RTB_Görev3

Ömer Özcan

28/03/2025

—

Yusuf Nas

Modern Web Altyapıları ve Güvenlik Analizi

1. Bilgisayar Açıldığında Başlayan Süreçler

İlk adım: IP Adresi Almak **(DHCP)**.

- **Nasıl Çalışır?**
  Bilgisayar ağa bağlanınca, "IP lazım, kim verecek?" diye bağırır (DHCP Discover). DHCP sunucusu "Al bu IP'yi" der (DHCP Offer). Bilgisayar "Tamam, kabul" diye cevap verir (DHCP Request), sonunda sunucu "Tamamdır, kullanabilirsin" der (DHCP Ack).
- **Riskler**:
  - **Sahte DHCP Sunucusu**: Biri sahte sunucu kurup bana yanlış IP ve DNS atayabilir. Örneğin, "google.com"a gittiğimde sahte bir siteye yönlendirilebilirim.
  - **MITM Saldırısı**: Tüm trafiğim saldırganın cihazından geçebilir.
- **Çözüm**:
  Ağ yöneticisi, switch'lere **DHCP Snooping** aktif ederek sahte sunucuları engeller. Ayrıca, ağa bağlanan cihazların kimliği **802.1X** ile doğrulanır.

ARP Protokolü

IP'm var, şimdi diğer cihazlarla nasıl iletişim kuracağım? İşte **ARP** devreye giriyor.

- **Nasıl Çalışır?**
  "192.168.1.1'in MAC adresi nedir?" diye sorarım (ARP Request). O cihaz "Benim MAC'im şu" diye cevaplar (ARP Reply).
- **Riskler**:
  - **ARP Poisoning**: Saldırgan sahte ARP mesajları göndererek bana "Ben gateway'im" diyebilir. Tüm internet trafiğim onun üzerinden geçer ve verilerim çalınabilir.

- **Çözüm**:
  Switch'lerde **Dynamic ARP Inspection** aktif edilir. Bu, ARP mesajlarını DHCP veritabanıyla karşılaştırıp sahte olanları engeller.

DNS Sorgulamaları

"google.com" yazdığımda nasıl IP'ye çevriliyor?

- **Adımlar**:
  1. Önce bilgisayarımın **hosts dosyası**na bakarım (bu dosyaya elle IP ekleyip site engelleyebilirim).
  2. Yerel DNS önbelleğimi kontrol ederim.
  3. DNS sunucusuna sorarım.
- **Riskler**:
  - **DNS Spoofing**: Saldırgan DNS önbelleğimi zehirleyerek "google.com"u kendi sunucusuna yönlendirebilir.
  - **DNS Hijacking**: DNS sunucusu ele geçirilirse tüm sorgular manipüle edilir.
- **Çözüm**:
  DNSSEC ile DNS cevapları dijital imzalanır. Ayrıca, tarayıcıda **DNS Over HTTPS (DoH)** kullanarak sorgularım şifrelenir.

TCP/IP İletişimi

IP ve MAC'i öğrendim, şimdi veri göndereceğim.

- **NAT Nedir?**
  Evdeki tüm cihazlar tek bir genel IP ile internete çıkar. NAT, iç IP'leri dışarıya maskeler.
- **TCP Handshake**:
  Sunucuya bağlanmak için 3 adım:
  1. **SYN**: "Merhaba, bağlanabilir miyim?"

2. **SYN-ACK**: "Tabii, buyur."
3. **ACK**: "Tamam, başlıyoruz!"

- **Riskler**:
  - **SYN Flood**: Saldırgan binlerce SYN gönderip sunucunun kaynaklarını tüketir.
  - **Session Hijacking**: Bağlantım ele geçirilirse verilerim çalınabilir.
- **Çözüm**:
  Sunucular **SYN Cookies** kullanarak sahte bağlantıları engeller.
  Ayrıca, **IPSec** ile trafik şifrelenir.

2. Web Sunucusu ile İletişim

HTTP İstekleri

Tarayıcıda bir siteye girdiğimde arka planda neler oluyor?

- **GET vs. POST**:
  - **GET**: URL'de parametreler görünür (örneğin arama sonuçları).
  - **POST**: Veri gizli olarak gönderilir (örneğin şifre).
- **Riskler**:
  - **SQL Injection**: "Kullanıcı adı" alanına ' OR 1=1 -- yazarsam veritabanı tüm kullanıcıları listeleyebilir.
  - **XSS**: Bir yorum alanına <script>alert('Hacked')</script> yazarsam, bu kod başkalarının tarayıcısında çalışır.
  - **CSRF**: Sahte bir linke tıklarsam, sitemdeki oturumumla para transferi yapılabilir.
- **Çözüm**:
  Geliştiriciler **input validation** yapmalı (örneğin, tüm veriler filtrelenmeli).
  Ayrıca, **Web Application Firewall (WAF)** SQLi ve XSS'i engeller.

Firewall & DDoS Koruması

Firewall, trafiği nasıl kontrol ediyor?

- **Türleri**:
  - **Stateless**: Sadece port ve IP'ye bakar.
  - **Stateful**: Bağlantı durumunu takip eder (örneğin, TCP handshake tamamlandı mı?).
- **DDoS Saldırıları**:
  - **Volumetric**: UDP flood ile bant genişliği doldurulur.
  - **Application Layer**: HTTP flood ile sunucu kaynakları tüketilir.
- **Çözüm**:
  Cloudflare gibi CDN'ler trafiği dağıtır. Ayrıca, **rate limiting** ile saniyede 100 istekten fazlası engellenir.

Reverse Proxy & Load Balancer

Büyük siteler nasıl yükü kaldırıyor?

- **Reverse Proxy**:
  - Trafiği arka uç sunuculara dağıtır.
  - SSL şifrelemesini üstlenerek sunucuları rahatlatır.
- **Load Balancer**:
  - **Round Robin**: İstekleri sırayla sunuculara gönderir.
  - **Least Connections**: En az meşgul sunucuyu seçer.
- **Riskler**:
  - **HTTP Request Smuggling**: Yanlış yapılandırılmış proxy'ler, saldırganın geçersiz istek göndermesine izin verir.
  - **SSL Stripping**: Saldırgan, HTTPS'yi HTTP'ye düşürebilir.

- **Çözüm**:
  HSTS ile tarayıcıların sadece HTTPS kullanması zorunlu kılınır. Ayrıca, header'lar sıkı bir şekilde kontrol edilir.

3. Modern Web Altyapısı

Mikro Hizmetler & Veritabanı

Monolitik yapı yerine neden mikro hizmetler?

- **Avantaj**: Her hizmet bağımsız çalışır.
- **Riskler**:
  - **API Güvenliği**: Her mikro hizmetin API'si ayrı bir saldırı noktasıdır.
  - **Veritabanı Açıkları**: NoSQL Injection (örneğin, MongoDB'de $where manipülasyonu).
- **Çözüm**:
  JWT Token ile API'lere erişim kontrolü. Ayrıca, **RBAC** (Role-Based Access Control) kullanılır.

CDN & Statik Dosyalar

CDN'ler neden önemli?

- **İşlev**: Görselleri ve CSS/JS dosyalarını kullanıcıya en yakın sunucudan dağıtır.
- **Riskler**:
  - **Subdomain Takeover**: "cdn.sirket.com" boşsa, saldırgan bu subdomain'i ele geçirip zararlı içerik yükleyebilir.
  - **Cache Poisoning**: CDN önbelleğine sahte bir sayfa yerleştirilirse, tüm kullanıcılar zararlı içerik görür.
- **Çözüm**:
  DNS kayıtları düzenli kontrol edilir. Ayrıca, **Signed URLs** ile dosya erişimleri kısıtlanır.

Scalability (Ölçeklenebilirlik)

Trafik arttığında nasıl ölçeklenir?

- **Horizontal Scaling**: Sunucu sayısı artırılır (bulutta otomatik ölçeklendirme).
- **Vertical Scaling**: Mevcut sunucunun RAM/CPU'su yükseltilir.
- **Riskler**:
    - **Auto-Scaling Exploit**: Sahte trafikle sunucu sayısı artırılıp maliyet şişirilebilir.
- **Çözüm**:
  Health Check ile sağlıksız sunucular devre dışı bırakılır. Ayrıca, **Quota Management** ile limitler konur.

4. Gerçek Dünya Senaryoları ve Dersler

- **Equifax Veri İhlali (2017)**: Apache Struts'taki bir açık, 147 milyon kişinin verisinin çalınmasına neden oldu. **Öğrenilen**: Yama yönetimi hayati önemde!
- **GitHub Subdomain Takeover (2018)**: Boş bir subdomain ele geçirilerek phishing yapıldı. **Öğrenilen**: Kullanılmayan DNS kayıtları silinmeli.
- **Capital One İhlali (2019)**: AWS yapılandırma hatasıyla 100 milyon müşteri verisi sızdırıldı. **Öğrenilen**: IAM politikaları sıkılaştırılmalı.