Modern Web Altyapılarında Güvenlik Analizi ve Süreç Raporu

---

1 Bilgisayarın Yerel Ağ İletişim Süreci

1.1 Bilgisayar Açıldığında IP Adresi Tahsisi

- Bilgisayar açıldığında, işletim sistemi ağ arayüzünü başlatır ve IP adresi almak için **DHCP Discover** yayını (broadcast) yapar.
- Ağdaki DHCP sunucusu, **DHCP Offer** paketi ile uygun bir IP adresi ve ağ yapılandırmasını sunar.
- Bilgisayar, **DHCP Request** paketi ile bu teklifi kabul ettiğini bildirir.
- DHCP sunucusu, **DHCP Ack** ile bu adresin tahsis edildiğini bildirir.

Güvenlik Sorunu: DHCP Spoofing

- Kötü niyetli bir cihaz, sahte DHCP sunucusu gibi davranarak bilgisayarlara yanlış ağ yapılandırması verebilir.

Çözüm:

- **DHCP Snooping** özelliği aktif edilerek sadece yetkili DHCP sunucularına izin verilir.
- Port güvenliği sağlanmalıdır.

1.2 ARP Protokolü (Adres Çözümleme Protokolü)

- Bilgisayar, ağdaki diğer cihazların MAC adreslerini öğrenmek için **ARP Request** yayını yapar.
- Hedef cihaz, kendi MAC adresini içeren **ARP Reply** ile yanıt verir.

Güvenlik Sorunu: ARP Spoofing/Poisoning

- Saldırgan, sahte ARP cevapları göndererek trafiği üzerine çekebilir (Man-in-the-Middle).

Çözüm:

- **ARP Spoofing Detection** araçları kullanılmalı.
- Statik ARP kayıtları tanımlanabilir.
- Güvenli anahtar yönetimi sağlanmalıdır.

1.3 DNS Sorgulama Süreci

- Bilgisayar, bir alan adı çözmek istediğinde önce **hosts** dosyasına bakar.
- Çözümleme bulunamazsa, **Recursive DNS Server** üzerinden isim çözümleme başlatılır.
- Alan adının hangi IP'ye karşılık geldiği öğrenilir.

Güvenlik Sorunu: DNS Spoofing & Cache Poisoning

- Saldırgan sahte DNS yanıtları ile kullanıcıyı sahte sitelere yönlendirebilir.

Çözüm:

- **DNSSEC** ile DNS kayıtlarının imzalanması.
- **Secure DNS Resolver** kullanımı.
- DNS sorgu loglarının izlenmesi.

1.4 TCP/IP İletişimi ve Three-Way Handshake

- İletişim öncesi, istemci ve sunucu arasında **SYN-SYN/ACK-ACK** şeklinde üç aşamalı el sıkışma gerçekleştirilir.
- NAT cihazları, iç IP ve portları dış IP ve portlara dönüştürerek internet erişimi sağlar.

Güvenlik Sorunu: SYN Flood (DDoS)

- Saldırgan sürekli sahte SYN paketleri göndererek hedef sistemin kaynaklarını tüketir.

Çözüm:

- **SYN Cookies** kullanımı.
- Rate Limiting ve DoS koruma mekanizmaları.

---

2 Web Sunucusu ile İletişim Süreci

2.1 HTTP İstekleri ve TCP Katmanı

- Kullanıcı bir web sayfasını ziyaret ettiğinde:
  - **DNS çözümleme** yapılır.
  - **TCP el sıkışması** tamamlanır.
  - Sunucuya **HTTP GET/POST** istekleri iletilir.
- HTTP/2 veya HTTP/3 gibi modern protokoller, performans için kullanılabilir.

Güvenlik Sorunu: Sniffing ve Manipülasyon

- HTTP ile gönderilen veriler şifrelenmediği için araya giren saldırgan tarafından okunabilir ve değiştirilebilir.

Çözüm:

- **HTTPS kullanımı** (TLS 1.3 önerilir).
- HSTS ve Content Security Policy (CSP) uygulanması.

2.2 Firewall

- Web sunucusuna gelen/giden trafiği denetler.
- **DDoS Koruması**, **IP Whitelisting**, **GeoBlocking** gibi özellikler eklenebilir.

Güvenlik Sorunu: Yanlış Konfigürasyon

- Açık portlar ve zayıf kurallar saldırıya açık kapılar bırakabilir.

Çözüm:

- Minimum izin politikası (Least Privilege).
- Düzenli firewall log ve kural denetimi.
- Otomatik IP bloklama sistemleri.

2.3 Reverse Proxy ve Load Balancer

- Gelen talepler, **Reverse Proxy** tarafından karşılanır.
- Proxy, yükü birden çok sunucuya dağıtır (Load Balancing).
- Ayrıca SSL sonlandırma, önbellekleme ve kimlik doğrulama gibi işlemler de yapılır.

Güvenlik Sorunu: Header Manipülasyonu & Forwarded Attacks

- X-Forwarded-For header'ı manipüle edilerek IP Spoofing yapılabilir.

Çözüm:

- Güvenli proxy konfigürasyonu.
- Orijinal kaynak IP doğrulaması.

Modern Web Altyapısının Bileşenleri ve Görevleri

Bileşen	Görevi	Güvenlik Sorunu	Çözüm
Mikro Hizmetler	Servisleri bölüp yönetir	Zayıf API güvenliği	API Gateway kullanımı, JWT doğrulama
Veritabanı	Veri saklar	SQL Injection	Parametrik sorgu, WAF kullanımı
Redis/Session	Oturum yönetimi	Oturum hırsızlığı	Session hashing, timeout yönetimi
CDN	Statik dosya sunumu	Cache Poisoning	Signed URL, Cache kontrol
Load Balancer	Trafik dağıtımı	DDoS	Rate Limiting, IP Reputation
Firewall	Trafik filtresi	Yanlış yapılandırma	Düzenli denetim, log analizi
Reverse Proxy	SSL sonlandırma, önbellekleme	Header Spoofing	Güvenli header yönetimi

Güvenlik Özet Tavsiyeleri

Tüm iletişim HTTPS üzerinden yapılmalı.
DNS, ARP ve DHCP seviyesinde koruma mekanizmaları eklenmeli.

Tüm loglar merkezi olarak toplanmalı ve analiz edilmelidir.
İç ve dış trafiği izleyen bir IDS/IPS kullanılmalı.
WAF ile web uygulaması seviyesinde saldırılar engellenmeli.
API güvenliği için Rate Limit, IP Whitelist, Token doğrulama sağlanmalı.
Mikroservislerde kimlik doğrulama merkezi yapılmalı.
Veritabanı ve session servisleri, şifrelenmiş bağlantılar üzerinden erişilmeli.