DNS'in DETAYLARI

Kaynak

İÇERİK

DNS: İnternetin Adres Defteri (Temeller ve Mantık)

İnternet dünyasında cihazların birbirini bulabilmesi için kullanılan en temel mekanizma **DNS (Domain Name System - Alan Adı Sistemi)** yapısıdır. Bir siber güvenlik uzmanı veya sistem yöneticisi için DNS'in nasıl çalıştığını bilmek, sadece web sitelerine girmek değil; ağ trafiğini analiz etmek, **Exfiltration** (veri sızdırma) tekniklerini anlamak veya **Man-in-the-Middle** (aradaki adam) saldırılarını kavramak için kritiktir.

DNS Neden Var? (İnsan vs. Makine Mantığı)

İnternete bağlı olan her cihazın, tıpkı fiziksel dünyadaki ev adresleri gibi, kendine has bir kimlik numarası vardır. Buna **IP Adresi (Internet Protocol Address)** diyoruz.

- **IP Adresi Yapısı:** Standart bir IPv4 adresi, noktalarla ayrılmış, 0 ile 255 arasında değişen 4 rakam grubundan oluşur.
  - *Örnek:* `104.26.10.229`

Problem: Bir insan olarak her gün girdiğimiz onlarca sitenin (Google, TryHackMe, banka adresleri vb.) bu karmaşık numara dizilerini ezberlememiz imkansızdır.

Çözüm: DNS, bu karmaşık IP adreslerini `tryhackme.com` gibi akılda kalıcı, sözel **Alan Adları (Domain Names)** ile eşleştirir. Yani DNS, internetin devasa bir "telefon rehberidir". Siz tarayıcıya bir isim yazarsınız, DNS arka planda bu ismin hangi numaraya (IP) karşılık geldiğini bulur ve sizi oraya yönlendirir.

Teknik Detaylar ve İşleyiş Mantığı

Bir alan adını tarayıcıya yazdığınızda süreç şu mantık zinciriyle ilerler:

1. **Sorgu Başlatma:** Bilgisayarınız önce kendi yerel belleğine (**DNS Cache**) bakar. Eğer daha önce bu siteye gittiyse adresi hatırlar.
2. **Çözümleme (Resolution):** Eğer bilgisayar adresi bilmiyorsa, bu soruyu bir **DNS Resolver**'a (genelde internet servis sağlayıcınızın sunucusu) sorar.

3. **Hiyerarşik Arama:** Sistem, en üstten başlayarak (Root Hint, TLD gibi) doğru IP adresini bulana kadar sorgu yapar.

IP Adresi Aralıkları Hakkında Not

IP adreslerinin her bir bölümü (oktet) **0-255** arasındadır. Bunun sebebi, her bir bölümün 8 bitlik bir alanı temsil etmesidir (2^8 2 kombinasyon). Eğer bir analiz sırasında bu aralık dışında bir rakam görürseniz (örneğin `192.168.1.300`), bu geçersiz bir IP yapılandırmasıdır ve bağlantı kurulamaz.

Özet Vurgu

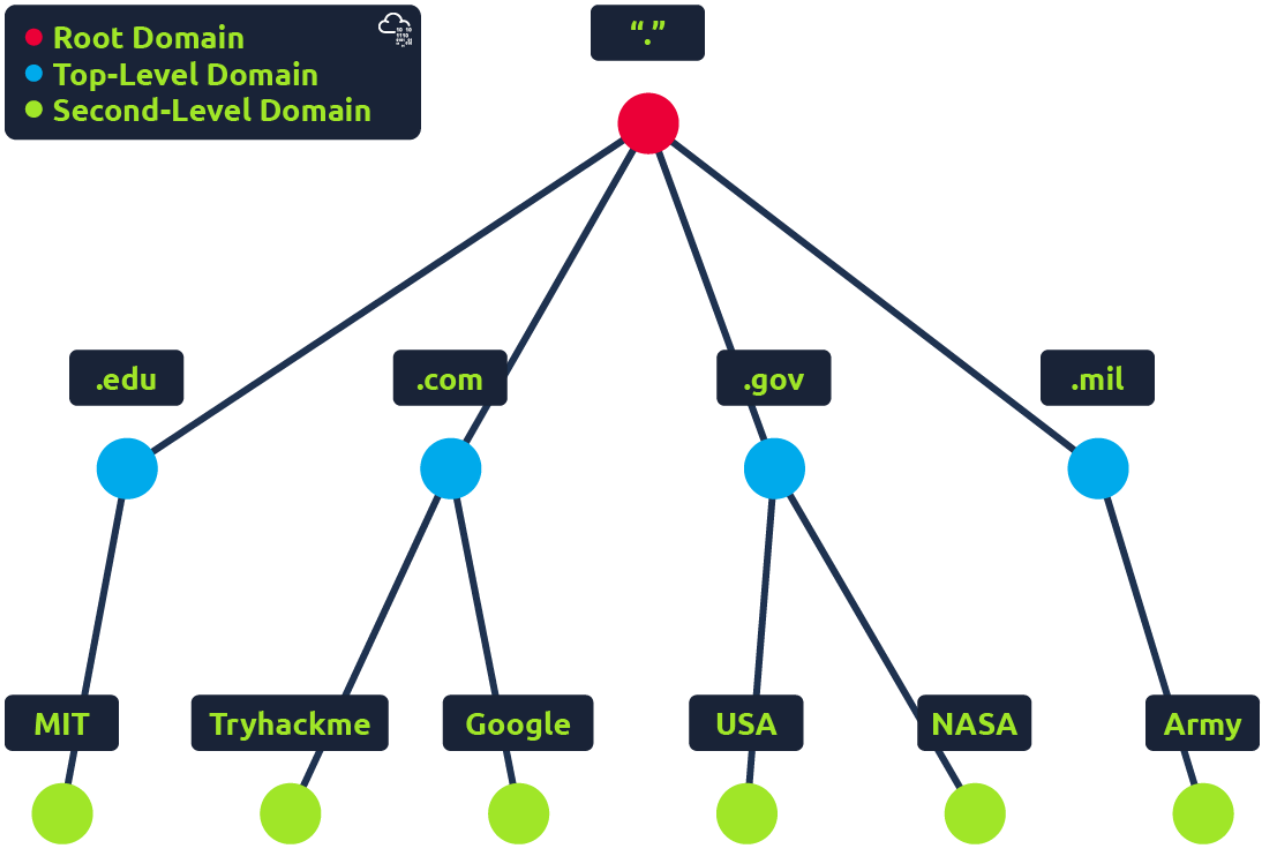
- **Domain Name:** İnsanların okuyabildiği adres (`tryhackme.com`).
- **IP Address:** Makinelerin birbirini tanıdığı gerçek sayısal adres (`104.26.10.229`).
- **DNS:** Bu ikisi arasındaki tercüman.

Bu temel yapıyı bilmek, ileride göreceğimiz **DNS Enumeration** (DNS üzerinden bilgi toplama) aşamasında hangi kayıtların (A, AAAA, MX, TXT) ne işe yaradığını anlamamız için temel taşıdır.

Alan Adı Hiyerarşisi (Domain Hierarchy)

DNS dünyasını anlamak için bir alan adının yapısını sağdan sola doğru, yani hiyerarşinin en üstünden en altına doğru incelemek gerekir. Her nokta (`.`) aslında bir hiyerarşik katmanı temsil eder. Bir siber güvenlikçi için bu yapıyı bilmek, **subdomain discovery** (alt alan adı keşfi) yaparken veya **phishing** (oltalama) saldırılarındaki ufak harf oyunlarını yakalarken

hayati önem taşır.



1. TLD (Top-Level Domain - Üst Düzey Alan Adı)

Bir alan adının en sağında bulunan kısımdır. Hiyerarşinin en tepesini (Kök dizinden hemen sonraki adım) temsil eder. Örneğin, `tryhackme.com` adresinde TLD kısmı **.com** ifadesidir.

TLD'ler kendi içinde iki ana gruba ayrılır:

- **gTLD (Generic Top-Level Domains):** Amacı, sitenin neyle ilgili olduğunu kullanıcıya bildirmektir.
  - `.com` : Ticari (Commercial) amaçlı.
  - `.org` : Organizasyonlar/Vakıflar (Organization) için.
  - `.edu` : Eğitim kurumları (Education) için.
  - `.gov` : Devlet kurumları (Government) için.
  - *Not:* Günümüzde talepten dolayı `.online` , `.club` , `.biz` gibi çok sayıda yeni gTLD türetilmiştir.
- **ccTLD (Country Code Top-Level Domains):** Coğrafi konumu veya ülkeyi belirtmek için kullanılır.
  - `.ca` : Kanada merkezli siteler.
  - `.co.uk` : Birleşik Krallık merkezli siteler.
  - `.tr` : Türkiye merkezli siteler.

2. Second-Level Domain (İkinci Düzey Alan Adı)

TLD'nin hemen solunda yer alan, genellikle marka veya kurum isminin bulunduğu kısımdır. `tryhackme.com` örneğinde **tryhackme** kısmı Second-Level Domain'dir.

Kayıt Kuralları ve Kısıtlamalar: Bir alan adı satın alırken (register ederken) uyman gereken teknik kurallar şunlardır:

- **Uzunluk:** TLD hariç en fazla **63 karakter** olabilir.
- **Karakter Seti:** Sadece `a-z`, `0-9` ve **tire (-)** kullanılabilir.
- **Tire Kuralı:** Alan adı tire ile başlayamaz, tire ile bitemez ve ardışık iki tire (--) içeremez.

3. Subdomain (Alt Alan Adı)

Second-Level Domain'in soluna eklenen ve bir nokta ile ayrılan kısımdır. Genellikle ana sitenin farklı bölümlerini (admin paneli, blog, mail sunucusu vb.) ayırmak için kullanılır.

- **Örnek:** `admin.tryhackme.com` adresinde **admin** kısmı subdomain'dir.
- **İç İçe Geçmiş Subdomainler:** Birden fazla subdomain noktalarla birleştirilebilir.
  - *Örnek:* `jupiter.servers.tryhackme.com`
  - Burada `jupiter`, `servers` subdomain'inin bir parçasıdır.

Teknik Sınırlar:

- **Karakter Kısıtlaması:** İkinci düzey alan adıyla aynıdır (63 karakter sınırı, tire kuralları, sadece alfanümerik karakterler).
- **Toplam Uzunluk:** Bir alan adının tamamı (subdomain + domain + TLD) toplamda **253 karakteri** geçemez.
- **Sayı Sınırı:** Bir alan adı için oluşturabileceğin subdomain sayısında teknik bir üst sınır yoktur.

Önemli Not: Neden Subdomain Araması (Enumeration) Yapıyoruz?

Sızma testlerinde (Pentest) bir hedefi incelerken `www.hedef.com` çok güvenli olabilir. Ancak saldırganlar `dev.hedef.com` (geliştirme aşamasındaki site) veya `test.hedef.com` gibi unutulmuş subdomainleri ararlar. Bu gizli kalmış alanları bulmak, genellikle **güvenlik duvarı (WAF)** arkasında olmayan veya güncellenmemiş eski sunuculara erişmemizi sağlar.

DNS Kayıt Türleri (Record Types)

DNS sadece web sitelerinin IP adreslerini tutmakla kalmaz; e-posta yönlendirmelerinden güvenlik doğrulamalarına kadar birçok farklı işlevi yerine getiren farklı **kayıt türlerine (Record Types)** sahiptir. Bir siber güvenlik analizinde, hedef domain üzerindeki bu kayıtları incelemek (DNS Enumeration), saldırı yüzeyini belirlemek için atılan ilk adımdır.

En sık karşılaşacağın ve mutlaka bilmen gereken kayıt türleri şunlardır:

1. A Kaydı (Address Record)

En temel DNS kayıt türüdür. Bir alan adını doğrudan bir **IPv4** adresine bağlar.

- **Görevi:** "Bu isim hangi bilgisayara (IP'ye) ait?" sorusuna yanıt verir.
- **Örnek:** `tryhackme.com` sorgusu yapıldığında dönen `104.26.10.229` cevabı bir A kaydıdır.

2. AAAA Kaydı (IPv6 Address Record)

A kaydı ile tamamen aynı mantıkta çalışır, ancak IPv4 yerine **IPv6** adreslerini çözümlemek için kullanılır.

- **Neden Farklı?:** IPv4 adresleri dünya genelinde tükendiği için daha uzun ve karmaşık olan IPv6 sistemine geçilmiştir.
- **Örnek:** `2606:4700:20::681a:be5` gibi bir çıktı alıyorsan bu bir AAAA kaydıdır.

3. CNAME Kaydı (Canonical Name Record)

Bir alan adını başka bir alan adına yönlendirmek (alias/takma ad) için kullanılır. Bu kayıt türünde doğrudan bir IP adresi dönmez, bunun yerine başka bir domain ismi döner.

- **İşleyiş Mantığı:** 1. Kullanıcı `store.tryhackme.com` adresine gitmek ister. 2. DNS sunucusu cevap olarak: "Bu adresin IP'si bende yok, sen git `shops.shopify.com` adresine sor" der (CNAME yanıtı). 3. Bilgisayar bu sefer gider `shops.shopify.com` için yeni bir DNS sorgusu yapar ve gerçek IP'ye ulaşır.
- **Kullanım Amacı:** Özellikle Shopify, AWS S3 veya CDN gibi üçüncü parti hizmetleri kendi subdomain'in üzerinden çalıştırmak istediğinde kullanılır.

4. MX Kaydı (Mail Exchange Record)

İlgili domain adına gelen e-postaların hangi sunuculara yönlendirileceğini belirtir.

- **Örnek:** `tryhackme.com` için bir MX sorgusu yaptığında `alt1.aspmx.l.google.com` gibi bir sunucu adresi döner.
- **Priority (Öncelik) Flag:** MX kayıtlarının yanında her zaman bir sayı (öncelik değeri) bulunur.
  - Sayı ne kadar **küçükse**, o sunucu o kadar önceliklidir.
  - **Mantık:** Eğer ana sunucu çökerse, e-postalar kaybolmasın diye bir sonraki (daha yüksek sayılı) yedek sunucuya yönlendirilir.

5. TXT Kaydı (Text Record)

İçerisinde herhangi bir metin verisi barındırabilen, "özgür yazım" alanlarıdır. Siber güvenlik ve sistem yönetimi açısından iki kritik kullanım alanı vardır:

- **Spam ve Spoofing Engelleme:** `SPF`, `DKIM` veya `DMARC` gibi protokoller bu alana yazılır. Bu sayede, "Sadece şu IP'ler benim adıma mail gönderebilir" diyerek sahte e-

postaların önüne geçilir.
- **Mülkiyet Doğrulama:** Bir hizmete (örneğin Google Search Console) kayıt olurken, domainin gerçekten size ait olduğunu kanıtlamak için sizden TXT kaydına özel bir kod eklemeniz istenir.

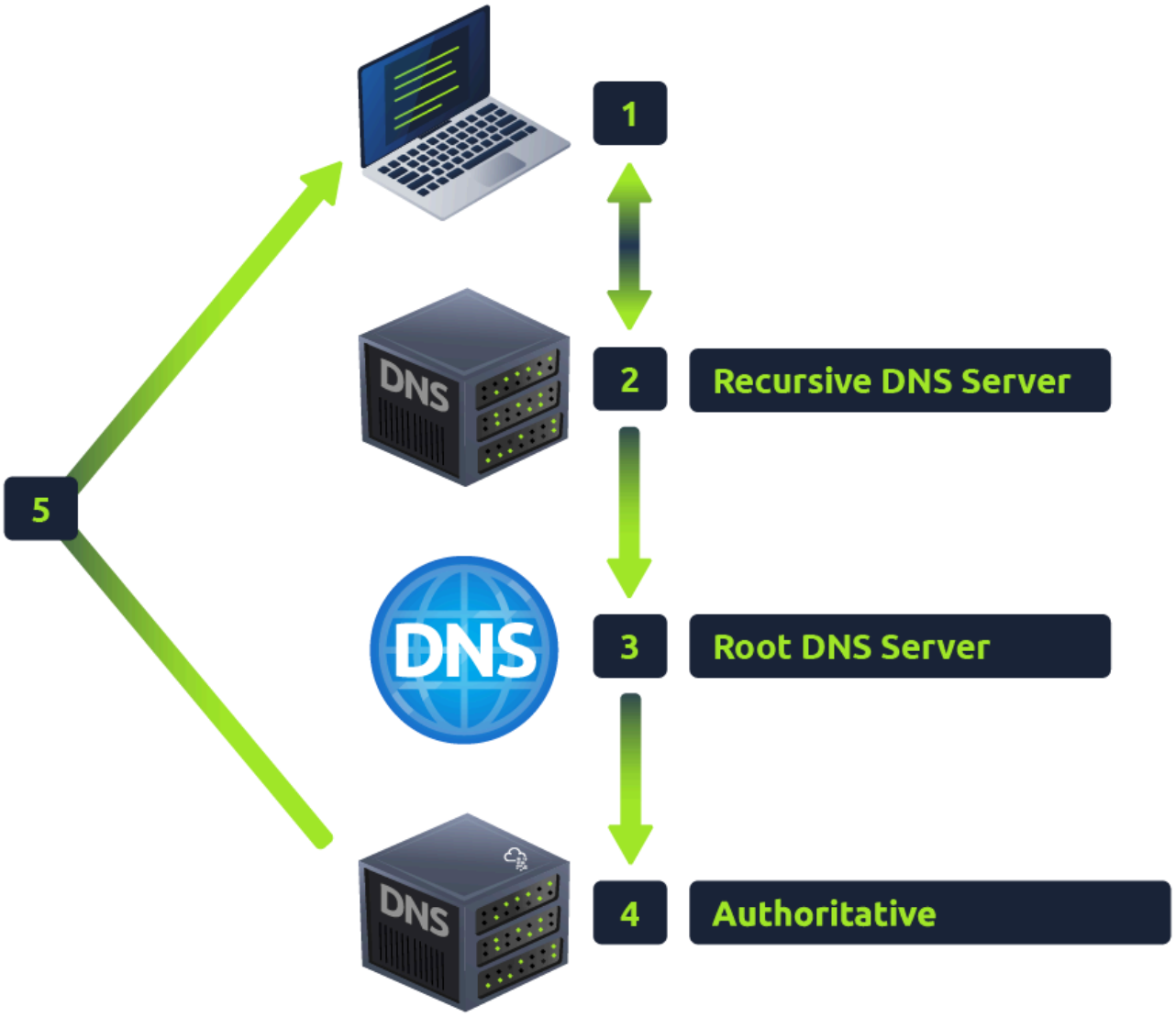
Bir Siber Güvenlikçi Gözüyle Neden Önemli?

- **A/AAAA:** Hedefin doğrudan IP adresini (saldırı yüzeyini) verir.
- **CNAME:** Hedefin hangi üçüncü parti servisleri (bulut sağlayıcılar vb.) kullandığını ifşa eder.
- **MX:** Şirketin mail altyapısını (Office 365 mi, Google mı, kendi sunucusu mu?) gösterir. Bu da **Phishing** (oltalama) senaryoları için kritik bilgidir.
- **TXT:** Sızma testlerinde bazen bu kayıtlarda unutulmuş şifreler, API anahtarları veya sunucu konfigürasyon detayları bulunabilir.

Bir DNS Sorgusu Nasıl Gerçekleşir? (Step-by-Step Request Journey)

Tarayıcına bir adres yazıp "Enter" tuşuna bastığında, arka planda milisaniyeler içinde gerçekleşen karmaşık bir trafik başlar. Bir siber güvenlikçi için bu süreci bilmek, **DNS Poisoning** (DNS zehirlemesi) gibi saldırıların hangi aşamada gerçekleşebileceğini anlamak adına kritiktir.

İşte bir DNS sorgusunun adım adım yolculuğu:



1. Yerel Kontrol: Cache (Önbellek) Mekanizması

Bilgisayarın dış dünyaya sormadan önce "Ben bunu zaten biliyor muyum?" diye kontrol eder.

- **Local Cache:** İşletim sistemin, yakın zamanda ziyaret ettiğin adreslerin IP karşılıklarını yerel belleğinde tutar.
- **Sonuç:** Eğer kayıt buradaysa, yolculuk başlar başlamaz biter.

2. Recursive DNS Resolver (Özyinelemeli Çözümleyici)

Eğer yerel bellekte yoksa, bilgisayarın bu soruyu **Recursive DNS Server**'a sorar.

- **Kimdir?:** Genellikle internet servis sağlayıcın (ISP) tarafından sağlanır (Ancak 8.8.8.8 - Google veya 1.1.1.1 - Cloudflare gibi servisleri de kullanabilirsin).
- **Görevi:** Senin adına tüm interneti gezip cevabı bulan "haberci"dir. Kendi belleğinde popüler siteler (Facebook, Google vb.) varsa direkt cevap verir; yoksa hiyerarşik sorgu sürecini başlatır.

3. Root Servers (Kök Sunucular)

Hiyerarşinin en tepesidir, internetin omurgasını oluştururlar.

- **Görevi:** IP adresini bilmezler ama seni **kimin bildiğine** yönlendirirler.
- **Mantık:** Sen `www.tryhackme.com` adresini sorduğunda, Root Server sondaki **.com** uzantısına bakar ve seni ilgili **TLD Server**'a (Top Level Domain) yönlendirir.

4. TLD Nameservers (Üst Düzey Alan Adı Sunucuları)

Uzantılara göre özelleşmiş sunuculardır (.com, .org, .net, .edu gibi).

- **Görevi:** İlgili domainin (tryhackme) kayıtlarının hangi **Authoritative Nameserver** (Yetkili Sunucu) üzerinde tutulduğu bilgisini verir.

5. Authoritative Nameserver (Yetkili Sunucu)

Yolculuğun son durağıdır. Bu sunucu, ilgili domainin DNS kayıtlarının (A, MX, TXT vb.) asıl sahibidir.

- **Örnek:** `tryhackme.com` için bu sunucular `kip.ns.cloudflare.com` ve `uma.ns.cloudflare.com`'dur.
- **Yedeklilik:** Genellikle birden fazla yetkili sunucu bulunur; biri çökerse diğeri isteklere cevap vermeye devam eder.
- **Cevap:** IP adresi buradan alınır ve Recursive Resolver üzerinden sana geri gönderilir.

Kritik Kavramlar: TTL ve Caching

Sorgu bittiğinde, Recursive Resolver bu bilgiyi sana iletirken aynı zamanda kendi belleğine de kaydeder. Böylece bir sonraki kullanıcı aynı siteyi sorduğunda tüm interneti tekrar gezmek zorunda kalmaz.

- **TTL (Time To Live):** Her DNS kaydıyla birlikte gelen, saniye cinsinden bir "ömür" değeridir.
  - **Örnek:** TTL değeri 3600 ise, bu kayıt 1 saat boyunca önbellekte saklanır.
  - **Neden Önemli?:** Eğer bir sunucunun IP adresini değiştirirsen, dünyanın geri kalanının bu değişikliği görmesi TTL süresinin dolmasına bağlıdır (Buna **DNS Propagation** denir).

Özet Akış Şeması

`Bilgisayar` -> `Recursive Resolver` -> `Root Server` -> `TLD Server (.com)` -> `Authoritative Server (Cloudflare)` -> `IP Adresi Alındı!`