hakkında eksiksiz bilgi çoğu zaman mevcut değildir ve bu durum IDS teknolojilerinin kapsamlı ve doğru analizler yapmasını zorlaştırır.

Saldırı Tespit Yaklaşımları

1. İstatistiksel tabanlı yaklaşım

- ✓ Durumsal protokol analiz yöntemlerinin bir dezavantajı, birçok oturumun aynı anda izlenmesi nedeniyle analiz sürecinin karmaşık ve kaynak kullanımının yüksek olmasıdır.
- ✓ Gözlenen olayların normal olarak belirlenen profillerden farklı olması saldırıların göstergesidir.
- ✓ Normal profil oluşturulurken ortalama, mod, medyan, varyans ve standart sapma gibi istatistiksel metrikler kullanılır.
- ✓ Temel olarak üç kategoride sınıflandırılabilir: tek değişkenli, çok değişkenli ve zaman serisi modeli.

Saldırı Tespit Yaklaşımları

1. İstatistiksel tabanlı yaklaşım

İstatistik tabanlı IDS, aşağıdaki gibi sıralanabilecek bazı avantajlar içerir:

1. Saldırı imzasına gerek olmadığı için sıfır gün saldırılarını tanıyabilir.
2. Güncellemeye gerek olmadığı için bakımı kolaydır.
3. DoS ve DDoS saldırılarını algılayabilir.

Öte yandan istatistik temelli yaklaşımın sakıncaları ise şu şekilde sıralanabilir:

1. Normal bir profil oluşturmak zaman alır.
2. Normal profil zamanla değişebilir.
3. Kullanılan istatistiksel dağılımların etkili ve doğru olması gerekir.

Saldırı Tespit Yaklaşımları

2. Kural tabanlı yaklaşım

- ✓ Kural tabanlı IDS, ağ trafiğindeki olası saldırıları tespit ederken kuralları kullanır.
- ✓ Aynı tür ve sayıda saldırıyı tanımak için, kural tabanlı yaklaşım sadece birkaç kural gerektirirken, imza tabanlı yaklaşım binlerce imza gerektirir.
- ✓ Kural tabanlı IDS'yi devam ettirmek kolaydır.
- ✓ Kural tabanlı tespit sistemleri yeni saldırıları tespit edebilir çünkü saldırıdaki basit değişiklikler izinsiz giriş modellerini tamamen değiştiremez.
- ✓ Ancak, ağdaki olası tüm saldırıları tespit etmek için çok fazla kural gerektirir.

Saldırı Tespit Yaklaşımları

3. Sezgisel tabanlı yaklaşım

- ✓ Sezgisel tabanlı IDS, kötü niyetli davranışlara dayalı izinsiz girişleri arar.
- ✓ Normal davranışlardan saldırı davranışlarını doğru bir şekilde ayırt etmek için sezgisel yaklaşım bilgi ve deneyim gerektirir.
- ✓ Sezgisel yaklaşımda, toplanan izler herhangi bir şüpheli davranış için analiz edilir.
- ✓ Sezgisel tabanlı yaklaşımlar ile iyi bilinen ve sıfır gün saldırıları tespit edilebilir.
- ✓ Ancak bazı saldırı türleri, buluşsal algılama motorundan kaçmak için gizleme tekniklerini kullanabilir.

Saldırı Tespit Yaklaşımları

4. Örüntü tabanlı yaklaşım

- ✓ Örüntü tabanlı yaklaşım, toplanan verilerdeki anlamlı kalıpları çıkarmak için karakterleri, dizileri ve formları tanımlar ve bu kalıplara dayalı saldırıları bulur .
- ✓ Bilinen saldırıları hızlı ve verimli bir şekilde tespit edebilir, ancak imzaları (kalıpları) henüz bilinmediği için sıfır gün saldırılarının çoğunu tespit edemez.
- ✓ Örüntü eşleme algoritmaları, tekli ve çoklu desen eşleme olmak üzere iki türe ayrılır.

Saldırı Tespit Yaklaşımları

5. Bulut tabanlı yaklaşım

- ✓ Bulut ortamları üç tür hizmet sağlar: SaaS (hizmet olarak yazılım), PaaS (hizmet olarak platform) ve IaaS (hizmet olarak altyapı).
- ✓ IDS'yi bulut ortamının üzerine inşa etmek çeşitli avantajlar sağlar.
- ✓ Bulut ortamları, kötü niyetli ağ aktivitelerinin farklı açılardan tanımlanmasını sağlar ve klasik saldırı tespit sistemlerindeki eksiklikleri tamamlar.
- ✓ Bulut tabanlı IDS, kullanıcı veri toplayıcı, bulut hizmeti ve bulut saldırı algılama dahil olmak üzere üç farklı bileşenden oluşur .
- ✓ Bulut tabanlı IDS yaklaşımı hala erken aşamadadır. Bu yaklaşım, model performanslarını artırmak için gelecekte saldırı tespit sistemlerinde daha fazla kullanılmalıdır.

Saldırı Tespit Yaklaşımları

6. Makine öğrenmesi tabanlı yaklaşım

- ✓ Makine öğreniminin amacı, insan müdahalesi olmadan analiz sürecini otomatikleştirmektir.
- ✓ Makine öğrenimi yaklaşımı, denetimli (etiketli/etiketsiz veri), denetimsiz (etiketsiz veri) ve yarı denetimli (birkaç etiketli, birkaç etiketsiz veri) dahil olmak üzere farklı öğrenme tekniklerini kullanabilir.
- ✓ Saldırı tespiti için kullanılan yeni kullanılmaya başlanan bir yaklaşımdır.
- ✓ ML yaklaşımının başlıca avantajları, uyarlanabilirlik, yüksek performans, esneklik ve yeni saldırı türlerini tespit edebilmedir.

Saldırı Tespit Yaklaşımları

6. Makine öğrenmesi tabanlı yaklaşım

ML tabanlı IDS'nin aşağıdaki gibi sıralanabilecek bazı dezavantajları vardır:

1. ML algoritmaları veriler hakkında varsayımda bulunur.
2. Aykırı değerlerle her zaman başa çıkamaz.
3. Bilinmeyen saldırıların tespiti ve önlenmesi zordur.
4. Büyük veri boyutu (milyonlarca ağ bağlantısı).
5. Veri ön işlemesi zordur (İzleme sisteminden gelen verileri analiz için uygun formata dönüştürmek)
6. Yalnızca IP adreslerine değil, bağlamsal özelliklere de ihtiyaç duyulmaktadır.
7. Algoritmalar alan bilgisini hesaba katmaz.

Saldırı Tespit Yaklaşımları

7. Makine öğrenmesi tabanlı yaklaşım

- ✓ Derin öğrenme, görüntü işleme, insan tanıma, yüz tanıma, sürüş güvenliği ve kötü amaçlı yazılım tespiti gibi birçok farklı alanda kullanılmıştır. Son zamanlarda saldırı tespit sistemlerinde de kullanılmaya başlanmıştır.
- ✓ Derin öğrenme tabanlı IDS, sınıflandırma ve boyut küçültme avantajlarından yararlanarak anormallikleri tespit edebilir.
- ✓ Derin öğrenme modeli, yeni trafiği normal veya saldırı olarak sınıflandırır. Ayrıca saldırı türlerini belirterek daha fazla sınıflandırma yapabilir.

Saldırıları tespit etmede derin öğrenme yaklaşımının avantajları şu şekilde sıralanabilir:

1. Otomatik özellik çıkarma.
2. Çok büyük veri kümelerini işleme.
3. Güçlüdür, etkilidir ve özellik alanını önemli ölçüde azaltır.

Saldırı Tespit Yaklaşımları

7. Makine öğrenmesi tabanlı yaklaşım

DL tabanlı IDS yaklaşımının dezavantajları şu şekilde sıralanabilir:

1. Anlamlı özellikler tasarlamak için verilerin zor anlaşılması
2. Uygulamayı kontrol edecek iyi eğitimli alan uzmanlarının ve veri bilimcilerinin olmaması
3. Yeterli etiketli veri olmaması
4. Gizli bir katman oluşturmak zaman almaktadır ve ekstra gizli katmanlar eklemek nadiren model performansını artırır.
5. Kaçınma saldırılarına karşı dayanıklı değildir.

Saldırı Tespit Yaklaşımlarının Değerlendirilmesi

- **İstatistik tabanlı yaklaşım**, bilinen saldırıların yanı sıra sıfır gün saldırılarını da tespit edebilir. Her seferinde güncellemeye ihtiyaç duymaz. Çok çeşitli saldırı türlerini tespit edebilir. Ancak normal bir profil oluşturmak zaman alır.
- **Kural tabanlı yaklaşım**, binlerce saldırıyı tespit etmek için yalnızca birkaç kural gerektirir. Saldırı kodlarındaki basit değişiklikler izinsiz giriş modellerini tam olarak değiştiremeyeceğinden, yeni saldırı türevlerini tanır. Ancak, ağdaki tüm olası saldırıları tanımlamak için birden fazla kural gerektirir.
- **Sezgisel tabanlı yaklaşım**, yeni saldırıların davranışlarını tespit ederken kötü niyetli davranışlar listesini genişletebilir. Sezgisel tabanlı bir yaklaşımla hem bilinen hem de bilinmeyen saldırılar tespit edilir. Bununla birlikte, bazı saldırı türleri, iletişim ağlarında ve ana bilgisayarlarda yakalanmamak için kaçma teknikleri kullanır.
- **Örüntü tabanlı yaklaşım**, bilinen saldırıları hızlı ve verimli bir şekilde tespit eder, ancak imzaları henüz mevcut olmadığı için bilinmeyen saldırıların çoğunu tespit edemez. Örüntü tabanlı bir yaklaşımın uygulanması hızlı ve kolaydır.

Saldırı Tespit Yaklaşımlarının Değerlendirilmesi

- **Bulut tabanlı yaklaşım**, daha düşük maliyetli sınırsız hizmetler, 7/24 veri erişimi, daha fazla hesaplama gücü vb. gibi birçok avantaj sağlar. Bulutun üzerine farklı IDS teknikleri uygulanabilir. IDS performansını artırırken analiz süresini kısaltır. Bulut tabanlı IDS yaklaşımı hala erken aşamadadır ve yakın gelecekte IDS'lerde daha fazla kullanılmalıdır.
- **Makine öğrenmesi tabanlı yaklaşım**, saldırıları tespit etmek için analiz sürecini otomatikleştirir. Makine öğrenimi yaklaşımının temel avantajları, yüksek performansı, uyarlanabilirliği, esnekliği desteklemesi ve sıfır gün saldırılarını tespit etmesidir. Ancak, ML tabanlı IDS'nin büyük verileri işlemenin zor olması, veri ön işlemesinin zor olması ve algoritmaların alan bilgisini hesaba katmaması gibi çeşitli dezavantajları vardır.
- **Derin öğrenmeye tabanlı yaklaşım**, öğrenme süreci sırasında birden çok ardışık katman kullanır. Verilerdeki anormallikleri algılayabilir, büyük ölçekli ve çok boyutlu verileri tanıyabilir ve zamanla değişen dinamik verileri işleyebilir. Öte yandan, akışlar içinde yeterli bilgi bulunmaması, uygulamayı kontrol etmek için iyi eğitimli alan uzmanlarının olmaması, yeterli etiketli veri olmaması gibi dezavantajları vardır.