OSI Modelini Çözümlemek: Siber Güvenlikte Temel Bilgilere Giriş

Ahsen Beyza Özkul

ahsenbeyza@securedebug.com

İçindekiler

Giriş

Bilgilerin bilgisayar ağları üzerinden nasıl iletildiğini anlamak karmaşık görünebilir, ancak Açık Sistemler Bağlantısı (OSI) Modeli bu süreci daha yönetilebilir hale getirir. 1984 yılında Uluslararası Standardizasyon Örgütü (ISO) tarafından geliştirilen bu model, ağ iletişimini yedi farklı katmana ayırır ve her biri belirli bir role sahiptir.

OSI Modelini, verilerin iletimini farklı açılardan ele alan bir katmanlar yığını olarak düşünebilirsiniz. Bu yaklaşım, ağ süreçlerinin anlaşılmasını kolaylaştırır, sorunların giderilmesine, ağların tasarlanmasına ve verilerin güvenliğinin sağlanmasına yardımcı olur. Günümüzde daha çok TCP/IP modeli kullanılsa da, OSI Modeli, ağ sorunlarının görselleştirilmesi ve ele alınmasında hala değerli bir araç olarak kalmaya devam etmektedir.

Bu yazının devamında, OSI Modelinin her bir katmanını ele alacağız, net açıklamalar, basit örnekler ve her katmanın nasıl güvence altına alınacağına dair ipuçları sunacağız. Amaç, OSI Modelini daha anlaşılır ve pratik ağ ve güvenlik senaryolarında uygulanabilir hale getirmektir.

OSI Modeli Nedir?

Açık Sistemler Bağlantısı (OSI) modeli, bir bilgisayar ağının farklı parçalarının nasıl birlikte çalışarak iletişimi sağladığını anlamak ve tanımlamak için kullanılan bir yöntemdir. Bunu, her biri kendi özel görevine sahip katmanlardan oluşan bir yığın gibi düşünebilirsiniz. Bu, karmaşık ağ süreçlerinin daha basit ve yönetilebilir parçalara ayrılmasına yardımcı olur.

Daha basit bir ifadeyle, OSI Modeli, bir bilgisayar ağının farklı parçalarının iletişimi nasıl sağladığını anlamak için kullanılan bir kavramsal çerçevedir. 1984 yılında Uluslararası Standardizasyon Örgütü (ISO) tarafından tanıtılan bu model, ağı yapılandırılmış bir yaklaşımla ele alır ve karmaşık süreci yedi farklı katmana ayırır. Modern ağlar çoğunlukla daha basit olan TCP/IP modelini kullansa da, OSI Modeli, ağ sorunlarının görselleştirilmesi ve giderilmesi için hala önemlidir.

OSI Modeli Neden Önemlidir?

1. Standartlaştırılmış İletişim: OSI modelini, farklı cihazların ve programların birbiriyle iletişim kurmasını sağlayan ortak bir dil gibi düşünün. Tıpkı İngilizce konuşarak farklı yerlerden gelen insanlarla anlaşabildiğiniz gibi, cihazlar ve yazılımlar da OSI modeli sayesinde birbirlerini anlar, hatta farklı şirketlerden gelseler bile.

2. Sorun Giderme Kolaylığı: Ağınızda bir problem varsa—mesela internete bağlanamıyorsanız—OSI modeli, sorunun nerede olduğunu bulmanıza yardımcı

olur. Karmaşık bir sistemde hangi kısmın çalışmadığını bulmak için bir haritaya sahip olmak gibidir. Her bir katmanı kontrol ederek nerede bir sorun olduğunu tespit edebilirsiniz.

3. Ürün Tasarımına Yardım: Ağ ekipmanları veya yazılım üreten şirketler için OSI modeli, ürünlerini tasarlarken onlara yol gösterir. Örneğin, “Ürünümüz 4. Katmanda çalışıyor” diyebilirler (bu katman bağlantıların yönetimi ile ilgilidir) böylece ne işe yaradığını tam olarak bilirsiniz. Bu da ihtiyaçlarınıza uygun ürünleri seçmenizi kolaylaştırır.

4. Yazılım Geliştirme Kılavuzu: Geliştiriciler, yeni uygulamalar oluştururken OSI modelini kullanır. Bu model, iletişim sürecinin hangi bölümünün uygulamanız tarafından ele alınacağını bilmenizi sağlar, böylece diğer uygulamalar ve cihazlarla uyum içinde çalıştığından emin olabilirsiniz.

5. Güvenliği Artırmak: OSI modeli, verilerin güvende kalmasına da yardımcı olur. Hangi katmanın hangi tür verileri işlediğini anlayarak, güvenlik uzmanları doğru koruma önlemlerini devreye sokabilir ve bilgilerinizi güvende tutabilir.

6. Uzun Vadeli Kullanım: Daha yeni teknolojiler olmasına rağmen, OSI modeli hala faydalıdır. Farklı ağ sistemlerini anlamak ve karşılaştırmak için net bir yol sunar ve her şeyin sorunsuz bir şekilde çalışmasını sağlar.

OSI modelini anlamak, farklı ağ bileşenlerinin ve protokollerinin nasıl birlikte çalıştığını kavramanıza yardımcı olur. Ağ sorunlarını gidermek, ağları tasarlamak ve çeşitli teknolojilerin birbiriyle uyumlu çalışmasını sağlamak için faydalıdır.

OSI modeli, daha çok teorik bir çerçeve olsa da, gerçek dünyadaki ağ senaryolarını ve güvenlik hususlarını anlamanıza ve yönetmenize yardımcı olur.

Her bir katmanı çözümleyip rolünü anladığınızda, verilerin bir ağ üzerinden nasıl hareket ettiğini ve farklı protokoller ile cihazların nasıl etkileşimde bulunduğunu görebilirsiniz. Bu temel bilgi, ağlarla çalışan ya da ağlar hakkında öğrenen herkes için kritik öneme sahiptir.

OSI Katmanları

1) Katman 7: Uygulama Katmanı

- Ne Yapar: Bu katman, son kullanıcıya en yakın olan katmandır. Tüm uygulamaların ve hizmetlerin bulunduğu yerdir. Web tarayıcıları ve e-posta istemcileri gibi uygulamalara ağ hizmetleri sağlamaktan sorumludur.
- Basit Bir Örnek: Bir web tarayıcısı kullanarak bir web sitesini ziyaret ettiğinizde, Uygulama Katmanı isteğinizi işler ve web sitesini ekranınızda gösterir. HTTP

(HyperText Transfer Protocol) gibi protokoller kullanarak web sunucularıyla iletişim kurar.

2) Katman 6: Sunum Katmanı

- Ne Yapar: Sunum Katmanı, Uygulama Katmanından gelen verileri ağa uygun bir formata çevirir ve tam tersi işlemi yapar. Ayrıca veri şifreleme ve sıkıştırma işlemlerini de yönetir.
- Basit Bir Örnek: Şifrelenmiş bir e-posta gönderiyorsanız, Sunum Katmanı e-postayı göndermeden önce şifreler. Alıcı e-postayı aldığında, bu katman e-postayı çözerek okunabilir hale getirir. Ayrıca, verilerin Uygulama Katmanının çalışabileceği bir formatta olmasını sağlar.

3) Katman 5: Oturum Katmanı

- Ne Yapar: Bu katman, bilgisayarlar arasındaki bağlantıları yönetir ve kontrol eder. Farklı cihazlardaki uygulamalar arasında iletişim oturumları kurar, sürdürür ve sonlandırır. Ayrıca veri akışını ve iletişimdeki kesintileri de yönetir.
- Basit Bir Örnek: Bir video görüşmesi sırasında, Oturum Katmanı, bilgisayarınız ile arkadaşınızın bilgisayarı arasındaki bağlantının aktif ve düzenli kalmasını sağlar. Görüşmenin kesilmemesi için oturumu yönetir ve her şeyi senkronize tutar.

4) Katman 4: Taşıma Katmanı

- Ne Yapar: Taşıma Katmanı, verilerin cihazlar arasında güvenilir bir şekilde ve doğru sırada aktarılmasını sağlar. Verileri daha küçük paketlere böler, hata kontrolünü yönetir ve veri akışını kontrol eder.
- Basit Bir Örnek: İnternetten bir dosya indirdiğinizde, Taşıma Katmanı dosyayı daha küçük paketlere böler, bu paketleri bilgisayarınıza gönderir ve doğru sırayla yeniden birleştirir. Ayrıca iletim sırasında oluşabilecek hataları kontrol eder ve gerekirse yeniden iletim talep eder. Bu katmandaki iki ana protokol, güvenilir teslimata odaklanan TCP (Transmission Control Protocol) ve daha hızlı ama daha az güvenilir olan UDP'dir (User Datagram Protocol).

5) Katman 3: Ağ Katmanı

- Ne Yapar: Bu katman, verilerin farklı ağlar arasında yönlendirilmesini sağlar. Verilerin kaynaktan hedefe nasıl ulaşacağına karar verir ve veri paketlerine adres bilgilerini ekler.
- Basit Bir Örnek: Bilgisayarınızdan farklı bir ağdaki bir arkadaşınıza e-posta gönderdiğinizde, Ağ Katmanı e-postanın internet üzerinden nasıl iletileceğine karar verir. E-posta doğru yere ulaşsın diye ona bir IP (Internet Protocol) adresi ekler. Bu katmandaki yönlendiriciler, e-postayı en iyi yoldan yönlendirmeye yardımcı olur.

6) Katman 2: Veri Bağlantı Katmanı

- Ne Yapar: Veri Bağlantı Katmanı, verilerin yerel ağ üzerinde doğru bir şekilde aktarılmasını sağlar. Hata tespit ve düzeltme işlemlerini yönetir ve aynı ağdaki cihazlar arasında veri akışını düzenler.
- Basit Bir Örnek: Ev Wi-Fi ağınız üzerinden bir dosya gönderdiğinizde, Veri Bağlantı Katmanı dosyanın yerel ağınızdaki doğru cihaza gönderildiğinden emin olur. Veri paketlerine MAC (Media Access Control) adresleri ekler ve veriyi fiziksel ağ ortamı (kablolar veya kablosuz sinyaller gibi) üzerinden iletmek için düzenler.

7) Katman 1: Fiziksel Katman

- Ne Yapar: Bu en alt katmandır ve cihazlar arasındaki fiziksel bağlantıyla ilgilenir. Kablolar, anahtarlar ve ağ kartları gibi donanımları ve verilerin fiziksel olarak iletilmesini sağlar.
- Basit Bir Örnek: Fiziksel Katman, Ethernet kabloları, Wi-Fi sinyalleri ve verileri ileten gerçek donanımlar (ağ kartları gibi) gibi şeyleri içerir. Verileri kablolar veya hava üzerinden seyahat eden elektrik sinyallerine veya ışık darbelerine dönüştürmekten sorumludur.

OSI Modelinde Güvenlik ve 7 Katman

1) Fiziksel Katman (Katman 1):

    i. Tehditler: Kablosuz sinyallerin dinlenmesi ve fiziksel saldırılar.
    ii. Önlemler: Güvenlik kameraları ve güvenli kablolama kullanımı.

2) Veri Bağlantı Katmanı (Katman 2):

    i. Tehditler: MAC adresi sahteciliği ve anahtarlama saldırıları.
    ii. Önlemler: MAC adresi filtreleme ve VLAN'lar ile trafiği izole etme.

3) Ağ Katmanı (Katman 3):

    i. Tehditler: IP sahteciliği ve yönlendirme saldırıları.
    ii. Önlemler: Güvenlik duvarları ve VPN'ler kullanma.

4) Taşıma Katmanı (Katman 4):

    i. Tehditler: Ortadaki adam saldırıları ve DoS saldırıları.
    ii. Önlemler: TLS/SSL şifreleme ve güvenli oturum yönetimi.

5) Oturum Katmanı (Katman 5):

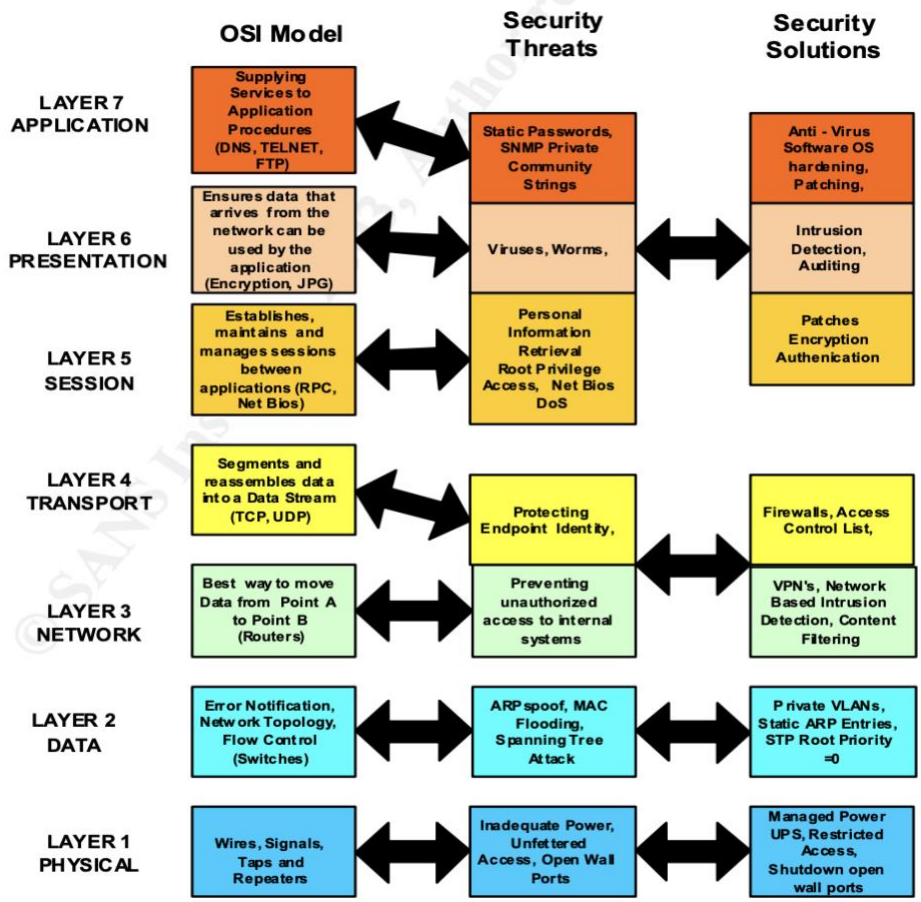
   i. Tehditler: Oturum korsanlığı.
   ii. Önlemler: Oturum şifreleme ve zaman aşımı politikaları.

6) Sunum Katmanı (Katman 6):

   i. Tehditler: Şifrelenmemiş veri.
   ii. Önlemler: Veri şifreleme ve güvenli veri formatları kullanma.

7) Uygulama Katmanı (Katman 7):

   i. Tehditler: Yazılım açıkları ve kimlik avı.
   ii. Önlemler: Güvenli kodlama, sık sık güvenlik testi, ve güçlü kimlik doğrulama.



Şekil 1
Güvenlik ile İlişkili OSI Modeli. *SANS Güvenlik Temel Bilgileri GSEC Pratik Görevi v1.4b* adlı eserden alıntılandı, Kim Holl, 2003, SANS Enstitüsü.

Kaynaklar

- Bangalore, K. (2023, 14 Eylül). Ağ katmanları (OSI modeli) genelinde güvenlik zorlukları. Medium. https://medium.com/@kavib/security-challenges-across-network-layers-osi-model-d03d5d187c7
- Froehlich, A., Rosencrance, L., & Gattine, K. (2021, Şubat). OSI. TechTarget. https://www.techtarget.com/searchnetworking/definition/OSI
- InfoSecTrain. (2023, 25 Ocak). OSI katman modeli ile ilgili yaygın güvenlik saldırıları. InfoSecTrain. https://www.infosectrain.com/blog/common-security-attacks-in-the-osi-layer-model/
- Plixer. (t.y.). Ağ katmanları açıklandı. Plixer. https://www.plixer.com/blog/network-layers-explained/
- Shaw, K. (2024, 9 Temmuz). OSI modeli açıklandı ve 7 katmanı kolayca nasıl hatırlanır. NetworkWorld. https://www.networkworld.com/article/964816/the-osi-model-explained-and-how-to-easily-remember-its-7-layers.html
- [CyberSpecs]. (2024, 1 Nisan). OSI modelinin farklı katmanlarındaki güvenlik uygulamaları. Medium. https://cyberspecs.medium.com/security-implementations-at-different-layers-of-the-osi-model-426df664a766
- Holl, K. (2003). *Uygulama güvenliğini artırmak için OSI savunma derinliği* [Şekil 2]. *SANS Güvenlik Temel Bilgileri GSEC Pratik Görevi v1.4b* içinde. SANS Enstitüsü. https://www.sans.org/ [eğer çevrimiçi mevcutsa]