TCP, UDP ve IP'nin Temelleri: Siber Güvenlikte Yeni Başlayanlar için Genel Bakış

Ahsen Beyza Özkul

ahsenbeyza@securedebug.com

İçindekiler

Ağ Protokolleri

Ağ protokolleri, internet gibi bir ağ üzerinden cihazların birbirleriyle iletişim kurarken uymaları gereken kurallar gibidir. Nasıl ki insanlar birbirlerini anlamak için aynı dili konuşmak zorundaysa, cihazlar da bilgi alışverişinde bulunabilmek için aynı protokolü kullanmak zorundadır. Bu kurallar, verinin bir cihazdan diğerine doğru ve güvenli bir şekilde iletilmesini sağlar; ister e-posta gönderiyor, ister video izliyor veya webde geziniliyor olsun.

Siber güvenlikte, ağ protokollerini anlamak çok önemlidir çünkü bu kurallar, verinin nasıl paylaşıldığının ve korunduğunun temelini oluşturur. Bu protokollerin nasıl çalıştığını bilmek, siber güvenlik uzmanlarının, bilgileri çalmaya çalışan hackerlar gibi tehditlere karşı ağları korumalarına yardımcı olur. Örneğin, HTTPS gibi güvenli protokoller, çevrimiçi alışveriş yaparken veya banka hesabınıza giriş yaparken verilerinizi güvende tutar. Ağ protokolleri hakkında iyi bir kavrayışa sahip olmadan, bir ağı güvence altına almak veya sorunları çözmek zor olurdu. Bu yüzden bu protokolleri öğrenmek, çevrimiçi ortamda güvende kalmanın ve dijital bilgileri korumanın önemli bir parçasıdır.

IP Nedir?

IP, İnternet Protokolü'nün kısaltmasıdır. Bilgisayarlar, telefonlar ve tabletler gibi cihazların internet üzerinden birbirleriyle iletişim kurmasını sağlayan bir dizi kuraldır. IP adresi, cihazınızın dijital bir ev adresi gibidir; bu adres, diğer cihazlardan çevrimiçi bilgi alıp gönderebilmenizi sağlar.

IP Adresleme

IP adresi, her cihazı bir ağda tanımlayan benzersiz bir sayı dizisidir. Bu, gerçek dünyadaki ev adresine benzer.

1) Özel IP Adresi: Bu, cihazınızın evinizde veya ofisinizdeki ağ içinde kullandığı addir. Örneğin, dizüstü bilgisayarınız, telefonunuz ve yazıcınız, birbirleriyle bağlanıp iletişim kurabilmeleri için özel bir IP adresine sahiptir.

2) Genel IP Adresi: Bu, tüm ağınızın (örneğin evdeki Wi-Fi) internete bağlanırken kullandığı addir. Bir web sitesini ziyaret ettiğinizde, web sitesinin gördüğü şey bu genel IP adresidir.

IP Yönlendirme

IP yönlendirme, verinin bir cihazdan diğerine internet üzerinden nasıl taşındığını ifade eder. Bir mesaj gönderdiğinizde veya bir web sitesini ziyaret ettiğinizde, veri küçük parçalara, yani paketlere bölünür. Her paketin üzerinde sizin IP adresiniz ve hedef IP adresi bulunur. Router'lar (yönlendiriciler), internette trafik yöneticileri gibi çalışır; bu

adresleri okuyarak paketleri farklı ağlar üzerinden en iyi yoldan hedefe ulaştırır. Paketler hedefe ulaştığında, orijinal mesaj veya web sayfası olarak tekrar bir araya getirilir.

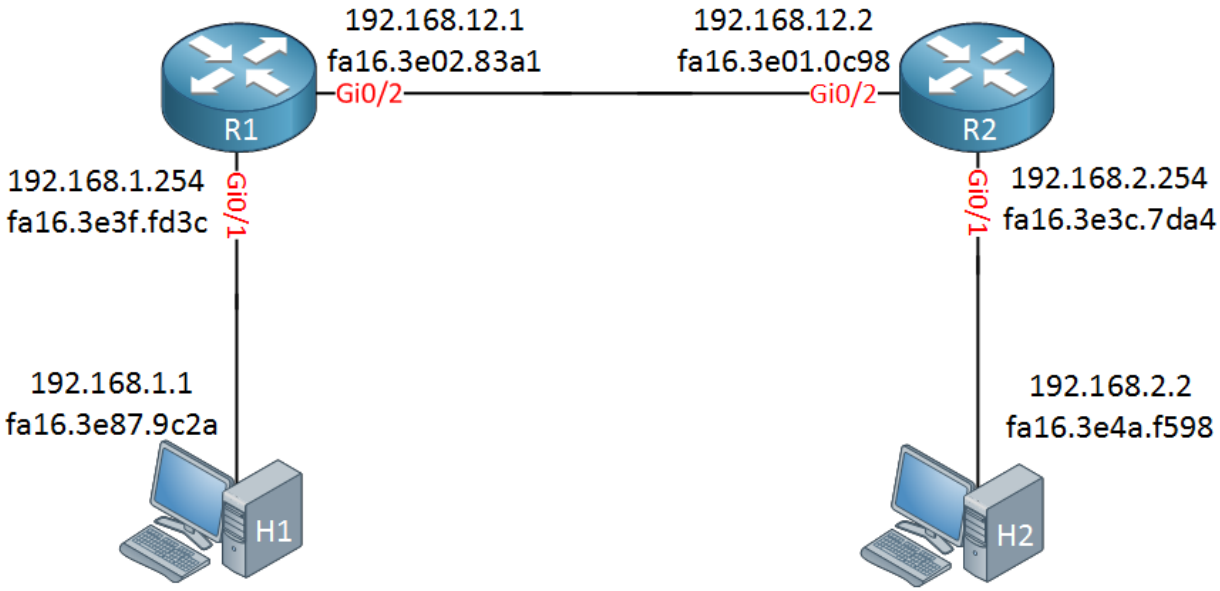
IP Yönlendirme Nasıl Çalışır?

IP yönlendirme, internetin posta dağıtım sistemi gibidir. Adım adım şöyle çalışır:

1. Cihazınızın Verdiği Karar

Cihazınız veri göndermek istediğinde (örneğin bir web sitesini yüklemek veya e-posta göndermek), önce verinin nereye gönderileceğine karar vermesi gerekir:

- Aynı Ağ: Hedef aynı ağdaysa (örneğin evdeki başka bir cihaz), cihazınız, hedefin MAC adresini zaten bilip bilmediğini görmek için bir listeyi (ARP tablosu) kontrol eder. Eğer MAC adresi bulunursa, veri doğrudan o cihaza gönderilir.
- Farklı Ağ: Eğer hedef, yerel ağınızın dışındaysa (örneğin internetteki bir web sitesi), cihazınız veriyi router'a (ağ geçidi) gönderir. Router'ın MAC adresi için ARP tablosunu kontrol eder ve veriyi oraya gönderir.



2. Router'ın Yaptıkları

Router veriyi aldığında, verinin nereye gönderileceğine karar vermesi gerekir. İşte olanlar:

- Hataları Kontrol Etme: Router önce verinin bozulup bozulmadığını kontrol eder. Eğer veri bozulmuşsa, router veriyi siler (göndermez).

- Adresi Kontrol Etme: Router, verinin kendisi için mi, yoksa başka bir cihaza mı iletilmesi gerektiğini görmek için hedef adresi inceler.

- En Mantıklı Yolu Bulma: Router, kendi haritasını (yönlendirme tablosu) kullanarak hedefe ulaşmak için en iyi yolu bulur. Verinin hangi yoldan gitmesi gerektiğine karar verir.

- Veriyi Hazırlama: Router, verinin bir sonraki aşamaya geçmesi için veriyi hafifçe değiştirir. Time to Live (TTL) adı verilen, verinin süresini belirten değeri azaltır. Eğer TTL süresi dolarsa, veri daha ileriye gönderilmez.

- Veriyi Gönderme: Son olarak, router veriyi ya doğrudan hedefe ya da yol boyunca başka bir router'a gönderir.

Bu süreç, veri farklı router'lardan geçerken tekrar tekrar gerçekleşir ve sonunda veri hedefe ulaşır. Her router, veriyi gitmesi gereken yere bir adım daha yaklaştırır, tıpkı farklı posta dağıtıcılarının bir mektubu doğru adrese ulaştırmasına yardımcı olması gibi.

Yaygın IP Zafiyetleri

- IP Sahteciliği: Bu, bir hacker'ın sahte bir IP adresi kullanarak başkasıymış gibi davranmasıdır. Bu, sistemleri zararlı veriyi kabul etmeleri için kandırabilir.
- IP Adresi Takibi: IP adresiniz, çevrimiçi faaliyetlerinizi izlemek veya konumunuzu tespit etmek için kullanılabilir. Bu durum istenmeyen dikkat veya saldırılara yol açabilir.
- DDoS Saldırıları: Bu, Dağıtılmış Hizmet Engelleme anlamına gelir. Hackerlar, bir ağı aşırı veriyle doldurup çökmesine neden olur. Bunu, savunmasız cihazların IP adreslerini hedef alarak yapabilirler.

TCP Nedir?

İletim Kontrol Protokolü (TCP), internet üzerindeki verinin trafik yöneticisi gibidir. Bir mektubu postayla gönderdiğinizi düşünün. TCP, mektubunuzun doğru yere, güvenli ve doğru sırayla ulaşmasını sağlayan posta hizmeti gibidir.

TCP, Verilerin Doğru Şekilde Ulaşmasını Nasıl Sağlar?

İnternette veri gönderdiğinizde, veri küçük parçalara, yani paketlere bölünür. TCP'nin işi, bu paketlerin doğru şekilde teslim edilmesini sağlamaktır:

1. Veriyi Düzenler: TCP, verinizi alır ve paketlere böler. Her pakete bir numara verir, böylece TCP, paketlerin diğer tarafta hangi sırayla olması gerektiğini bilir.
2. Hataları Kontrol Eder: TCP, her pakete bir kontrol kodu (checksum) ekler. Bu kod, paketlerin yolculuk sırasında zarar görüp görmediğini kontrol eder. Eğer bir paket hatalı gelirse, TCP, tekrar gönderilmesini isteyebilir.
3. Veriyi Yeniden Birleştirir: Tüm paketler hedefe ulaştığında, TCP bunları doğru sırayla yeniden birleştirerek orijinal veriyi tekrar oluşturur.

Üç Aşamalı El Sıkışma

Veri gönderilmeden önce TCP, bir bağlantı kurmalıdır. Bunu, bir konuşma öncesi el sıkışma gibi düşünebilirsiniz. İşte nasıl çalışır:

1. SYN (Senkronize Etme): Gönderici, "Merhaba, ben sohbet etmek istiyorum," diyerek bir SYN mesajı gönderir.
2. SYN-ACK (Senkronize-Accept): Alıcı, "Merhaba, konuşmaya hazırım," diyerek göndericinin isteğini onaylayan ve kendi SYN mesajını içeren bir yanıt gönderir.
3. ACK (Kabul Etme): Son olarak, gönderici, "Harika, başlayalım!" diyerek bir onay mesajı gönderir.

Bu el sıkışma, her iki tarafın da hazır olduğunu ve nasıl iletişim kuracaklarına dair anlaşmaya vardıklarını sağlar.

Veri Akışını Yönetme ve Tıkanıklığı Önleme

TCP, verinin hızlı bir şekilde gönderilmesini ve aşırı yüklenmeyi önlemeyi de yönetir:

1. Pencereleme: Bir konveyör bandını (veri paketleri) hareket ettirdiğinizi düşünün. TCP, alıcının kutuları (paketleri) ne kadar hızlı işleyebileceğine bağlı olarak konveyör bandının (pencere boyutu) boyutunu kontrol eder. Bu boyutu, her şeyin düzgün çalışmasını sağlamak için ayarlar.
2. Yavaş Başlangıç: Bir bağlantı başladığında, TCP veriyi yavaşça gönderir, böylece ağı aşırı yüklemez. Her şey yolunda giderse, hızını kademeli olarak artırır.
3. Tıkanıklık Kontrolü: Ağ kalabalıklaşırsa, TCP veri akışını yavaşlatarak sıkışıklığı ve çarpışmaları önler, bu da yoğun bir bölgede trafik hızını azaltmaya benzer.

Yaygın Sorunlar: TCP Zafiyetleri

Bazen, saldırganlar TCP bağlantılarını bozmayı hedefler. Yaygın bir saldırı türü:

• SYN Flooding (SYN Taşkınlığı): Saldırgan, bir sunucuya bir dizi SYN mesajı gönderir ama asla el sıkışmayı tamamlamaz. Bu, sunucuyu aşırı yükler ve gerçek bağlantıları işleyemez hale getirir.

Bu tür saldırılara karşı korunmak için, geçerli bağlantıları kontrol etme ve bağlantı girişimlerini sınırlama gibi çeşitli teknikler kullanılır.

UDP Nedir?

Kullanıcı Datagram Protokolü (UDP), internet üzerinden veri göndermek için kullanılan bir yöntemdir. Bunu, bir mektup yerine bir dizi kartpostal göndermek gibi

düşünebilirsiniz. Her kartpostal (veya "datagram"), bağımsız olarak gönderilir ve hepsinin sırayla veya hiç gelmeyeceği garantisi yoktur. Bu, UDP'yi hızlı yapar ancak TCP gibi diğer protokollere göre daha az güvenilir kılar.

UDP Nasıl Çalışır?

UDP, hız ve kolaylık için tasarlanmıştır:

1. Bağlantı Kurulumu Yok: TCP'nin aksine, UDP veri göndermeden önce bir bağlantı kurmaz. Paketleri doğrudan hedefe gönderir ve bir el sıkışma işlemi gerçekleştirmez.
2. Sıra ve Hata Kontrolü Yok: UDP paketlerinin sırayla gelmesi gerekmez ve UDP, paketlerin doğru gelip gelmediğini kontrol etmez. Paketler kaybolursa, yerleştirilmiş bir onaylama veya yeniden gönderme işlemi yoktur.
3. Paketler Bağımsızdır: Her paket (veya datagram) bağımsız olarak gönderilir, bu nedenle paketler farklı yollar izleyebilir ve sırayla veya kaybolarak gelebilir.

UDP Ne Zaman Kullanılır?

UDP, hızın mükemmel güvenilirlikten daha önemli olduğu uygulamalar için idealdir:

1. Video Yayını: Çevrimiçi film izleme gibi video akışlarında, birkaç kaybolmuş paket yerine yeniden gönderilmeyi beklemek daha iyidir. Video, her paket yeniden gönderilene kadar beklemek yerine birkaç kesinti ile daha akıcı oynar.
2. Çevrimiçi Oyunlar: Çevrimiçi oyunlarda, gerçek zamanlı etkileşim çok önemlidir. Paket onayı beklemekten kaynaklanan küçük bir gecikme, oyun deneyimini bozabilir. UDP, bazı paketler kaybolsa bile oyunun sorunsuz çalışmasını sağlar.
3. VoIP (Ses Üzerinden IP): İnternet telefon görüşmeleri gibi VoIP hizmetleri UDP kullanır çünkü küçük bir gecikme veya kaybolmuş paket, görüşmenin gecikmesine veya kesilmesine göre daha az rahatsız edicidir.
4. DNS Sorguları: Bir web sitesini aradığınızda, DNS sunucuları UDP kullanarak sorgulara hızlı bir şekilde yanıt verir. UDP'nin hızı burada faydalıdır ve birkaç DNS sorgusunun eksik olması genellikle büyük sorunlara yol açmaz.

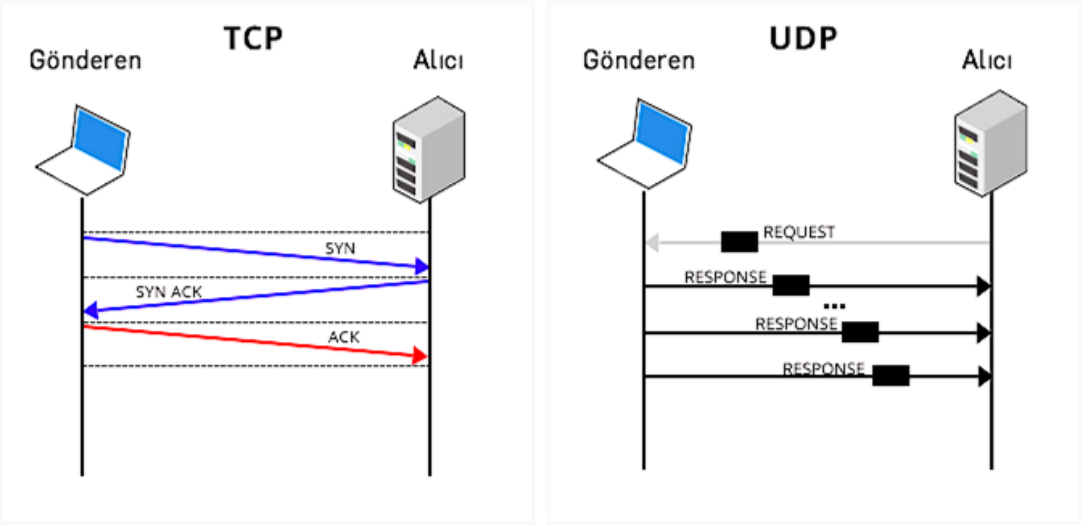
Yaygın UDP Tabanlı Saldırılar

UDP'nin hızı çeşitli şekillerde sömürülebilir:

1. UDP Taşkın Saldırısı: Saldırganlar, bir sunucuyu sayısız UDP paketi ile boğar ve sunucunun hata mesajlarıyla yanıt vermesine neden olur ve bu da sunucunun çökmesine veya yavaşlamasına yol açabilir.
2. DNS Güçlendirme Saldırısı: Saldırganlar, sahte bir kurbanın IP adresini içeren küçük UDP istekleri gönderir, bu da büyük yanıtların kurbanın üzerine yağmasına ve boğulmasına neden olur.

3. UDP Port Tarayıcı: Saldırganlar, çeşitli portlara UDP paketleri göndererek hangi portların açık olduğunu keşfeder. Açık portlar daha sonra diğer saldırılar için hedef alınabilir.

TCP ve UDP Farklılıkları



1. Bağlantı:
    - TCP (İletim Kontrol Protokolü): Bağlantı odaklıdır. Veri transferine başlamadan önce gönderici ve alıcı arasında bir bağlantı kurar.
    - UDP (Kullanıcı Datagram Protokolü): Bağlantısızdır. Bağlantı kurmadan veya alıcının hazır olup olmadığını kontrol etmeden veri gönderir.
2. Güvenilirlik:
    - TCP: Güvenilirdir. Veri paketlerinin sırayla, tekrar olmadan veya kaybolmadan teslim edilmesini sağlar, onaylamalar ve yeniden gönderimler kullanır.
    - UDP: Güvenilmezdir. Teslimat, sıralama veya hata kontrolü garanti edilmez. Paketler kaybolabilir veya sırayla gelmeyebilir.
3. Hız:
    - TCP: Bağlantı kurulumu, hata kontrolü ve yeniden gönderimler nedeniyle daha yavaştır.
    - UDP: Bağlantı kurulumu ve hata kontrolü süreçlerini atladığı için daha hızlıdır.
4. Hata Yönetimi:
    - TCP: Onaylamalar ve yeniden gönderimler ile hata düzeltme sağlar. Veri bütünlüğünü ve doğru sıralamayı garanti eder.
    - UDP: Minimum hata kontrolü sağlar ve hata düzeltme veya paket sıralama işlemi yapmaz. Sadece kontrol toplamları (checksums) kullanır.
5. Kullanım Alanları:

    - TCP: Güvenilirliğin kritik olduğu uygulamalarda kullanılır, örneğin web tarayıcılığı (HTTP/HTTPS), e-posta (SMTP/IMAP) ve dosya transferleri (FTP).
    - UDP: Hızın güvenilirlikten daha önemli olduğu zaman duyarlı uygulamalarda kullanılır, örneğin video akışı, VoIP ve çevrimiçi oyunlar.
6. Aşırı Yük:
    - TCP: Bağlantı yönetimi, hata kontrolü ve yeniden gönderimler nedeniyle daha yüksek aşırı yük (overhead) gerektirir.
    - UDP: Bağlantı yönetimi ve hata kurtarma mekanizmalarının eksikliği nedeniyle daha düşük aşırı yük gerektirir.
7. Veri Sıralaması:
    - TCP: Veri paketlerinin gönderildikleri sırayla alındığından emin olur.
    - UDP: Paketlerin sıralamasını garanti etmez, bu yüzden paketler sırasız olarak gelebilir.

Kaynaklar

- Somani, S. (2023, 23 Ekim). *TCP ve UDP: Farkları anlama*. Scaler. https://www.scaler.com/topics/computer-network/tcp-vs-udp/
- Karel. (2023, 1 Eylül). *TCP ve UDP arasındaki farklar nedir?* Karel. https://www.karel.com.tr/bilgi/tcp-ve-udp-arasindaki-farklar-nedir
- Cloudflare. (t.y.). *Kullanıcı Datagram Protokolü (UDP)*. 2 Eylül 2024 tarihinde erişildi, https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/
- JavaTpoint. (t.y.). *UDP protokolü*. 2 Eylül 2024 tarihinde erişildi, https://www.javatpoint.com/udp-protocol
- HAProxy. (2024, 13 Mayıs). *Kullanıcı Datagram Protokolü (UDP) nedir?* HAProxy. https://www.haproxy.com/glossary/what-is-user-datagram-protocol-udp
- Allied Telesis. (t.y.). *TCP nedir?* Allied Telesis. 2 Eylül 2024 tarihinde erişildi, https://www.alliedtelesis.com/tr/en/foundations/what-is-tcp
- Pramatarov, M. (2023, 22 Kasım). *TCP: Transmission Control Protocol—Nedir ve nasıl çalışır?* CloudNS. https://www.cloudns.net/blog/tcp-transmission-control-protocol-what-is-it-and-how-does-it-work/
- Kaspersky. (t.y.). *IP adresi nedir?* Kaspersky. 2 Eylül 2024 tarihinde erişildi, https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address
- Cloudflare. (t.y.). *Internet Protokolü*. 2 Eylül 2024 tarihinde erişildi, https://www.cloudflare.com/learning/network-layer/internet-protocol/
- Network Lessons. (t.y.). *IP yönlendirme açıklaması*. 2 Eylül 2024 tarihinde erişildi, https://networklessons.com/cisco/ccna-routing-switching-icnd1-100-105/ip-routing-explained