

SECURITY CHECK

ÖZET

Günümüzün hızla dijitalleşen dünyasında, siber tehditlere karşı zamanında bilgi edinmek ve doğru hamleleri yapmak her zamankinden daha kritik hale gelmiştir. Bu ihtiyaca yanıt vermek üzere geliştirilen **Security Check**, kullanıcılara kapsamlı güvenlik sorguları yapabilecekleri çok yönlü bir platform sunmaktadır. Nmap taramalarından Whois sorgularına, MX ve DMARC kayıt analizlerinden DNS ve kara liste (Blacklist) kontrollerine kadar birçok önemli aracı tek bir sistemde birleştirerek, hem bireysel kullanıcıların hem de kurumların dijital varlıklarını daha etkin koruyabilmelerini sağlamaktadır.

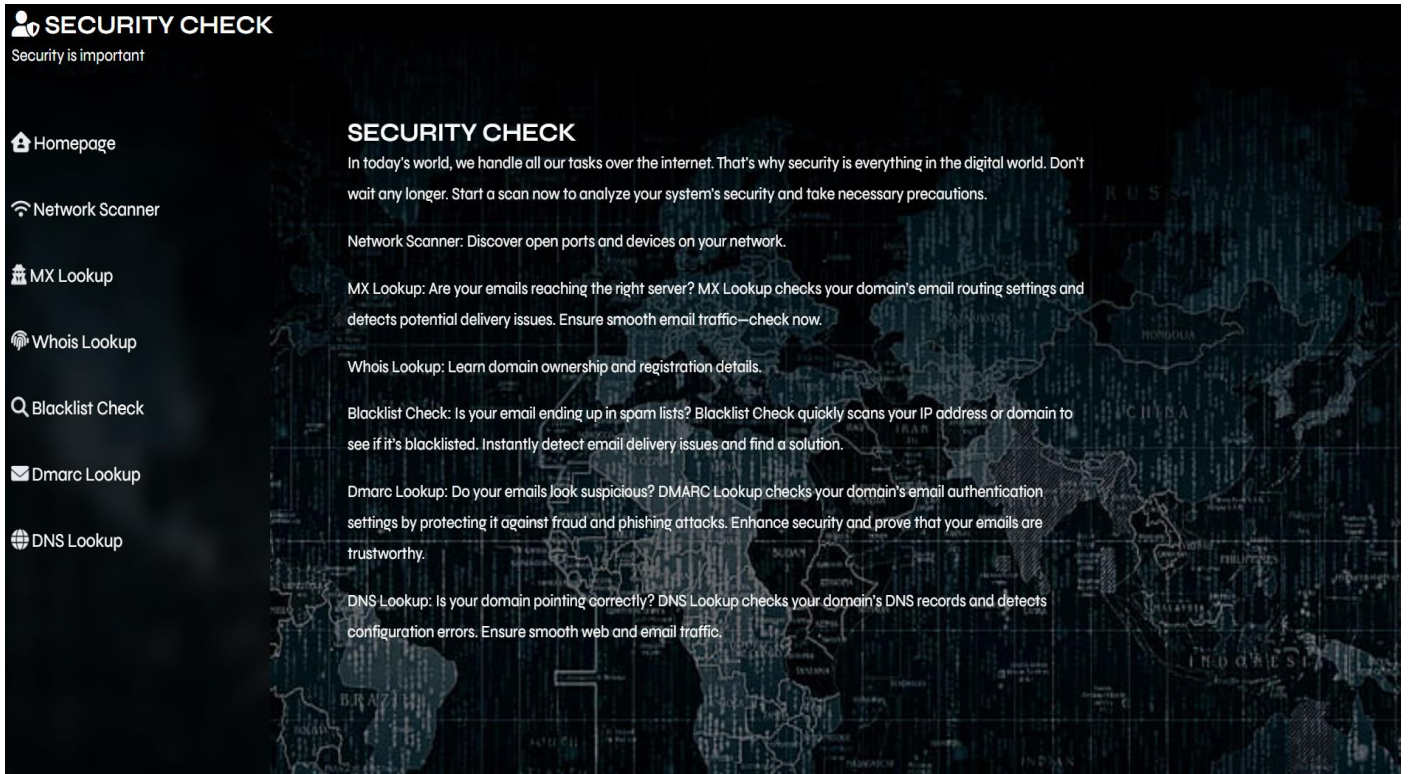
Bu çalışmada, Security Check platformunda yer alan araçlar detaylı şekilde açıklanmakta; her bir aracın temel işlevi, teknik ve pratik kullanım senaryoları, dijital güvenliğe katkıları sade ve anlaşılır bir dille ele alınmaktadır. Ayrıca, bu araçların etik siber güvenlik testlerinde (Nmap ile zafiyet analizi gibi) nasıl kullanılabileceği, spam gibi tehditlere karşı alınabilecek önlemler ve ağ sorunlarının tespiti gibi konulara da yer verilmiştir. Amacımız, teknik bilgi düzeyi ne olursa olsun herkesin siber güvenlik farkındalığını artırmak ve kendi dijital dünyalarını daha güvenli hale getirmelerine destek olmaktır.

GİRİŞ

İnternet, hayatımıza hız ve kolaylık kattığı kadar, görünmeyen birçok tehlikeyi de beraberinde getirmiştir. Bir alan adı veya IP adresi arkasında hangi bilgilerin bulunduğunu bilmeden dijital dünyada ilerlemek, adeta gözleri kapalı bir yolda yürümeye benzer. Kişisel verilerin korunması, kurumsal ağların güvenliği ve çevrimiçi kimliklerin doğrulanması gibi birçok konuda doğru bilgiye zamanında ulaşmak günümüzde kritik bir ihtiyaç haline gelmiştir.

Bu ihtiyaca yanıt vermek amacıyla geliştirilen **Security Check**, kullanıcıların dijital güvenliklerini sağlamlaştırmalarına yardımcı olmayı amaçlamaktadır. Platform üzerinden yapılan sorgular sayesinde bir web sitesinin açık portlarını keşfetmek, sahiplik bilgilerine ulaşmak, e-posta altyapılarını ve spam filtreleme sistemlerini analiz etmek, kara liste durumlarını kontrol etmek ve DNS altyapısal verilerini incelemek mümkün hale gelmektedir. Ayrıca, Nmap gibi araçlarla ağların zafiyet analizi yapılabilen ve bu sayede etik siber güvenlik testleri de desteklenmektedir.

Karmaşık güvenlik kontrollerini sadeleştirerek her seviyeden kullanıcının rahatlıkla erişebileceği bir sistem sunan platform, teknik bilgi düzeyi ne olursa olsun herkes için dijital güvenliği ulaşılabilir kılmaktadır. Bu makalede, Security Check platformunda sunulan güvenlik araçlarının her biri detaylı olarak ele alınacak; her aracın amacı, çalışma prensibi ve siber güvenliğe olan katkısı anlaşılır ve sistematik bir şekilde açıklanacaktır. Böylece okuyucular, internet ortamında karşılaşılabilecekleri riskleri daha yakından tanıyarak dijital varlıklarını koruma konusunda daha bilinçli adımlar atabileceklerdir.



Dijital güvenliğin saęlanmasında doęru bilgiye zamanında ulaşmak kadar, bu bilgiyi elde ederken kullanılan araçların güvenilir ve doęru sonuçlar üretmesi de büyük önem taşır.

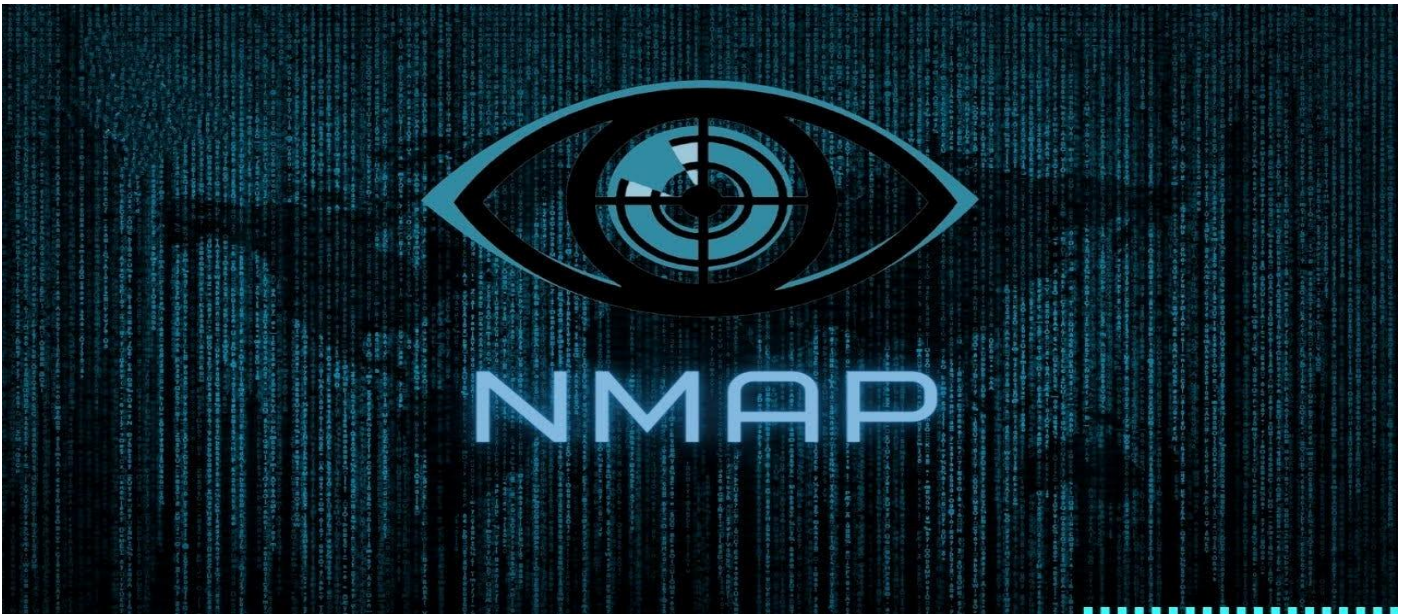
Security Check platformu üzerinde sunulan araçlar, internet dünyasının farklı katmanlarında gizlenen riskleri tespit etmeye yardımcı olur. Bu bölümde, her bir güvenlik aracını ayrı ayrı ele alacak, hangi amaçla kullanıldıklarını ve kullanıcılar için nasıl deęer yarattıklarını açıklayacağız.



Nmap : Discover Your Network

Aę yöneticileri, BT profesyonelleri ve güvenlik uzmanları, aęlarında hangi cihazların çalıştığını, hangi hizmetlerin sunulduęunu ve potansiyel güvenlik açıklarını sürekli olarak izlemek zorundadır. Bu tür izlemeler için pek çok araç mevcut olsa da Nmap, sağladığı çok yönlülük ve kullanılabilirlik ile öne çıkmaktadır. Bu özellikler, Nmap'ı aę tarama ve güvenlik denetimi alanında bir standart haline getirmiştir.

Nmap (Network Mapper), ücretsiz ve açık kaynaklı bir aę keşfi ve güvenlik tarama aracıdır. Aę yöneticileri ve güvenlik uzmanları, Nmap'ı kullanarak aęlarındaki cihazları keşfeder, aktif olan ana bilgisayarları belirler, açık portları tespit eder ve bu portların güvenlik durumlarını analiz eder. Bununla birlikte, Nmap yalnızca küçük aęlar için deęil, büyük ölçekli aęlarda da etkili bir şekilde kullanılabilir.



Nmap'ın temel işlevi, ağ üzerindeki cihazların portlarına ham paketler göndererek bu cihazlarla iletişime geçmek ve ardından yanıtları analiz etmektir. Bu şekilde, her bir portun açık, kapalı veya filtrelenmiş olup olmadığını belirlemek mümkündür. Port taraması, port keşfi veya port numaralandırma gibi terimlerle de tanımlanabilir ve ağ güvenliği açısından büyük önem taşır.

Port Taraması

Nmap, gönderdiği paketler aracılığıyla, ağ üzerindeki IP adreslerini, donanım bilgilerini ve yazılım özelliklerini içeren çeşitli verileri toplar. Bu veriler, ağın genel özelliklerini tanımlamanıza, bir ağ profili veya haritası oluşturmanıza ve hatta ağındaki cihazların donanım ve yazılım envanteri üzerinde detaylı bir inceleme yapmanıza olanak tanır.

SECURITY CHECK
Security is important

Target IP or Domain:

192.168.1.1

Scan

Results:

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-09 07:17 Türkiye Standart Saati
Nmap scan report for 192.168.1.1
Host is up (0.0068s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Cisco router telnetd
Service Info: OS: IOS; Device: router; CPE: cpe:/o:cisco:ios

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.13 seconds
```

Nmap, farklı ağ protokollerini kullanarak çeşitli türlerdeki paket yapılarını işler. Bu protokoller arasında TCP (İletim Kontrol Protokolü), UDP (Kullanıcı Datagram Protokolü), SCTP (Akış Kontrol İletim Protokolü) gibi taşıma katmanı protokollerinin yanı sıra, ICMP (İnternet Kontrol Mesaj Protokolü) gibi destekleyici protokoller de yer alır.

Her bir protokol, farklı sistem portları ve kullanım amaçları için optimize edilmiştir. Örneğin, UDP protokolü, düşük kaynak yükü ile hızlı veri iletimi sağladığı için gerçek zamanlı video akışı gibi uygulamalarda kullanılır. Bu protokolde bazı veri kayıpları, hız karşılığında kabul edilebilir. Öte yandan, TCP protokolü ise daha güvenilir bir bağlantı sağlar ancak hız açısından biraz daha yavaştır ve genellikle YouTube gibi gerçek zamanlı olmayan video akışları için tercih edilir.

Bunlar dışında, Nmap'in temel port tarama ve paket yakalama yetenekleri sürekli olarak gelişmektedir. Nmap'in yazarı Gordon Lyon, yazılımla ilgili bir soruya verdiği yanıtta, "Windows için Npcap paketini geliştirmeye odaklanıyoruz. Bu, Nmap'i daha hızlı ve güçlü kılıyor ve artık birçok diğer uygulama tarafından da kullanılabilir" şeklinde bir açıklama yapmıştır. (seclists.org)

Nmap Kurucusu : Gordon Lyon (Fyodor)

Nmap, ilk kez 1997 yılının Eylül ayında C++ dilinde yazılmış bir versiyonuyla Phrack Magazine' de kaynak koduyla tanıtılmıştır. Daha sonra C, perl ve python dilleri ile geliştirilmiştir. Kurucusu olan Gordon Lyon, Fyodor Dostoyevski'nin Yeraltı Notları'nı okuduktan sonra Fyodor Vaskovitch takma adını benimsemiş ve Fyodor tutamacını Nmap'teki çalışmasında kullanmıştır.

Nmap, zaman ilerledikçe büyüyen meraklılar ve geliştiriciler topluluğunun katkılarından yararlanarak şuan günde binlerce kez indiriliyor. Nmap'in popüleritesinin nedenlerinden biri, çeşitli işletim sistemlerinde kullanılabilir olmasıdır. Windows ve macOS'ta çalışır ve Red Hat, Mandrake, SUSE ve Fedora gibi Linux dağıtımlarını destekler. Ayrıca BSD, Solaris, AIX, ve AmigaOS gibi diğer işletim sistemlerinde de çalışır.

Nmap Nasıl Kullanılır?

Ağ güvenliği denince akla gelen araçlardan biri olan Nmap, sadece teknik uzmanlar için değil, ağlarla yeni tanışanlar için de güçlü ve esnek bir yardımcıdır. Birçok ücretsiz araç arasında öne çıkmasının sebebi, hem gelişmiş hem de kullanıcı dostu bir yapıya sahip olmasıdır.

Nmap'in temel işlevi port taraması olsa da, sunduğu imkanlar sadece bununla sınırlı değil.

Örneğin:

- **Ağ Eşlemesi (Host Discovery):** Nmap, bir ağda yer alan cihazları (sunucular, yönlendiriciler, anahtarlar vb.) tanıyabilir ve bu cihazların birbiriyle olan fiziksel bağlantılarını ortaya çıkarabilir.
- **İşletim Sistemi Tespiti:** Hangi cihazın hangi işletim sistemini kullandığını belirleyebilir. Hatta bazı durumlarda yazılım sürümünü ve cihazın ne kadar süredir açık olduğunu bile tahmin edebilir.
- **Hizmet Keşfi:** Nmap, bir cihazın sadece varlığını değil, o cihazda hangi hizmetlerin (örneğin web sunucusu, e-posta servisi) çalıştığını ve hangi yazılım sürümünün kullanıldığını da belirleyebilir.
- **Güvenlik Denetimi:** Cihazlarda çalışan yazılım ve sürümleri analiz ederek, bilinen açıklara (zafiyetlere) karşı ağın ne kadar savunmasız olduğunu anlamaya yardımcı olur. Gerekirse, ilgili sistemlerin güncellenmesi veya yamalanması için önlem alınabilir.

Bu gibi özellikler, sadece büyük firmalar için değil; küçük ölçekli ağlar yöneten bireyler veya yeni başlayanlar için de oldukça kıymetlidir. Üstelik Nmap'in komutları çok detaylı ayarlanabilir. Basit komutlarla temel bir tarama yapılabilirken, daha gelişmiş kullanıcılar daha karmaşık tarama türlerini tercih ederek daha detaylı bilgiler elde edebilir.

Örneğin bir taramada, -sV komutu sayesinde servislerin versiyonları öğrenilebilir. --version-intensity gibi parametreler kullanıldığında, taramanın derinliği yani ne kadar detaylı bilgi toplayacağı da kontrol edilebilir. 0'dan 9'a kadar ayarlanabilen bu yoğunluk derecesi, taramanın hızını ve doğruluğunu etkiler. Düşük seviyelerde hızlı ama yüzeysel sonuçlar alınırken, yüksek seviyelerde daha detaylı ama uzun süren analizler yapılabilir.

Nmap ayrıca, Lua diliyle yazılmış komut dosyaları sayesinde çeşitli görevleri otomatikleştirme imkânı sunar. Bu sayede örneğin, belirli bir zafiyetin ağda olup olmadığını anlamak veya sık yapılan taramaları tek komutla gerçekleştirmek mümkün olur.

Zenmap – Nmap GUI'si

Zenmap, nmap güvenlik tarayıcısı arayüzüdür. Taramaları kaydetme ve karşılaştırma, ağ topoloji haritalarını görüntüleme imkanı ve ana bilgisayarda çalışan bağlantı noktalarının görüntülenmesi veya bir ağdaki tüm bilgisayarların görüntü ve taramaları, aranabilir bir veritabanında saklama gibi imkanlar sunar.

Nmap Hacking

Port taraması tek başına birçok ülkede, özellikle de ABD'de, doğrudan yasa dışı kabul edilmese de, Nmap gibi güçlü araçların yanlış kullanımı ciddi sonuçlar doğurabilir. Çünkü Nmap sadece ağları keşfetmek için değil, aynı zamanda kötü niyetli kişiler tarafından açıkları bulup istismar etmek amacıyla da kullanılabilir.

Özellikle, izinsiz yapılan taramalar — ister iyi niyetle bir güvenlik kontrolü yapmak isteyin, ister başka bir amaç taşıyın — çeşitli yasal sorunlara yol açabilir. Bazı Nmap taramaları ağlar üzerinde çok az iz bıraksa da ve güvenlik sistemleri tarafından kolayca algılanmasa da, her zaman taramadan önce ilgili izinleri almak en doğru yaklaşım olacaktır. Kendi kurumunuzda dahi çalışıyor olsanız, yetkili kişilerden onay almak güvenliğinizi artırır.

Ayrıca şunu unutmamak gerekir: Nmap'in işletim sistemi tespiti gibi bazı özellikleri root (yönetici) yetkileri gerektirir. Bu da kullanıcıların sistem üzerinde tam erişim haklarına sahip olması gerektiği anlamına gelir.

Sonuç olarak, yapmak istediğiniz işlemin yasal olup olmadığı konusunda bir tereddütünüz varsa, özellikle bağımsız çalışıyorsanız ve arkanızda bir hukuk departmanı yoksa, bilgisayar dolandırıcılığı ve siber suçlar konusunda uzman bir danışmana başvurmanız önemlidir. Böylece hem kendinizi hem de çalıştığınız yapıyı gereksiz risklerden korumuş olursunuz.

Kaynakça :

- Karel. (t.y.). *Nmap nedir? Bu ağ tarayıcısına neden ihtiyacınız var?* Karel.
<https://www.karel.com.tr/blog/nmap-nedir-bu-ag-tarayicisina-neden-ihtiyaciniz-var>

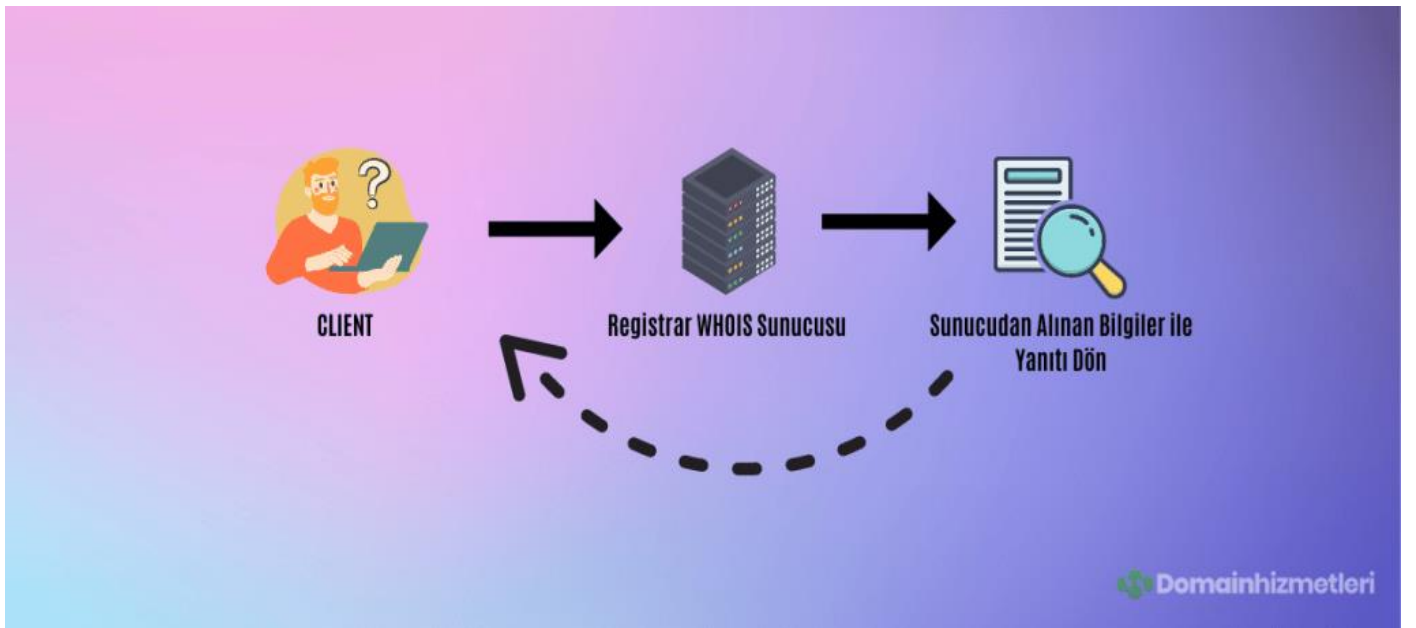
Nmap Taramalarında kullanılan Parametreler

- **-sn:** Port taraması yapma anlamına gelir.
- **-n:** DNS Çözümlemesi yapma anlamına gelir.
- **-v, -vv, -vvv:** Ekrana gösterilecek detayları artırır.
- **-F:** Daha hızlı tarama yapar. Daha az sonuç bulur.
- **-sS:** Syn Taraması Yapar.
- **-reason:** Bulduğu bir sonucun sebebini gösterir.
- **-open:** Sadece açık Portları gösterir.
- **-p-:** Bir IP üzerinde bulunması muhtemel 65535 portun hepsini tarar.
- **-sV:** Açık portta çalışan servisin ne olduğunu bulmaya çalışır. -sC ile birlikte kullanılırsa işe yarar.
- **-sC:** -sV ile versiyon tespiti yapılırken nmap scriptlerini kullanır.
- **-p:** Sadece bu parametreden sonra belirtilen portları tarar.
- **-top-ports:** En çok kullanılan portları tarar.

WHOİS : Domain Request Tool

İnternet dünyasında bir alan adının kime ait olduğunu öğrenmek bazen hem güvenlik hem de iletişim açısından kritik bir ihtiyaç haline gelebiliyor. İşte tam bu noktada devreye WHOİS sistemi giriyor.

Bir alan adı (domain) tescil edildiğinde, bu alan adının sahibiyle ilgili iletişim bilgileri ve teknik bilgiler bir veritabanında saklanır. İşte bu veritabanı üzerinden yapılan yetkili bilgi sorgulamasına WHOİS denir. WHOİS kavramı aslında çok eskilere dayanıyor; 1970'li yıllarda, ARPANET kullanıcılarının iletişim bilgilerini listelemek için geliştirilen basit bir sistem olarak hayatımıza girdi. Zamanla internetin yaygınlaşmasıyla birlikte, WHOİS verileri marka sahipleri, firmalar, bireysel kullanıcılar ve hatta kolluk kuvvetleri için önemli bir bilgi kaynağı haline geldi.



1998 yılında ICANN (Internet Corporation for Assigned Names and Numbers) kurulduğunda, WHOİS protokolünün yönetimi de bu kuruluşa devredildi. ICANN, WHOİS hizmetinin daha sağlıklı bir şekilde çalışabilmesi için ana kayıt şirketleri ve ofisleriyle çeşitli anlaşmalar yaptı. Böylece WHOİS'in nasıl işletileceğine dair bir standart ve politika çerçevesi oluşturulmuş oldu. Günümüzde WHOİS verilerinin güvenilir ve güncel kalabilmesi için bu politikalar kayıt kuruluşlarıyla iş birliği içinde yürütülüyor.

Ancak WHOİS protokolü ilk tasarlandığında internetin bu kadar büyüyeceği pek öngörülmemişti. Kullanımın artmasıyla birlikte WHOİS'in erişim, uyumluluk, dolandırıcılık ve mahremiyet gibi konularda bazı zorluklar yaşadığı görüldü. Bu problemleri çözebilmek için ICANN sürekli yeni gereklilikler getirdi. Bunlardan biri, 2014 yılında yürürlüğe giren RAA (Registrar Accreditation Agreement) sayesinde gelen e-posta doğrulama zorunluluğudur. Artık bir domain ilk tescil edildiğinde veya domain sahibinin iletişim bilgileri değiştiğinde, e-

posta üzerinden onay alınmadan hiçbir deęişiklik yapılamıyor. Böylece alan adlarının izinsiz el deęiřtirmesi veya sahte bilgilerle kaydedilmesi gibi riskler büyük ölçüde azaltılmış oldu.

WHOIS günümüzde hâlâ internet dünyasının şeffaflık ve güvenlik açısından önemli yapı taşlarından biri olarak işlevini sürdürüyor.

WHOIS Nasıl Çalışır?

WHOIS sistemi, bir alan adının kime ait olduğunu ve bazı önemli teknik bilgileri öğrenmemize yarayan bir sorgulama mekanizmasıdır. Bir WHOIS sorgulaması yaptığınızda, alan adının hangi kayıt şirketine ait olduğu, sahibinin adı soyadı, telefon numarası, e-posta adresi, şirket ya da ev adresi, domainin oluşturulma ve güncellenme tarihleri, ayrıca yönlendirildięi isim sunucu (NS) kayıtları gibi verilere ulaşabilirsiniz. Teknik olarak WHOIS'in çalışma mantığı şöyle işler: Bir alan adının bilgilerini öğrenmek istediğinizde, domain uzantısına (örneğin .com, .org, .net gibi) göre ilgili WHOIS sunucusuna TCP protokolü kullanılarak 43 numaralı port üzerinden bir istek gönderilir. Bu WHOIS sunucusu ise, sisteminde kayıtlı olan ve herkese açık durumdaki domain sahiplik bilgilerini size sunar.

SECURITY CHECK
Security is important.

Homepage
Network Scanner
MX Lookup
Whois Lookup
Blacklist Check
Dmarc Lookup
DNS Lookup

Whois Query

github.com Query

Results:

```
Creation Date: 2007-10-09T18:20:50Z
Domain Name: github.com
Name Servers: DNS1.P08.NSONE.NET, DNS2.P08.NSONE.NET,
DNS3.P08.NSONE.NET, DNS4.P08.NSONE.NET, NS-1283.AWSDNS-32.ORG, NS-
1707.AWSDNS-21.CO.UK, NS-421.AWSDNS-52.COM, NS-520.AWSDNS-01.NET,
ns-520.awsdns-01.net, ns-1707.awsdns-21.co.uk, ns-1283.awsdns-
32.org, dns1.p08.nsonone.net, ns-421.awsdns-52.com,
dns2.p08.nsonone.net, dns3.p08.nsonone.net, dns4.p08.nsonone.net, ns-
520.awsdns-01.net, ns-1707.awsdns-21.co.uk, ns-1283.awsdns-32.org,
dns1.p08.nsonone.net, ns-421.awsdns-52.com, dns2.p08.nsonone.net,
dns3.p08.nsonone.net, dns4.p08.nsonone.net
Registrant Country: US
Registrar: MarkMonitor Inc.
Registrar URL: http://www.markmonitor.com
Registry Expiry Date: 2026-10-09T18:20:50Z
Updated Date: 2024-09-07T09:16:33Z
```

WHOİS Sorgusu

WHOİS sorgulaması yapabilmek için internette hizmet sunan birçok site bulunmaktadır. Ancak bu siteleri kullanırken bazı sıkıntılarla karşılaşabiliyoruz. Örneğin, sorgu hızının yavaş olması, bilgilerin sadece ham veri şeklinde sunulması ya da site tasarımındaki eksiklikler doğru ve verimli bir sorgu yapmamızı zorlaştırabiliyor.

Bu gibi sıkıntılar nedeniyle bazı ekipler kendi özel WHOİS sorgulama araçlarını geliştirmiştir. Örneğin, DH ekibi, yaşadığı bu sorunlardan yola çıkarak kendi WHOİS sorgulama sistemini kurmuş ve herkesin ücretsiz olarak kullanabilmesi için whois.dh.web.tr adresinden hizmete açmıştır.

Bu tarz WHOİS araçları sayesinde, bir alan adına ait kayıt firması (Registrar bilgileri), isim sunucuları (NameServer - DNS bilgileri), alan adı sahibinin iletişim bilgileri (adı-soyadı, şirketi, e-posta adresi, telefon numarası, açık adresi, ülkesi gibi) ve ayrıca domainin kayıt tarihi, son güncelleme tarihi, bitiş tarihi gibi önemli zaman bilgilerine ulaşmak mümkündür. Ayrıca transfer kilidi durumu ve tüm bu bilgilerin ham veri halleri de görüntülenebilir.

Kaynakça : Domain Hizmetleri. (t.y.). *WHOİS nedir?* Domain Hizmetleri.

<https://www.domainhizmetleri.com/blog/whois-nedir/>

MX Lookup :

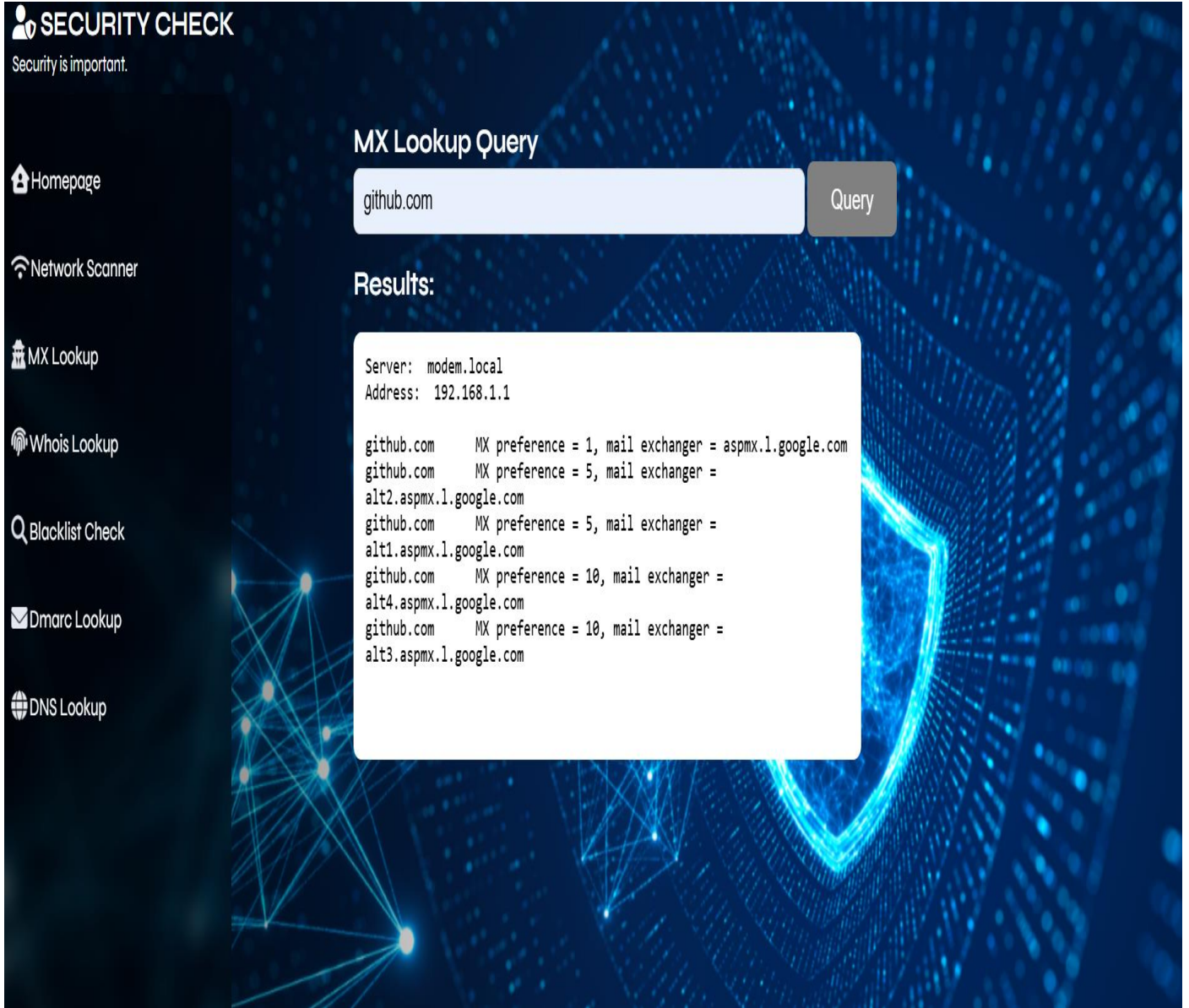
MX Kayıtları Nedir ve Nasıl Çalışır?

MX (Mail Exchange) kayıtları, bir alan adına bağlı e-posta hesaplarına gelen iletilerin hangi sunucuya yönlendirileceğini belirleyen DNS kayıt türüdür. Alan adınıza gelen e-postaların doğru şekilde iletilmesini sağlar. Genellikle birden fazla MX kaydı tanımlanabilir ve bu kayıtlar öncelik sırasına göre 10, 20 gibi değerlerle derecelendirilir.

Örneğin, bir kullanıcıya e-posta gönderildiğinde sistem, ilgili alan adına ait MX kayıtlarını kontrol eder. Önceliği 10 olan sunucuya ulaşılabilirse ileti bu sunucu üzerinden teslim edilir. Ancak bu sunucu yanıt vermezse, sistem sıradaki örneğin 20 öncelikli sunucuya yönelir. Bu yapı sayesinde, bir sunucu çalışmasa bile diğerleri devreye girerek kesintisiz bir e-posta iletişimi sağlanmış olur.



Mesaj aktarım aracı (MTA) yazılımı MX kayıtlarını sorgulamaktan sorumludur. Bir kullanıcı bir e-posta gönderdiğinde, MTA e-posta alıcıları için posta sunucularını tanımlamak üzere bir DNS sorgusu gönderir. MTA, öncelikli etki alanlarıyla başlayarak bu posta sunucularıyla bir SMTP bağlantısı kurar (yukarıdaki ilk örnekte, mailhost1).



SECURITY CHECK
Security is important.

Homepage
Network Scanner
MX Lookup
Whois Lookup
Blacklist Check
Dmarc Lookup
DNS Lookup

MX Lookup Query

github.com **Query**

Results:

```
Server: modem.local
Address: 192.168.1.1

github.com    MX preference = 1, mail exchanger = aspmx.l.google.com
github.com    MX preference = 5, mail exchanger =
alt2.aspmx.l.google.com
github.com    MX preference = 5, mail exchanger =
alt1.aspmx.l.google.com
github.com    MX preference = 10, mail exchanger =
alt4.aspmx.l.google.com
github.com    MX preference = 10, mail exchanger =
alt3.aspmx.l.google.com
```

Yedek MX Kaydı

Yedek MX kaydı, daha yüksek bir 'öncelik' değerine sahip (daha düşük bir öncelik anlamına gelir) bir posta sunucusu için bir MX kaydıdır, böylece normal koşullar altında posta daha öncelikli sunuculara gider. Yukarıdaki ilk örnekte, mailhost2 'yedek' sunucu olurdu çünkü e-posta trafiği, çalışır durumda olduğu sürece mailhost1 tarafından yönetilir.

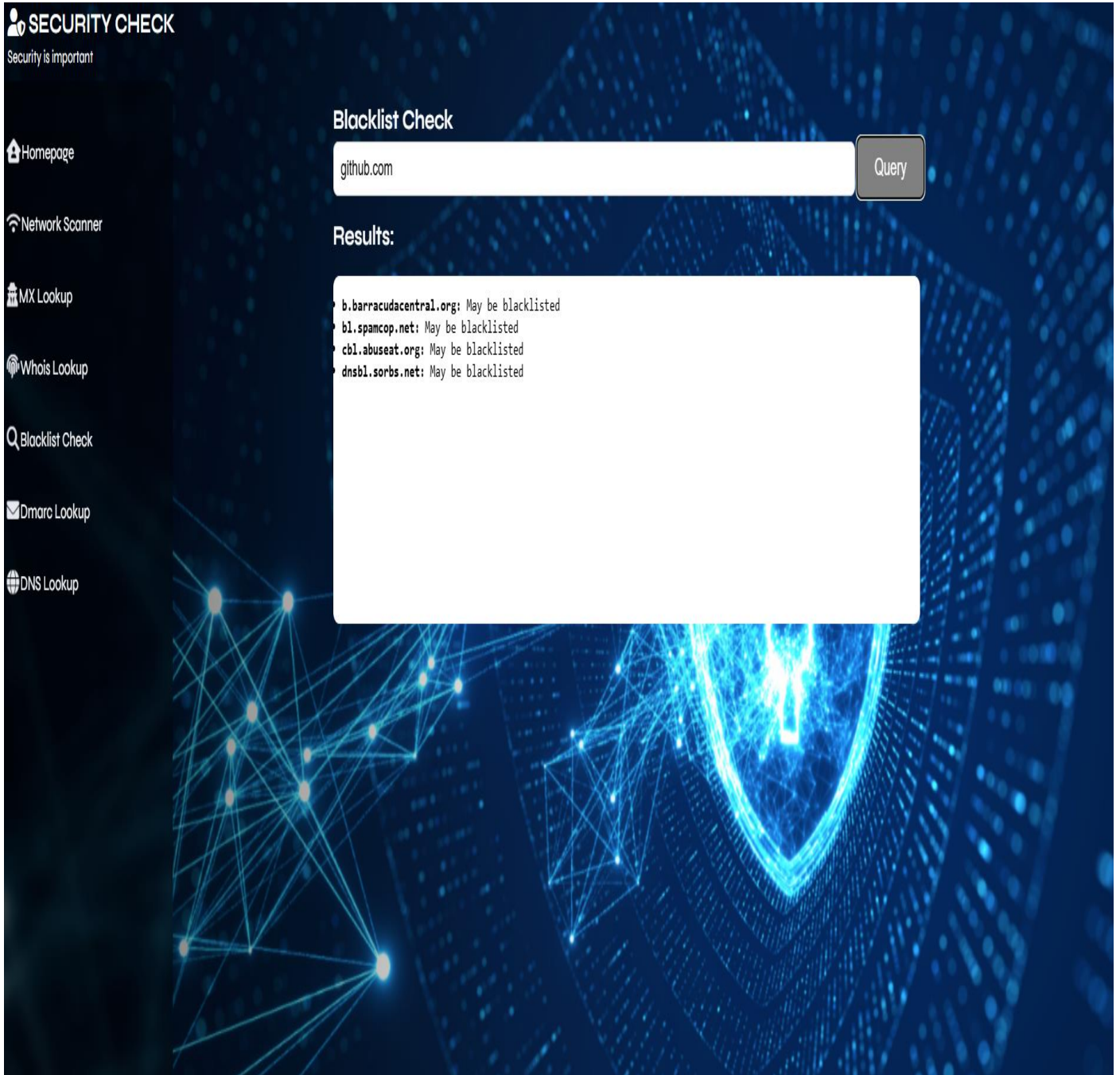
Kaynakça :

Uzman Posta. (t.y.). *MX Sorgulama Nedir? MX Kaydı Nedir, Nasıl Yapılır?* Erişim adresi: <https://uzmanposta.com/mx-sorgulama>

Blacklist Check : Kara Liste

Günlük dijital yaşamda sıkça karşılaştığımız **blacklist (kara liste)** kavramı, bir IP adresinin ya da posta sunucusunun, spam veya kötüye kullanım gibi nedenlerle çeşitli güvenlik veri tabanlarında engellenip engellenmediğini kontrol etmeye yarar. Eğer IP adresinizin bir kara listeye yanlışlıkla eklendiğini düşünüyorsanız, yapılan bu kontroller durumu doğrulamanıza ve nasıl bir yol izlemeniz gerektiğine karar vermenize yardımcı olur.

Kara liste denetimi, girilen bir IP adresinin veya alan adının DNS tabanlı kara liste (DNSBL) sistemlerinde yer alıp almadığını kontrol eden bir prosedürdür. Çeşitli DNSBL sistemleri farklı kriterlere göre spam kaynağı olduğuna inandıkları adresleri listelerine dahil eder. Bu listelere giren IP adresleri üzerinden e-posta gönderimi genellikle engellenir.



The screenshot shows a web application titled "SECURITY CHECK" with the tagline "Security is important". The left sidebar contains navigation links: Homepage, Network Scanner, MX Lookup, Whois Lookup, Blacklist Check (active), Dmarc Lookup, and DNS Lookup. The main content area is titled "Blacklist Check" and features a search input field containing "github.com" and a "Query" button. Below the input, the "Results:" section displays a list of DNSBL checks:

- b.barracudacentral.org: May be blacklisted
- bl.spamcop.net: May be blacklisted
- cbl.abuseat.org: May be blacklisted
- dnsbl.sorbs.net: May be blacklisted

Spam filtreleri, gelen e-postaların kara listeye alınmış kaynaklardan gelip gelmediğini kontrol eder. Bu nedenle, eğer e-posta sunucunuz bir kara listede yer alıyorsa, gönderdiğiniz iletiler karşı tarafa ulaşmayabilir. Ancak bazı durumlarda sistemler hatalı değerlendirme yaparak spam göndermeyen IP'leri de listeye alabilir. Bu gibi durumlar için çevrimiçi kara liste denetleyicileri büyük kolaylık sağlar.

Kara Listedeki nasıl çıkılır?

IP adresiniz kara listeye alındıysa öncelikle ağızda kötü amaçlı yazılım bulunmadığından emin olmalısınız. Ardından ilgili liste sağlayıcısı ile iletişime geçerek kaldırma talebinde bulunabilirsiniz. Her kara liste, kaldırma taleplerini farklı şekilde işlediğinden, süreç listeye göre değişkenlik gösterebilir. Ancak bu adımlar, IP'nizi tekrar kullanılabilir hale getirmek için en etkili yöntemdir.

Neden Kara Listeye Girilir?

Kara listeye alınma (blacklist) işlemi, bir IP adresinin zararlı veya güvenli olmayan etkinliklerde bulunduğu tespit edildiğinde, diğer kullanıcıları ve sistemleri korumak amacıyla gerçekleştirilir. Ancak bazı durumlarda güvenli IP'ler de yanlışlıkla kara listeye alınabilir. Bu nedenle çevrimiçi olarak IP kara liste sorgulaması yapmak, sistem güvenliği açısından oldukça önemlidir.

Bir IP adresi aşağıdaki nedenlerle kara listeye alınabilir:

- IP, spam e-posta kaynağı olarak görünüyorsa
- Zararlı içerik barındıran bir web sitesiyle ilişkilendirildiyse
- Ağa yayılabilecek kötü amaçlı yazılım içeren bir cihaza bağlıysa
- Karanlık ağ (dark web) gibi yasa dışı platformlara erişim sağladıysa



Blacklist Spam Filtrelemede Rolü

Kara liste sistemleri, spam içeriklerle mücadelede en önemli savunma mekanizmalarından biridir. Bu listeler, şüpheli IP adreslerini tespit ederek gelen kutularına zararlı içeriklerin ulaşmasını engeller. Bazı filtreleme sistemleri ayrıca e-postalardaki bağlantıları analiz ederek, mesaj gövdesindeki kötü niyetli web sitelerini de kara listelerle karşılaştırır. Böylece sadece IP değil, bağlantı üzerinden de spam tespiti yapılabilir.

Alan Adları Neden Kara Listeye Alınır?

- E-posta gönderimleriniz spam olarak raporlandıysa
- Sunucunuz hatalı yapılandırıldıysa veya kötü amaçlı yazılım içeriyorsa
- IP adresiniz yasa dışı faaliyetlerde bulunduysa veya saldırılarda kullanıldıysa

Bu durumlarda alan adınız veya IP'niz, DNS tabanlı kara listelere (DNSBL) dahil edilebilir. DNSBL sistemleri, genellikle spam kaynaklarını engellemek üzere tasarlanmış DNS tabanlı listelerdir. E-posta sunucuları bu listeleri sorgulayarak şüpheli kaynaklardan gelen mesajları engelleyebilir.

Kaynakça :

Ajans IO. (t.y.). Blacklist Nedir? Nasıl Kontrol Edilir? Erişim adresi: <https://www.ajansio.com.tr/blacklist-nedir-nasil-kontrol-edilir>

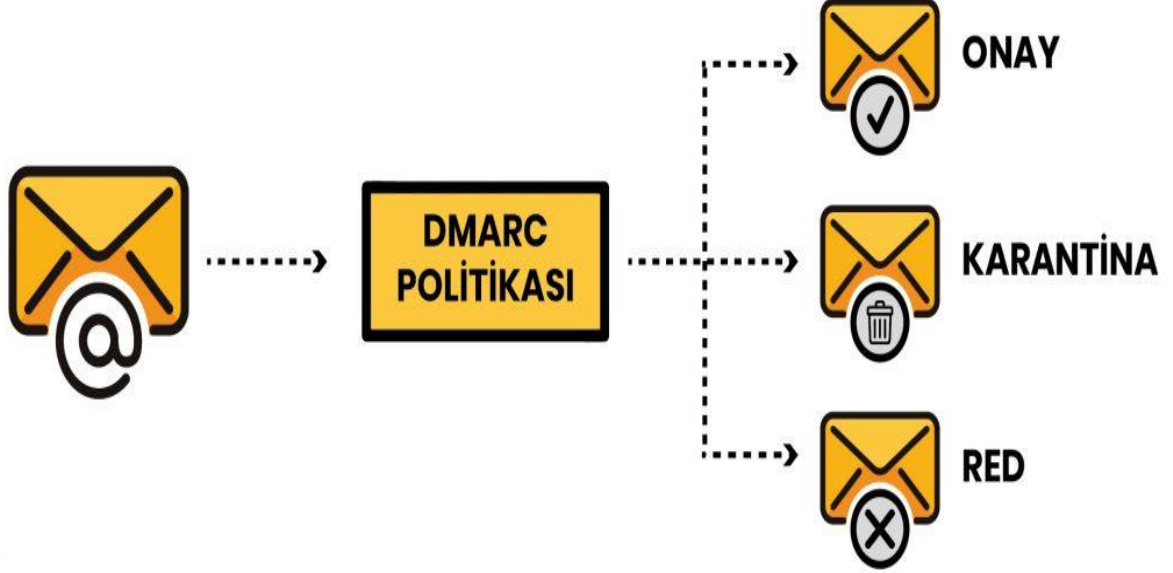
Dmarc Lookup :

DMARC (Domain-based Message Authentication, Reporting, and Conformance), yani "Alan Adı Tabanlı Mesaj Kimlik Doğrulama, Raporlama ve Uyum", e-posta güvenliğini artırmak amacıyla geliştirilmiş bir protokoldür. Temel amacı, bir e-posta mesajının gerçekten gönderici olduğunu iddia ettiği alandan gelip gelmediğini doğrulamak ve bu doğrulamaya göre ne yapılacağını belirlemektir.

DMARC, SPF (Gönderen Politikası Çerçevesi) ve DKIM (Alan Adı Anahtarlı Posta) adlı iki kimlik doğrulama yöntemini temel alır. Eğer bir e-posta bu iki testten geçemezse, yani alıcı sunucu gönderenin gerçekten iddia ettiği alan adıyla ilişkili olduğunu kanıtlayamazsa, DMARC devreye girer. Bu noktada DMARC, gelen e-postanın spam, oltalama (phishing) ya da kötü amaçlı yazılım içerip içermediğine göre şu üç işlemten birini uygular:

- E-postayı olduğu gibi kabul et
- Karantinaya al (spam klasörüne düşür)
- Reddet (hiçbir şekilde teslim etme)

Bu yönüyle DMARC, e-posta kutularına gelen tehlikeli mesajlara karşı bir tür güvenlik kapısı görevi görür. Özellikle kimlik avı saldırılarının önüne geçmek için oldukça etkili bir yöntemdir.



DMARC Kaydı Ne İşe Yarar?

DMARC politikaları, alan adına ait DNS (Domain Name System) üzerinden yayımlanır. Bu, o alan adıyla ilişkili e-posta trafiği için ne tür bir kontrol uygulanacağını belirleyen küçük bir yapılandırma kayıdır. Genellikle "TXT" tipi bir kayıtla gerçekleştirilir. Yani, DMARC kurulumu teknik olarak yalnızca DNS üzerinde yapılacak tek bir değişiklikle sağlanabilir.

DMARC kaydı; eğer e-postalar doğrulanamazsa nasıl bir işlem uygulanacağını tanımlar:

- Hiçbir işlem yapılmaz
- Mesaj karantinaya alınır
- Mesaj reddedilir

Bu politika, e-posta sunucularının göndericiyi kontrol etmesini ve mesajın güvenli olup olmadığına karar vermesini sağlar.

DMARC Nasıl Çalışır?

1. **DNS Kaydı Yayınlama:** Alan adı sahibi, DNS sağlayıcısı üzerinden DMARC kaydını yayımlar.
2. **E-posta Gönderimi:** Alan adından ya da o alanı taklit eden bir kaynaktan e-posta gönderilir.

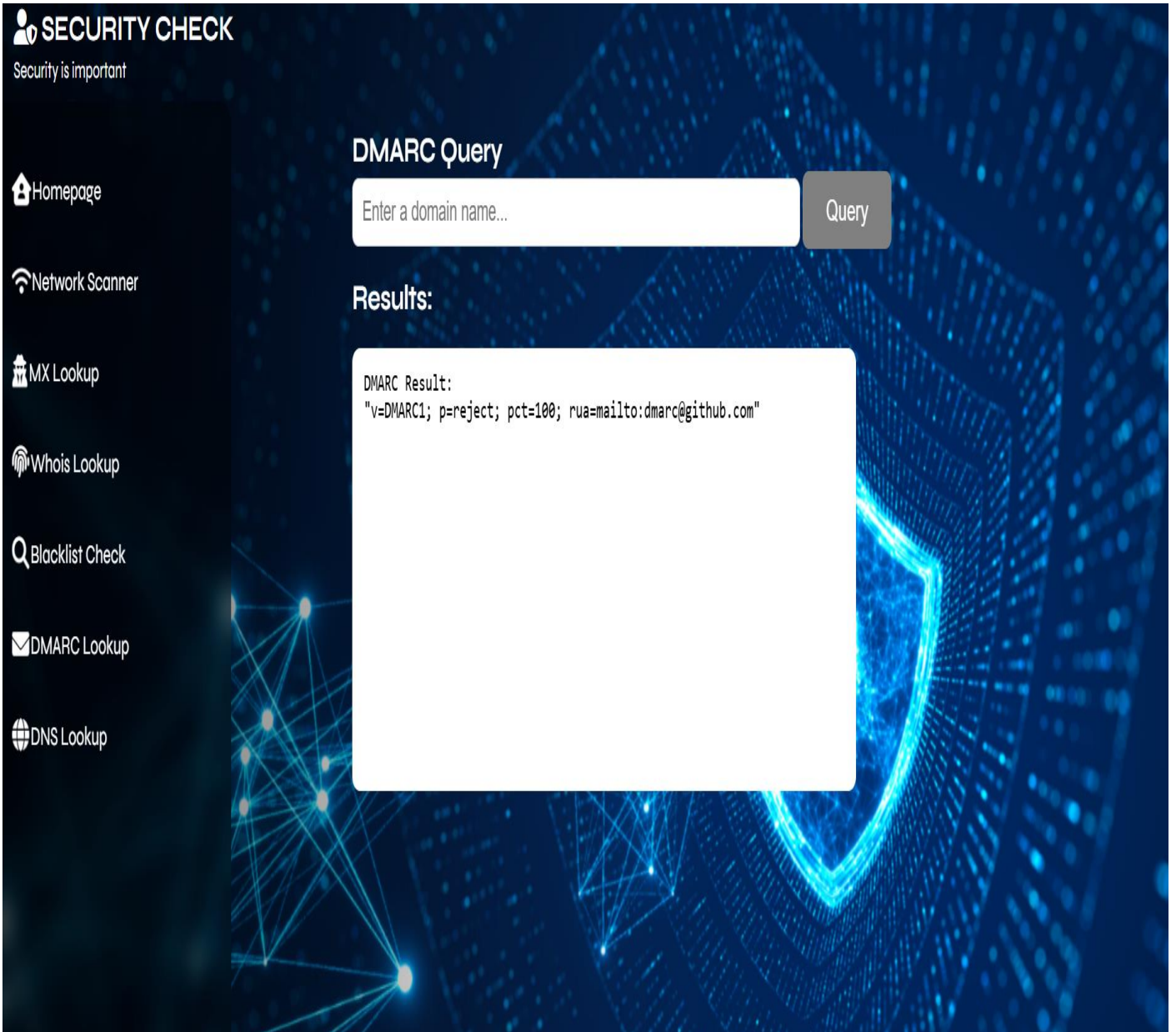
3. **Kimlik Doğrulama:** Alıcı sunucu, SPF ve DKIM testlerini uygular.

- E-posta, gönderici alanına ait mi?
- Dijital imza (DKIM) geçerli mi?
- Ip adresi, yetkili SPF kaydında yer alıyor mu?

4. **Politika uygulama:** Sonuçlara göre DMARC politikası devreye girer.

- Mesajı reddet
- Karantinaya al
- Kabul et

5. **Raporlama:** Son adımda, e-posta sistemleri DMARC doğrulama sonuçlarını günlük olarak raporlar ve bu raporları alan adı sahibine iletir. Bu raporlar sayesinde alan adı sahipleri, hangi sunucuların kendi adlarına e-posta gönderdiğini, ne kadarının geçerli olduğunu, hangilerinin başarısız olduğunu detaylıca görebilir.



DNS Lookup

İnternette bir web sitesini ziyaret ettiğinizde, genellikle sadece adres çubuğuna www.orneksite.com gibi bir alan adı yazarsınız. Ancak bilgisayarlar bu alan adlarını doğrudan anlayamaz; bunun yerine, her sitenin arka planda kullanılan bir IP adresi vardır örneğin (192.168.1.1) gibi. İşte tam bu noktada DNS devreye girer.

DNS (Domain Name System – Alan Adı Sistemi), alan adlarını IP adreslerine çeviren bir internet protokolüdür. Bu sistemi, telefon rehberine benzetebiliriz. Siz kişilerin isimlerini bilirsiniz, telefonunuz ise o ismin arkasındaki numarayı bulur. DNS de web siteleri için aynı işi yapar.

DNS Lookup, yani DNS sorgusu, tarayıcınıza yazdığınız alan adının hangi IP adresine karşılık geldiğini öğrenmek için yapılan aramadır. Böylece cihazınız, veriyi nereden alacağını bilir ve sizi doğru sunucuya yönlendirir.

DNS sorguları olmadan, her bir web sitesine ulaşmak için karmaşık IP adreslerini ezberlemek zorunda kalırdık. DNS Lookup, bu karmaşıklığı ortadan kaldırarak kullanıcı dostu bir internet deneyimi sağlar.

SECURITY CHECK
Security is important

Homepage
Network Scanner
MX Lookup
Whois Lookup
Blacklist Check
Dmarc Lookup
DNS Lookup

DNS Lookup Query

github.com Query

Results:

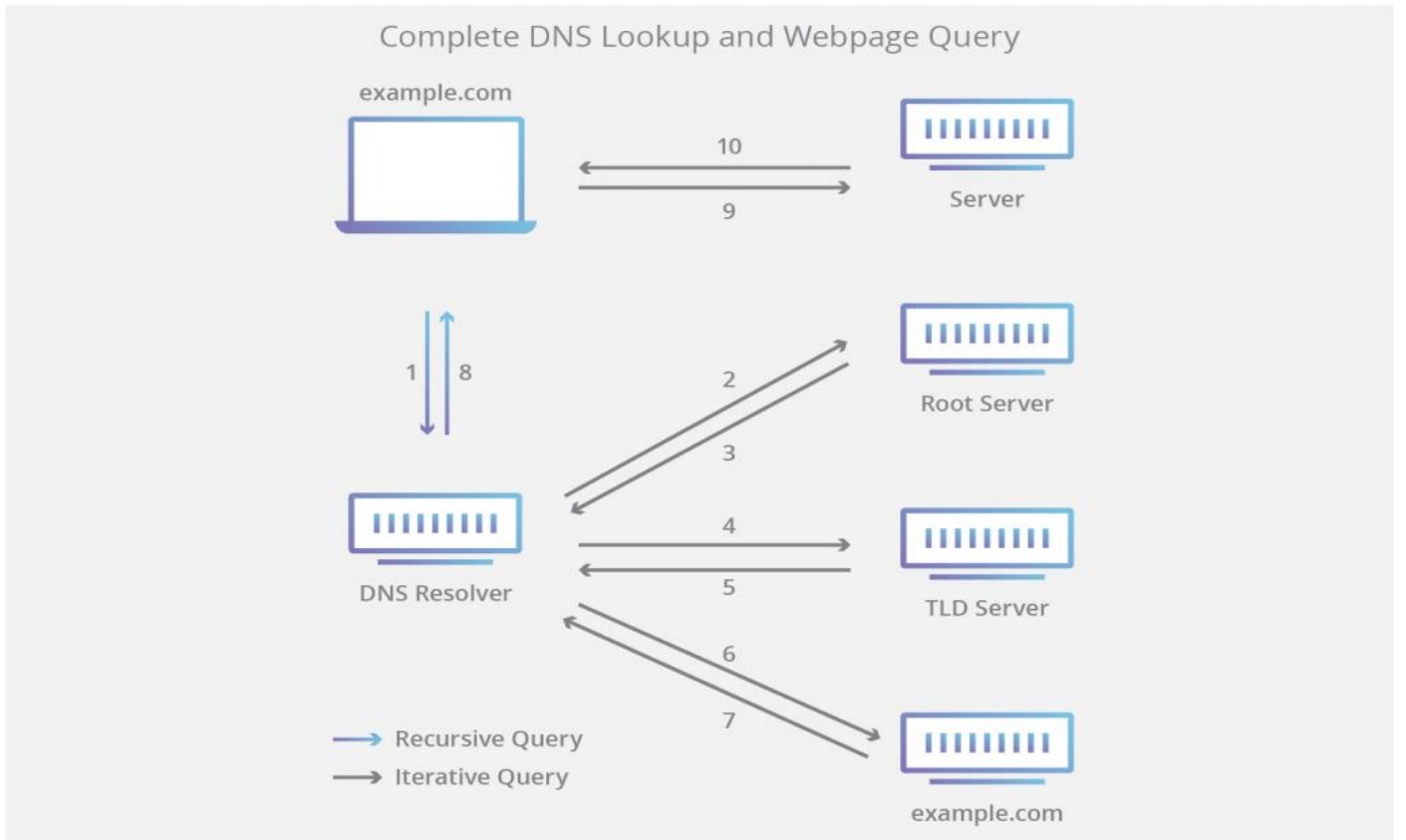
A Records:
- 140.82.121.3

DNS Arama Sorgusu Nasıl Çalışır?

DNS arama sorgularının nasıl çalıştığını bilmek ağ sorunlarının giderilmesinde yardımcı olmaktadır. Genel olarak nasıl çalıştığı şöyledir:

1. Web tarayıcısına URL girilir. Örneğin www.orneksite.com
2. Bu istek, bilgisayarınızdan bir DNS çözümleyicisine (genellikle internet servis sağlayıcınız tarafından sağlanır) gider. Bu çözümleyici, alan adının karşılık geldiği IP adresini bulmaya çalışır.
3. İlk olarak, çözümleyici kendi önbellegini kontrol eder. Daha önce aynı alan adı sorgulanmışsa, doğrudan bu kayıt kullanılır ve süreç hızlanır.
4. Önbellegde kayıt yoksa, çözümleyici kök DNS sunucularına bir sorgu gönderir. Bu sunucular, sizi yönlendirecek olan TLD (Üst Düzey Alan Adı) sunucularının nerede olduğunu söyler. (Örneğin, “.com” için ayrı bir sunucu bulunur.)
5. Ardından çözümleyici, ilgili TLD sunucusuna bir sorgu gönderir. Bu sunucu da sizi yetkili DNS sunucusuna yönlendirir – yani alan adının bağlı olduğu asıl sunucuya.
6. Yetkili DNS sunucusu, aradığınız alan adının gerçek IP adresini çözümleyiciye gönderir.
7. Çözümleyici bu IP adresini tarayıcınıza iletir.
8. Tarayıcınız artık doğru IP adresine sahip olduğu için, web sitesinin sunucusuna bağlanır ve sayfayı yükler.

Bu sistem saniyeler içinde işler, ancak arka planda oldukça organize bir süreçle çalışır. DNS'in bu karmaşık ama düzenli yapısı, internetin temellerinden biridir.



DNS Sorgu Türleri

Yinelemeli Sorgu (Recursive Query) : Yinelemeli sorgular, bir kullanıcının tarayıcısına bir web adresi yazmasıyla başlar. Bu aşamada DNS çözümleyicisi (resolver), talep edilen alan adının IP adresini bulmakla tamamen sorumludur. İlk olarak kendi önbellege bakar; eğer kayıt yoksa, doğru IP adresini bulana kadar kök DNS sunucularından başlayarak adım adım diğer sunuculara sorgu gönderir.

Yani kullanıcı bir kez istekte bulunur ve çözümleyici bu isteği nihai cevaba kadar takip eder. Sonuç olarak, kullanıcının cihazı sadece çözümleyiciden gelen yanıtı alır. Bu süreç genellikle hızlı çalışır ve kullanıcıya şeffaf bir deneyim sunar.

Tekrarlamalı Sorgu (Iterative Query) : Bu sorgu türünde, DNS çözümleyicisi bir ad sunucusuna istekte bulunduğunda, sunucu eğer cevabı biliyorsa doğrudan yanıt verir. Ancak bilgiye sahip değilse, çözümleyiciyi bir sonraki aşamaya yönlendirir – örneğin, “Bu konuda .com sunucusu yardımcı olabilir” diyerek ilgili sunucunun adresini verir.

Burada çözümleyici, her adımda yeni bir sunucuya kendisi sorgu gönderir. Sistem, IP adresini bulana kadar yönlendirilerek ilerler. Bu yapı, ağ üzerinde daha az yük oluşturur ve verimliliği artırır.

Tekrarlanmayan (Yetkili) Sorgu (Non-recursive Query) : Bu tür sorgular, çözümleyicinin doğrudan bilgiye sahip olan yetkili DNS sunucusuna ulaşması durumunda gerçekleşir. Eğer sunucu, sorgulanan alan adı hakkında kesin bilgiye sahipse, doğrudan ve eksiksiz bir yanıt döner.

Ancak bu yöntemde, tek sorguyla tüm detayları elde etmek mümkün olmayabilir. Bazen IP adresine ulaşmak için birkaç ek sorgu daha gerekebilir. Bu nedenle bu yöntem, bazı durumlarda daha yavaş çalışabilir.

Kaynakça :

Mailmodo. (t.y.). *DNS Lookup: What it is and how it works*. Erişim adresi:
<https://www.mailmodo.com/guides/dns-lookup/>

SONUÇ

Bu çalışmada geliştirilen Security Check platformu üzerinden, dijital güvenliğin temel taşları olan çeşitli analiz ve sorgulama araçları detaylı şekilde ele alınmıştır. Nmap ile yapılan port taramaları, Whois ile alan adı sahiplik kontrolleri, MX ve DMARC kayıtları ile e-posta güvenliği denetimleri, kara liste (Blacklist) kontrolleri ve DNS sorguları gibi birçok işlem, kullanıcıların çevrimiçi varlıklarını daha güvenli hale getirmeleri açısından büyük önem taşımaktadır.

Platformun sunduğu bu araçlar, yalnızca teknik uzmanlara değil, temel düzeyde bilgi sahibi olan kullanıcılara da dijital ortamda bilinçli hareket edebilme imkânı sunmaktadır. Her aracın nasıl çalıştığını bilmek, sadece güvenliğini artırmakla kalmaz; aynı zamanda ağ yönetimi, kimlik doğrulama ve bilgi sızdırma gibi sorunların önüne geçilmesine de yardımcı olur.

Giderek karmaşılaşan siber tehdit ortamında, bu tarz araçların doğru ve etik kullanımı, bireylerin ve kurumların dijital güvenliğe yönelik proaktif adımlar atabilmesini sağlar. Bu bağlamda Security Check, sadece bir platform değil; dijital güvenlik kültürünün gelişmesine katkı sağlayan bir araç niteliğindedir.

KAYNAKÇALAR :

- Karel. (t.y.). *Nmap nedir? Bu ağ tarayıcısına neden ihtiyacınız var?* Karel.
<https://www.karel.com.tr/blog/nmap-nedir-bu-ag-tarayicisina-neden-ihtiyaciniz-var>
- : Domain Hizmetleri. (t.y.). *WHOIS nedir?* Domain Hizmetleri.
<https://www.domainhizmetleri.com/blog/whois-nedir/>
- Uzman Posta. (t.y.). *MX Sorgulama Nedir? MX Kaydı Nedir, Nasıl Yapılır?* Erişim adresi:
<https://uzmanposta.com/mx-sorgulama>
- Ajans IO. (t.y.). *Blacklist Nedir? Nasıl Kontrol Edilir?* Erişim adresi:
<https://www.ajansio.com.tr/blacklist-nedir-nasil-kontrol-edilir>
- MXToolbox. (t.y.). *What is DMARC?* Erişim adresi: <https://mxtoolbox.com/dmarc/details/what-is-dmarc>
- Mailmodo. (t.y.). *DNS Lookup: What it is and how it works.* Erişim adresi:
<https://www.mailmodo.com/guides/dns-lookup/>