TCP ve UDP: Saldırganın ve Savunmacının Gözünden İki Farklı Ağ Felsefesi.

Hazırlayan : Muhammed Emin Öztekin

Bu sunumda, Ağ iletişiminin temelini oluşturan TCP ve UDP protokollerini, yalnızca teknik özellikleriyle değil; saldırgan ve savunmacı bakış açılarıyla ele alacağız.

KONU BAŞLIKLARI

1.TCP Nedir ?

2.UDP Nedir ?

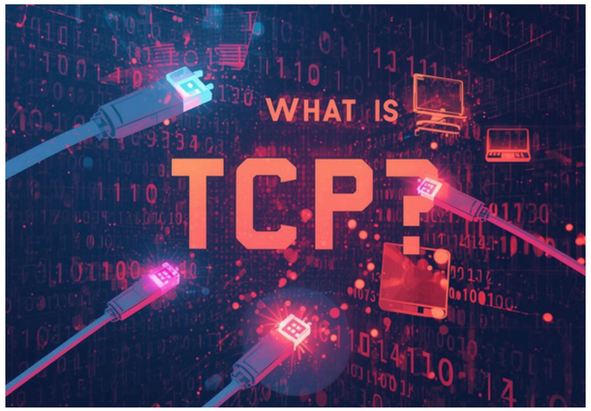
3.Güvenilirlik ve Hız : TCP ve UDP'nin temel yaklaşımı nasıl ?

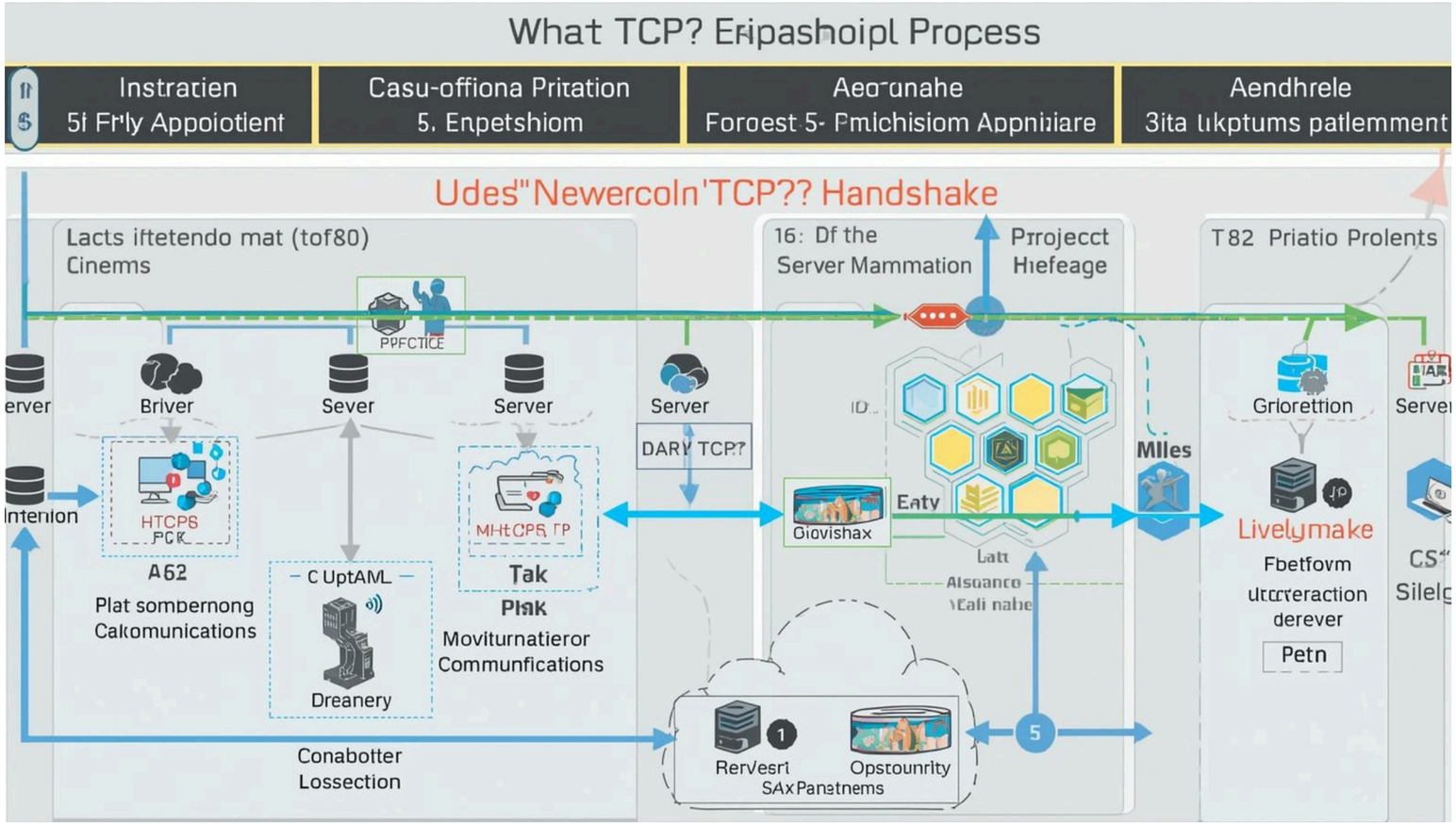
4.Bu iki protokol siber güvenlik senaryolarını nasıl şekillendiriyor ?

5.DNS gibi servisler neden UDP'yi tercih eder?

TCP NEDİR ?

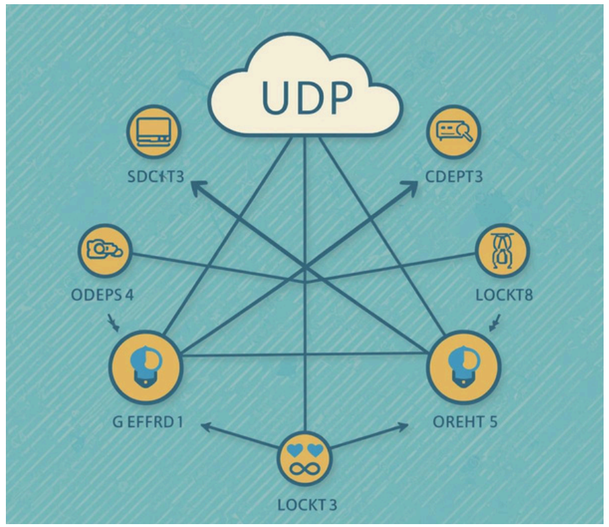
TCP (Transmission Control Protocol), iki sistem arasında bağlantı kurarak, gönderilen verilerin eksiksiz, doğru sırada ve güvenli biçimde iletilmesini sağlayan bir ağ protokolüdür. Veri kaybını kontrol eder, gerekirse paketleri yeniden gönderir ve iletişim süresince durumu takip eder.

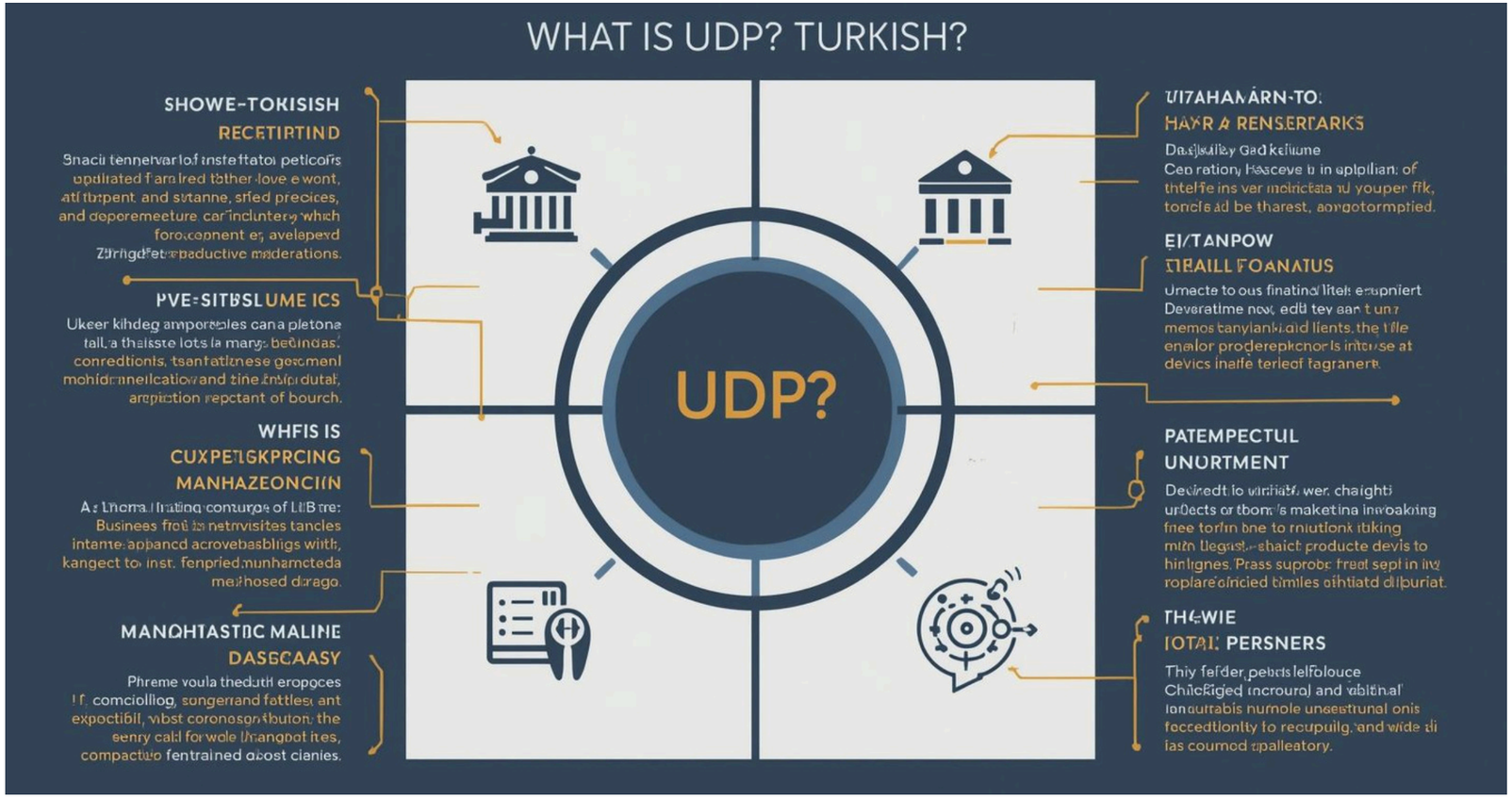




UDP NEDİR ?

UDP (User Datagram Protocol), bağlantı kurmadan çalışan, verilerin hedefe ulaşıp ulaşmadığını kontrol etmeyen hız odaklı bir ağ protokolüdür. Düşük gecikme sağladığı için gerçek zamanlı iletişimlerde tercih edilir.





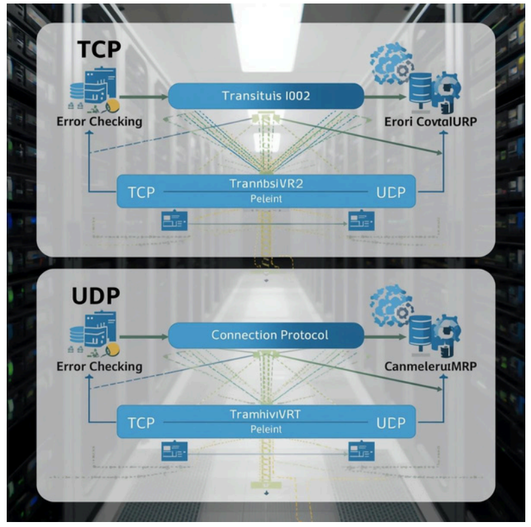
Güvenilirlik ve Hız : TCP ve UDP’nin temel yaklaşımı nasıl ?

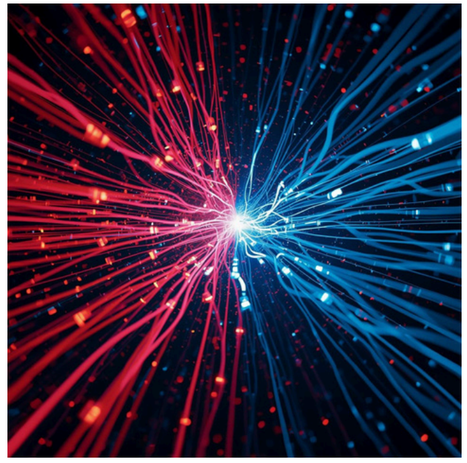
TCP – Güvenilirlik Odaklı Yaklaşım:

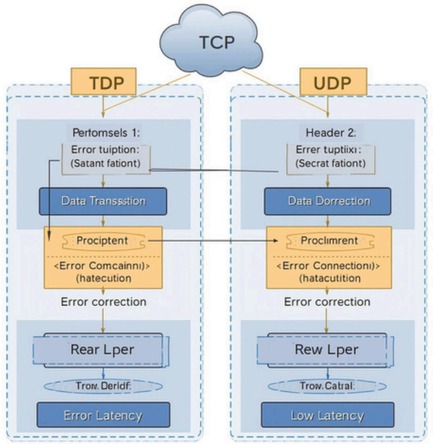
TCP, iletişim başlamadan önce bağlantı kurar ve gönderilen verilerin doğru sırayla, eksiksiz ulaştığını sürekli kontrol eder. Kayıp paketleri yeniden ileterek veri bütünlüğünü ön planda tutar; bu nedenle güvenilirliğin kritik olduğu durumlarda tercih edilir.

UDP – Hız Odaklı Yaklaşım:

UDP, bağlantı kurmadan veri gönderir ve iletimin durumunu takip etmez. Bu sayede gecikme minimuma iner ve hızlı iletişim sağlanır. Anlık veri akışının önemli olduğu senaryolarda hız, güvenilirliğin önüne geçer.



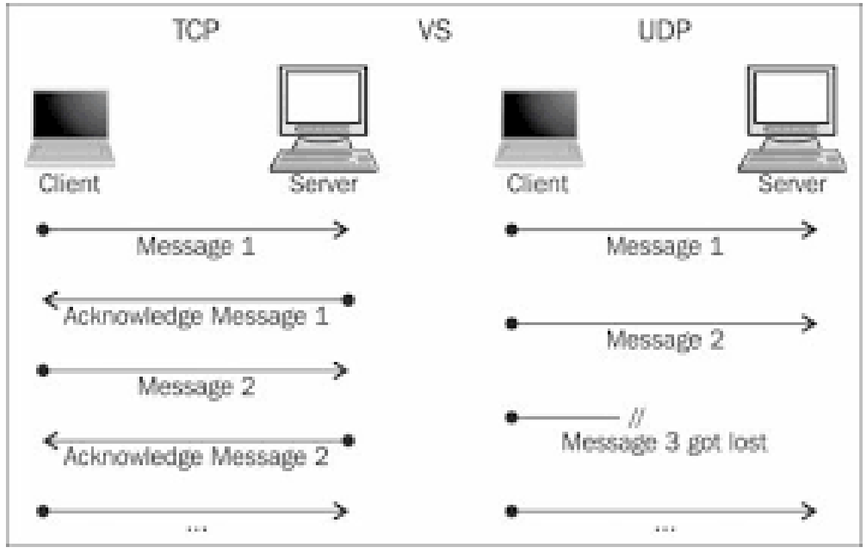


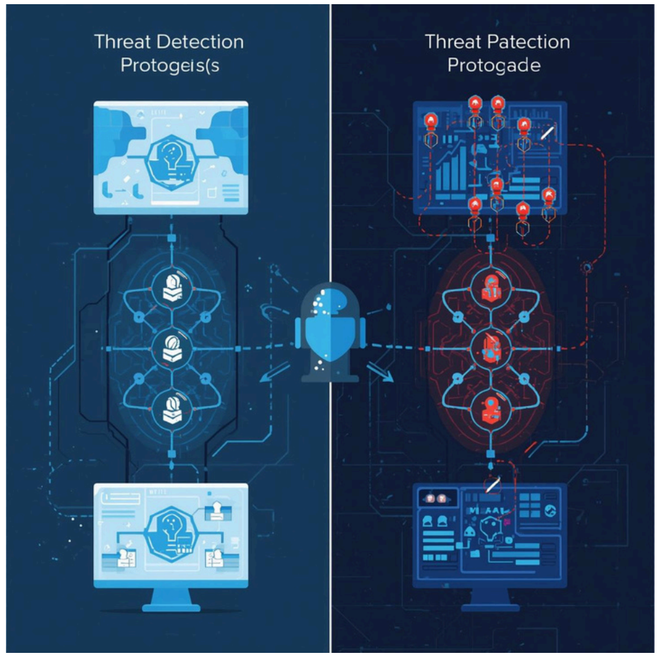


Bu iki protokol siber güvenlik senaryolarını nasıl şekillendiriyor ?

TCP ve UDP’nin temel çalışma prensipleri, siber güvenlikte hem saldırı hem de savunma yaklaşımlarını doğrudan etkiler. TCP’nin bağlantı kurma ve durum takibi yapan yapısı, SYN Flood gibi hedef sistemin kaynaklarını tüketmeye yönelik saldırıların ortaya çıkmasına zemin hazırlar. Bu tür saldırılarda, TCP’nin güvenilirlik için tasarlanmış mekanizmaları bir zafiyet haline gelebilir.

UDP ise bağlantısız ve doğrulama içermeyen yapısı nedeniyle hacim tabanlı saldırılarda öne çıkar. DNS Amplification gibi saldırılarda, küçük isteklerle büyük yanıtlar üretilerek hedef sistemler zorlanır. Port taramaları açısından bakıldığında, TCP daha net ve izlenebilir sonuçlar sunarken, UDP'nin sessizliği hem saldırganlar için avantaj hem de savunmacılar için tespiti zor bir risk alanı oluşturur. Bu nedenle TCP ve UDP, siber güvenlik senaryolarının şekillenmesinde belirleyici iki farklı yaklaşımı temsil eder.





Neden DNS gibi kritik servisler UDP’yi tercih eder ve bu durum siber güvenlikte nasıl bir risk oluşturur?

DNS gibi kritik servisler, çok kısa sürede çok sayıda isteğe yanıt vermek zorunda oldukları için UDP’yi tercih eder. Bağlantı kurma süreci olmadan çalışması, gecikmeyi azaltır ve sistemin yüksek performansla hizmet vermesini sağlar. Ancak bu tercih, kaynak doğrulaması ve bağlantı kontrolü olmadığı için IP spoofing ve DNS Amplification gibi saldırılara zemin hazırlar. Bu da UDP tabanlı servisleri hacim odaklı DDoS saldırıları açısından daha riskli hale getirir.