BİRUNİ UNIVERSITY
"Future of Science"

# Mühendislik Ve Doğa Bilimleri Fakültesi

## Bilgisayar Mühendisliği

# BLG424
# Ağ Güvenliği ve Şifrelemeye Giriş
# 2023 Güz



| | |
|---|---|
| Number: | 200404026 |
| Ad Ve Soyad : | Oğuz Sarı |
| WebSite: | yabanavmalzemeleri.com |

Test Türü:

- Blackbox Test

Amaç:

- Yabanavmalzemeleri.com web sitesinin güvenlik açıklarını dışarıdan bir saldırganın bakış açısıyla değerlendirmek.

Kapsam:.

a-)Pasif Bilgi Toplama:

- Genel Bakış
- Domain sonuçları
- Network bilgisi
- DNS bilgisi
- SPF Kaydı
- Site teknolojisi

b-) Hedef Web Sitesinin Ağ Haritasını Oluşturma

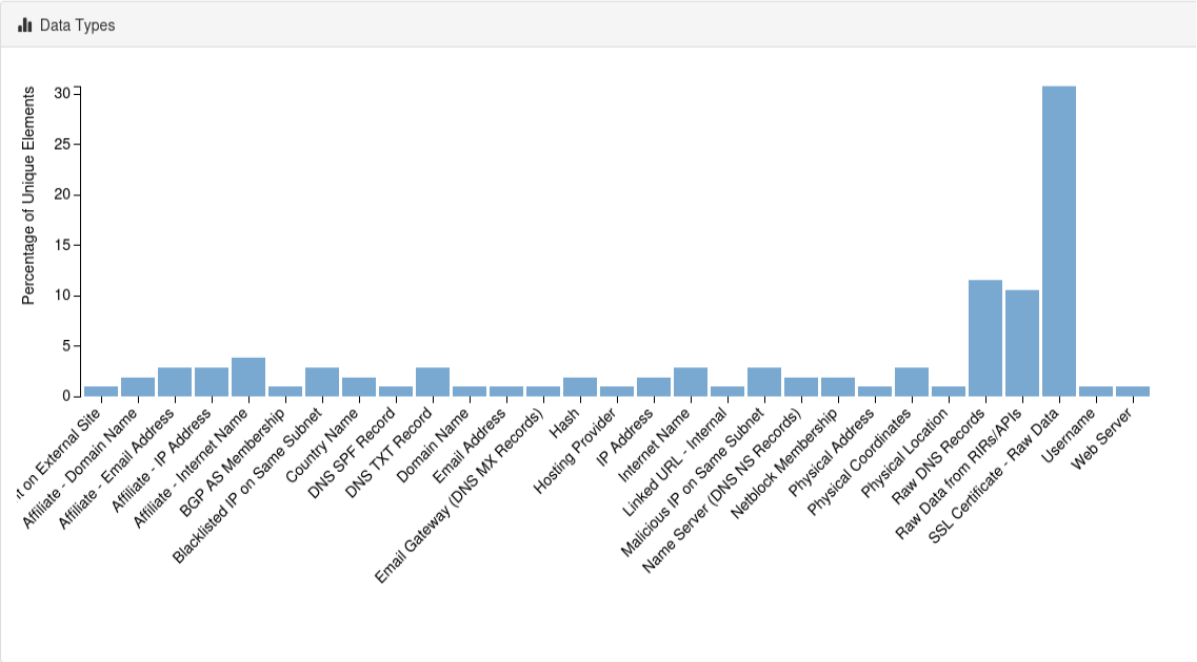
c-) Aktif Tarama:
- Nmap ile detaylı ağ taraması

Sınırlar:

- Sistem kaynaklı kesintilere sebep olacak testlerden kaçınılmıştır.
- Blackbox test yöntemi kullanıldığından, sistem ve ağ hakkında sınırlı bilgi edinilebilmiştir.
- Hukuki süreç oluşturulabilicek davranışlardan kaçınılmıştır. (Aktif Bilgi Toplama Sürecinde)

# Yabanavmalzemeleri.com ‘un Pasif Bilgi Toplama :

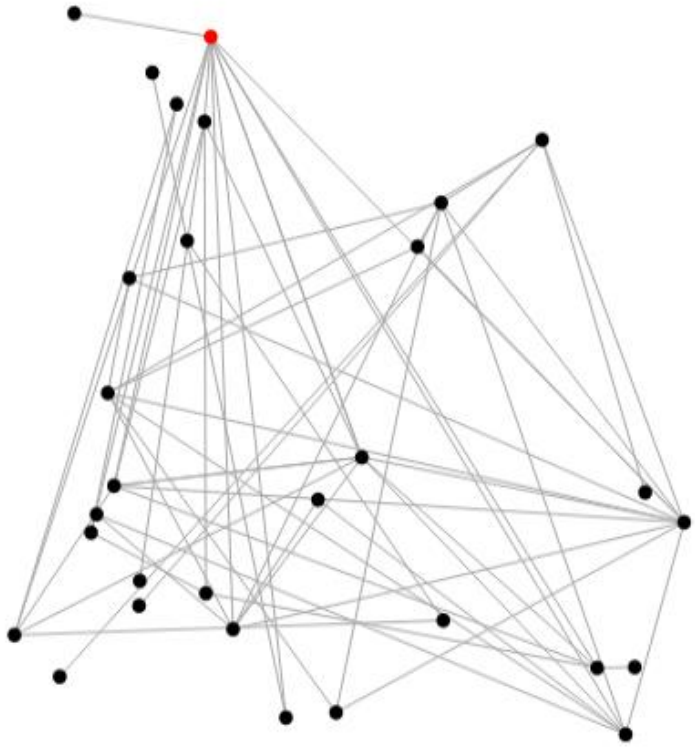
- GENEL BAKIŞ :
  Yabanavmalzemeleri.com Sitesindeki Veriler :




| Type | Unique Data Elements | Total Data Elements |
|---|---|---|
| Account on External Site | 1 | 1 |
| Affiliate - Domain Name | 2 | 5 |
| Affiliate - Email Address | 3 | 9 |
| Affiliate - IP Address | 3 | 3 |
| Affiliate - Internet Name | 4 | 10 |
| BGP AS Membership | 1 | 9 |
| Blacklisted IP on Same Subnet | 3 | 3 |
| Country Name | 2 | 4 |
| DNS SPF Record | 1 | 3 |
| DNS TXT Record | 3 | 9 |
| Domain Name | 1 | 2 |
| Email Address | 1 | 1 |
| Email Gateway (DNS MX Records) | 1 | 3 |
| Hash | 2 | 6 |
| Hosting Provider | 1 | 2 |
| IP Address | 2 | 4 |
| Internet Name | 3 | 62 |
| Linked URL - Internal | 1 | 3 |
| Malicious IP on Same Subnet | 3 | 3 |
| Name Server (DNS NS Records) | 2 | 6 |

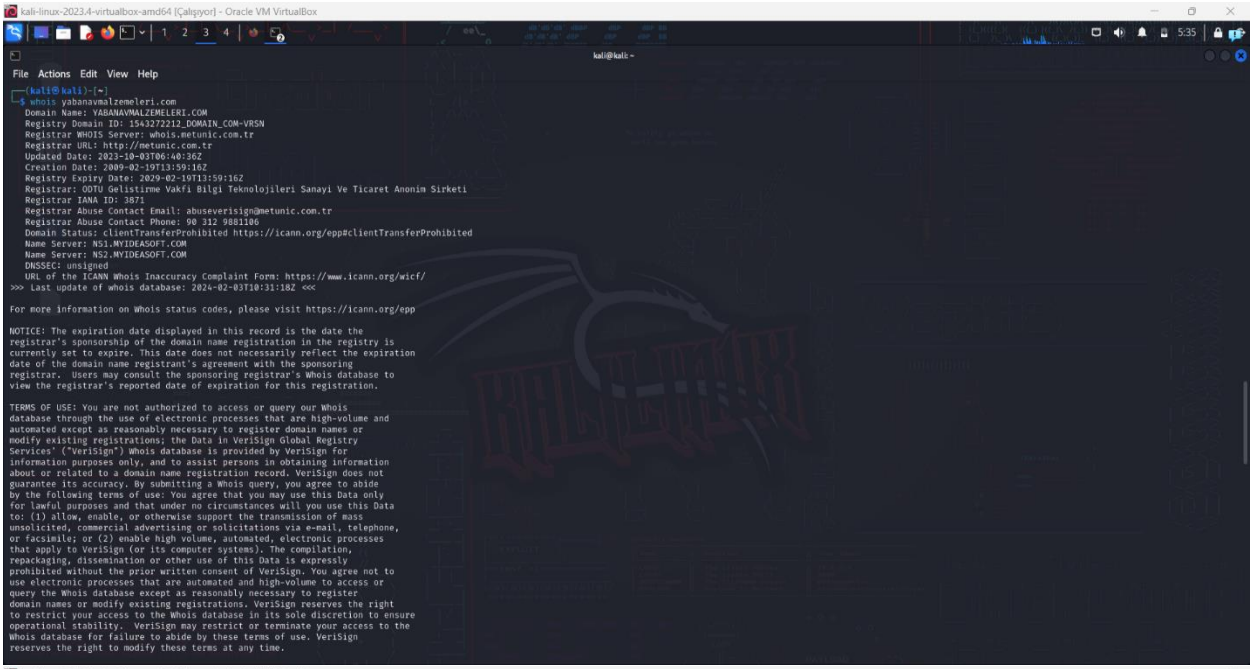
| | | |
|---|---|---|
| Netblock Membership | 2 | 6 |
| Physical Address | 1 | 3 |
| Physical Coordinates | 3 | 3 |
| Physical Location | 1 | 2 |
| Raw DNS Records | 12 | 12 |
| Raw Data from RIRs/APIs | 11 | 15 |
| SSL Certificate - Raw Data | 32 | 51 |
| Username | 1 | 1 |
| Web Server | 1 | 3 |

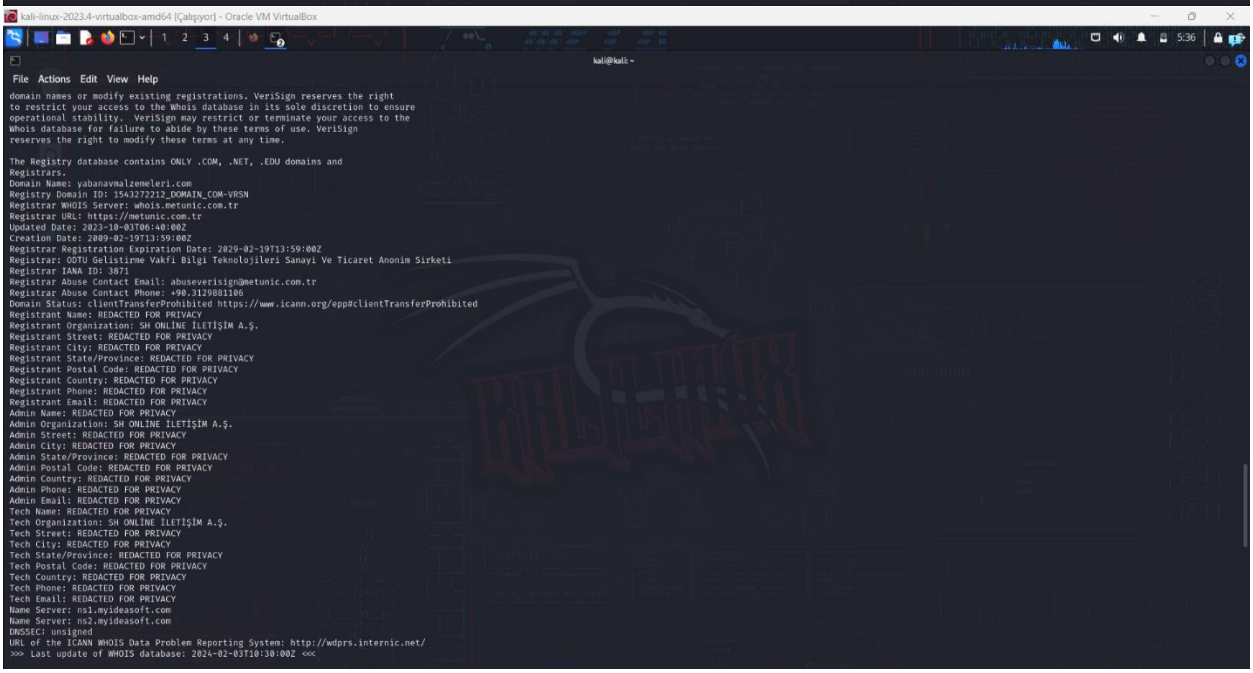
## Yabanavmalzemeleri.com Graf Yapısı :



## 1-)Domain Sorgusu :

- Whois Sorgusu :



Yukarıdaki resimlerde “yabanavmalzemeleri.com “ adlı sitenin whoıs sonuçları verilmiştir. Bu verilen sonuçlar ise şöyledir :

- Alan Adı Durumu: "yabanavmalzemeleri.com" alan adının kayıt durumu güncel ve 19 Şubat 2029 tarihine kadar geçerli. Ancak, "clientTransferProhibited" durumu, alan transferini şu anda engellediğini gösteriyor. Bu durum, alan sahibinin belirli bir dönemde başka bir kayıt sağlayıcıya transfer yapmasını sınırlayabilir.

- Kayıt Yaptıran ve WHOIS Sunucusu: ODTU Gelistirme Vakfi Bilgi Teknolojileri Sanayi Ve Ticaret Anonim Sirketi, alan adının kayıt yaptırıldığı ve WHOIS bilgilerinin sorgulandığı kuruluştur. Bu bilgiler, alan adıyla ilgili resmi kayıtların güncel ve sağlıklı bir şekilde tutulduğunu gösterir.

- Name Server Bilgileri: "yabanavmalzemeleri.com" için belirlenen iki adet name server, ns1.myideasoft.com ve ns2.myideasoft.com'dir. Bu name server'lar, alan adının DNS kayıtlarını yönetir ve web trafiğini yönlendirir.

- Kötüye Kullanım İletişim Bilgileri: Verilen kötüye kullanım iletişim e-postası (abuseverisign@metunic.com.tr) ve telefon numarası (+90.3129881106), alan adıyla ilgili kötüye kullanım veya güvenlik konularında iletişim kurmak için kullanılabilir.

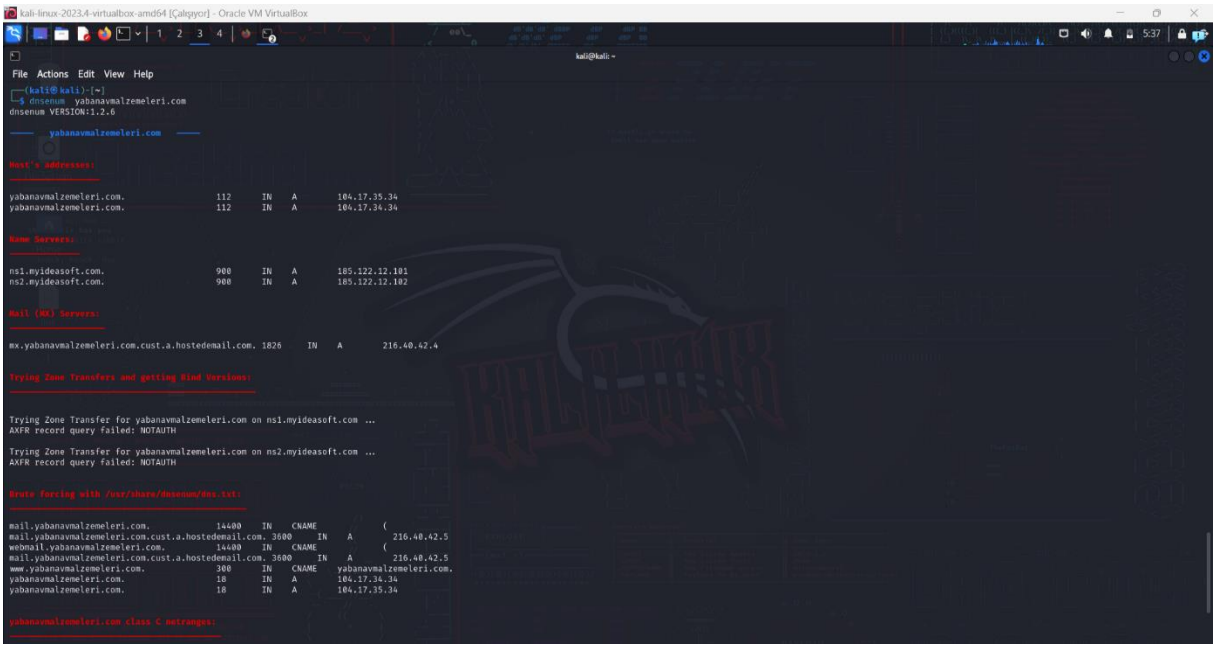
- Kayıt Sahibi Bilgileri: Kayıt sahibi olarak belirtilen "SH ONLİNE İLETİŞİM A.Ş." isimli firma, alan adının sahibidir. Ancak, bu aşamada daha fazla detay, kayıt sahibinin kimliği ve işletme bilgileri gizli tutulduğu için elde edilememektedir.

- Güncelleme Tarihi ve Güncellik Durumu: Son güncelleme 4 Şubat 2024 tarihinde yapıldı. Bu, WHOIS bilgilerinin güncel ve geçerli olduğunu gösterir. Ancak, bu tür bilgilerin düzenli olarak kontrol edilmesi ve güncellenmesi önemlidir.

Bu WHOIS bilgileri, "yabanavmalzemeleri.com" alan adının mevcut durumu, kayıt sağlayıcı, name server bilgileri ve kötüye kullanım iletişim bilgileri gibi önemli ayrıntıları içermektedir. Ancak, kayıt sahibi bilgilerinin gizliliği nedeniyle bazı detayları eksiktir.

## 2-) Dns Sorgusu :

- Dnsenum Sorgusu :





Yukarıdaki resimlerde “yabanavmalzemeleri.com “ adlı sitenin dnsenum sonuçları verilmiştir. Bu verilen sonuçlar ise şöyledir :

- Host IP Adresleri:

yabanavmalzemeleri.com, iki farklı IP adresine sahiptir: 104.17.34.34 ve 104.17.35.34.

- Name Servers (NS):

ns1.myideasoft.com ve ns2.myideasoft.com, yabanavmalzemeleri.com için name server (DNS sunucu) olarak belirlenmiştir.

- Mail (MX) Servers:

Mail sunucusu, mx.yabanavmalzemeleri.com.cust.a.hostedemail.com adresine işaret eder ve IP adresi 216.40.42.4'tür.

- Zone Transfer Denemeleri:

ns1.myideasoft.com ve ns2.myideasoft.com üzerinden yapılan zone transfer denemeleri başarısız olmuştur (NOTAUTH hata kodu alınmıştır). Bu, DNS sunucularının yetkilendirilmemiş talepleri reddettiğini gösterir.

- Brute Force Denemesi:

/usr/share/dnsenum/dns.txt dosyasını kullanarak yapılan brute force denemesi sonuçları arasında, CNAME kayıtları ve IP adresleriyle ilişkilendirilmiş alt alanlar bulunmaktadır.

- Reverse Lookup:

512 IP adresi üzerinde yapılan reverse lookup denemesi sonuç vermemiştir. Bu, IP adreslerinin alan adlarına çevrilemediğini gösterir.

- IP Blokları:

yabanavmalzemeleri.com'un IP blokları 104.17.34.0/24 ve 104.17.35.0/24'tür.

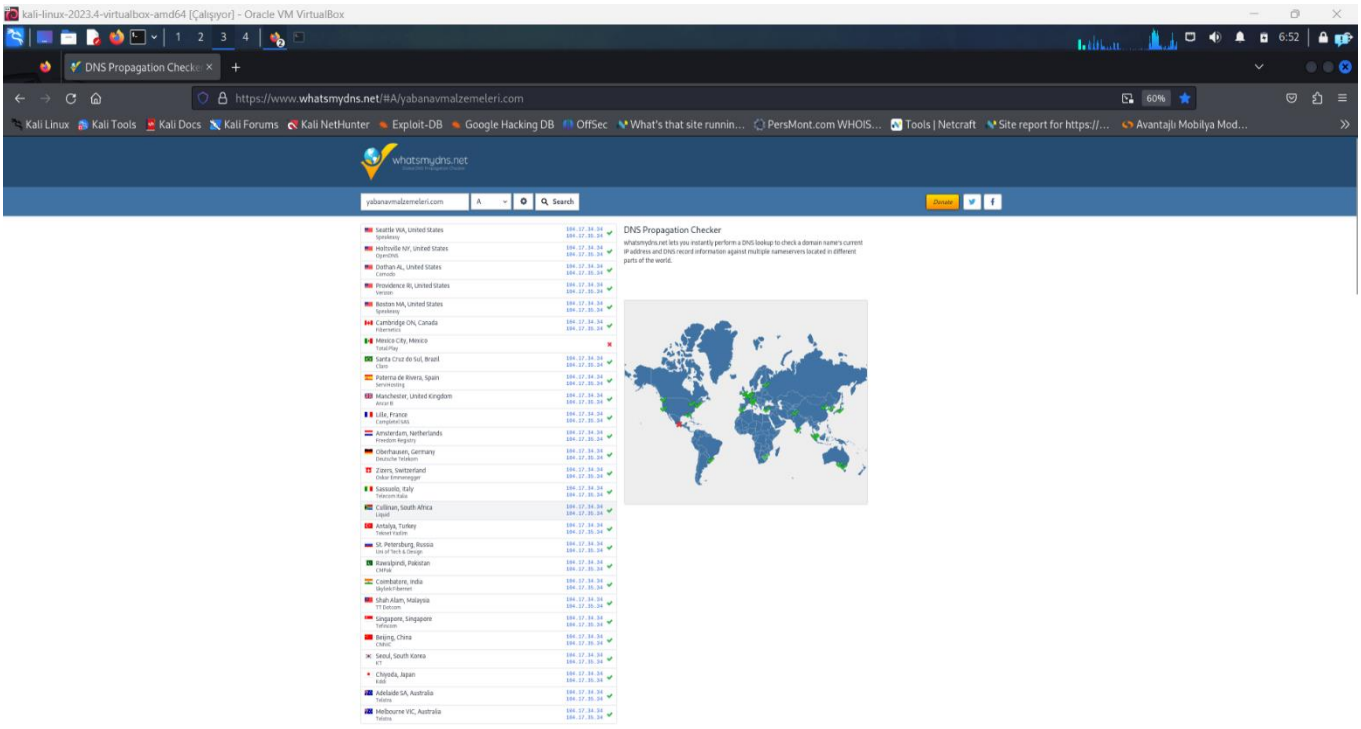
- Dns Kayıtları :

**DNS records**

| name | class | type | data | time to live |
|---|---|---|---|---|
| yabanavmalzemeleri.com | IN | A | 104.17.34.34 | 244s (00:04:04) |
| yabanavmalzemeleri.com | IN | A | 104.17.35.34 | 244s (00:04:04) |
| yabanavmalzemeleri.com | IN | NS | ns2.myideasoft.com | 86400s (1.00:00:00) |
| yabanavmalzemeleri.com | IN | NS | ns1.myideasoft.com | 86400s (1.00:00:00) |
| 34.35.17.104.in-addr.arpa | IN | HINFO | CPU: RFC8482<br>OS: | 3600s (01:00:00) |
| 17.104.in-addr.arpa | IN | NS | cruz.ns.cloudflare.com | 41418s (11:30:18) |
| 17.104.in-addr.arpa | IN | NS | kevin.ns.cloudflare.com | 41418s (11:30:18) |

Yukarıdaki resimde, "yabanavmalzemeleri.com" alan adına ait DNS kayıtları ve ilgili IP adresleri ile ilişkilendirilmiş ters DNS kayıtları hakkında bilgiler içermektedir.

- DNS Yayılma Kontrolcüsü:




Yukarıdaki resimde “yabanavmalzemeleri.com” ‘un mevcut IP adresini ve DNS kayıt bilgilerini dünya çapında farklı bölgelerde bulunan çeşitli nameserver'larla hemen karşılaştırıp ,DNS sorgusu gerçekleştirildi .

# 3-Network Sorgusu :

## Network

| | | | |
|---|---|---|---|
| **Site** | https://www.yabanavmalzemeleri.com | **Domain** | yabanavmalzemeleri.com |
| **Netblock Owner** | Cloudflare, Inc. | **Nameserver** | ns1.myideasoft.com |
| **Hosting company** | Cloudflare | **Domain registrar** | Unknown |
| **Hosting country** | US | **Nameserver organisation** | whois.registrar.eu |
| **IPv4 address** | 104.17.34.34 (VirusTotal) | **Organisation** | Unknown |
| **IPv4 autonomous systems** | AS13335 | **DNS admin** | domainmaster@myideasoft.com |
| **IPv6 address** | Not Present | **Top Level Domain** | Commercial entities (.com) |
| **IPv6 autonomous systems** | Not Present | **DNS Security Extensions** | Unknown |
| **Reverse DNS** | Unknown | | |

### IP delegation

**IPv4 address (104.17.34.34)**

| IP range | Country | Name | Description |
|---|---|---|---|
| ::ffff:0.0.0.0/96 | United States | IANA-IPV4-MAPPED-ADDRESS | Internet Assigned Numbers Authority |
| ↳ 104.0.0.0-104.255.255.255 | United States | NET104 | American Registry for Internet Numbers |
| ↳ 104.16.0.0-104.31.255.255 | United States | CLOUDFLARENET | Cloudflare, Inc. |
| ↳ 104.17.34.34 | United States | CLOUDFLARENET | Cloudflare, Inc. |

```
NetRange:       104.16.0.0 - 104.31.255.255
CIDR:           104.16.0.0/12
NetName:        CLOUDFLARENET
NetHandle:      NET-104-16-0-0-1
Parent:         NET104 (NET-104-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS13335
Organization:   Cloudflare, Inc. (CLOUD14)
RegDate:        2014-03-28
Updated:        2021-05-26
Comment:        All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref:            https://rdap.arin.net/registry/ip/104.16.0.0


OrgName:        Cloudflare, Inc.
OrgId:          CLOUD14
Address:        101 Townsend Street
City:           San Francisco
StateProv:      CA
PostalCode:     94107
Country:        US
RegDate:        2010-07-09
Updated:        2021-07-01
Ref:            https://rdap.arin.net/registry/entity/CLOUD14


OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse@cloudflare.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  rir@cloudflare.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

OrgNOCHandle: CLOUD146-ARIN
OrgNOCName:   Cloudflare-NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc@cloudflare.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN
```

```
RAbuseHandle: ABUSE2916-ARIN
RAbuseName:   Abuse
RAbusePhone:  +1-650-319-8930
RAbuseEmail:  abuse@cloudflare.com
RAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc@cloudflare.com
RNOCRef:    https://rdap.arin.net/registry/entity/NOC11962-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  rir@cloudflare.com
RTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN
```

Yukarıdaki resimlerde “yabanavmalzemeleri.com” adlı sitenin CDN sağlayıcısının Cloudflare olduğunu , Net Bilgileri, Organizasyon Bilgileri, Routing Bilgileri, NOC (Network Operations Center) Bilgileri, Teknik Bilgiler, Kötüye Kullanım (Abuse) Bilgileri, RNOCHandle (Reverse Network Operations Center) Bilgileri, RTechHandle (Reverse Technical) Bilgileri içermektedir .

# 4-) SPF Kaydı

| Qualifier | Mechanism | Argument |
|---|---|---|
| + (Pass) | mx | |
| + (Pass) | ip4 | 185.122.12.0/24 |
| + (Pass) | ip4 | 185.122.13.0/24 |
| + (Pass) | ip4 | 216.40.44.0/24 |
| + (Pass) | ip4 | 64.99.140.1/24 |
| - (Fail) | all | |

Yukarıdaki resimdeki SPF kaydı “yabanavmalzemeleri.com ” ’un ağ güvenliği kuralları veya güvenlik duvarı kurallarının bir listesidir. Üç sütunlu bir tablo olarak düzenlenmiştir: bir tanımlayıcı, bir mekanizma ve bir bağımsız değişken.

Tanımlayıcı sütununda, bir "+" (geç) veya "-" (başarısız) bulunur, bu da kuralın geçmesi veya engellenmesi gerektiğini gösterir.

Mekanizma sütunu, kuralın uygulandığı ağ mekanizma türünü belirtir. "mx" (posta değişim kayıtlarına başvuruyor) ve "ip4" (IPv4 adreslerine başvuruyor) değerleri vardır.

Bağımsız değişken sütunu, kuralın uygulandığı ağ varlığının özel ayrıntılarını içerir. IP adresleri veya alt ağlar.

Bu bilgilere dayanarak, kuralalaların ağ trafiği akışını denetlemek için hangi trafiklerin geçmesi veya engellenmesi gerektiğini belirlemesine yardımcı olmak için tasarlanmış olduklarını anlayabiliriz.

# 5-) Site Teknolojisi :

Aşağıda yer alan resimlerde, yabanavmalzemeleri.com adlı sitenin kullandığı teknolojiler, kullanım yerleri ve amaçları görülmektedir.

### HTTP Accelerator

A web accelerator is a proxy server that reduces web site access times.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Cloudflare | Content delivery network and distributed domain name server service | www.speedtest.net, www.inspq.qc.ca, www.ecosia.org |

### Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| PHP | PHP is supported and/or running | www.northamericanweather.net, www.babnet.net, www.w3schools.com |
| SSL | A cryptographic protocol providing communication security over the Internet | |

### Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

| Technology | Description | Popular sites using this technology |
|---|---|---|
| JavaScript | Widely-supported programming language commonly used to power client-side dynamic content on websites | accounts.google.com, l.facebook.com, mail.yahoo.com |

### Client-Side Scripting Frameworks

Frameworks or libraries allow for easier development of applications by providing an Application Program Interface (API) or a methodology to follow whilst developing.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| jQuery | A JavaScript library used to simplify the client-side scripting of HTML | www.amazon.ca, www.amazon.in, www.xvideos.com |

### Content Delivery Network

A content delivery network or content distribution network (CDN) is a large distributed system of servers deployed in multiple data centers in the Internet. The goal of a CDN is to serve content to end-users with high availability and high performance.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Cloudflare | Content delivery network and distributed domain name server service | www.chess.com, www.coingecko.com, www.ilovepdf.com |

### E-Commerce

Electronic commerce, commonly known as e-commerce, is the buying and selling of product or service over electronic systems such as the Internet and other computer networks.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| General Domain Holding | Loading temporary content under a domain name | www.essig-oel.de, www.taosamuebles.com, www.arco.co.uk |

## Mobile Technologies

Mobile technology is the technology used for hand held mobile devices.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Click to call | Markup language syntax intended for devices that can place calls (e.g. phones, VoIP, etc.) | www.nk.ca, www.fxpro.com, aspen.eccouncil.org |

## Web Stats

Web analytics is the measurement, collection, analysis and reporting of internet data for purposes of understanding and optimizing web usage.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Google Webmaster Tools | Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google | www.pinterest.com, www.disneyplus.com, www.ebay.com |

## Character Encoding

A character encoding system consists of a code that pairs each character from a given repertoire with something else such as a bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| UTF8 | UCS Transformation Format 8 bit | |

## HTTP Compression

HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Gzip Content Encoding | Gzip HTTP Compression protocol | www.virustotal.com, www.wildberries.ru, www.newsit.gr |

## Web Browser Targeting

Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| X-Content-Type-Options | Browser MIME type sniffing is disabled | www.facebook.com, www.linkedin.com, outlook.office.com |
| Content Security Policy | Detect and mitigate attacks in the browser | www.deepl.com, discord.com, twitter.com |
| X-XSS-Protection Block | Block pages on which cross-site scripting is detected | www.binance.com, mail-redir.mention.com, mail.google.com |

## Doctype

A Document Type Declaration, or DOCTYPE, is an instruction that associates a particular SGML or XML document (for example, a webpage) with a Document Type Definition (DTD).

| Technology | Description | Popular sites using this technology |
|---|---|---|
| HTML5 | Latest revision of the HTML standard, the main markup language on the web | |

## HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

| Technology | Description | Popular sites using this technology |
|---|---|---|
| Viewport meta tag | HTML5 tag usually used for mobile optimization | learn.microsoft.com |

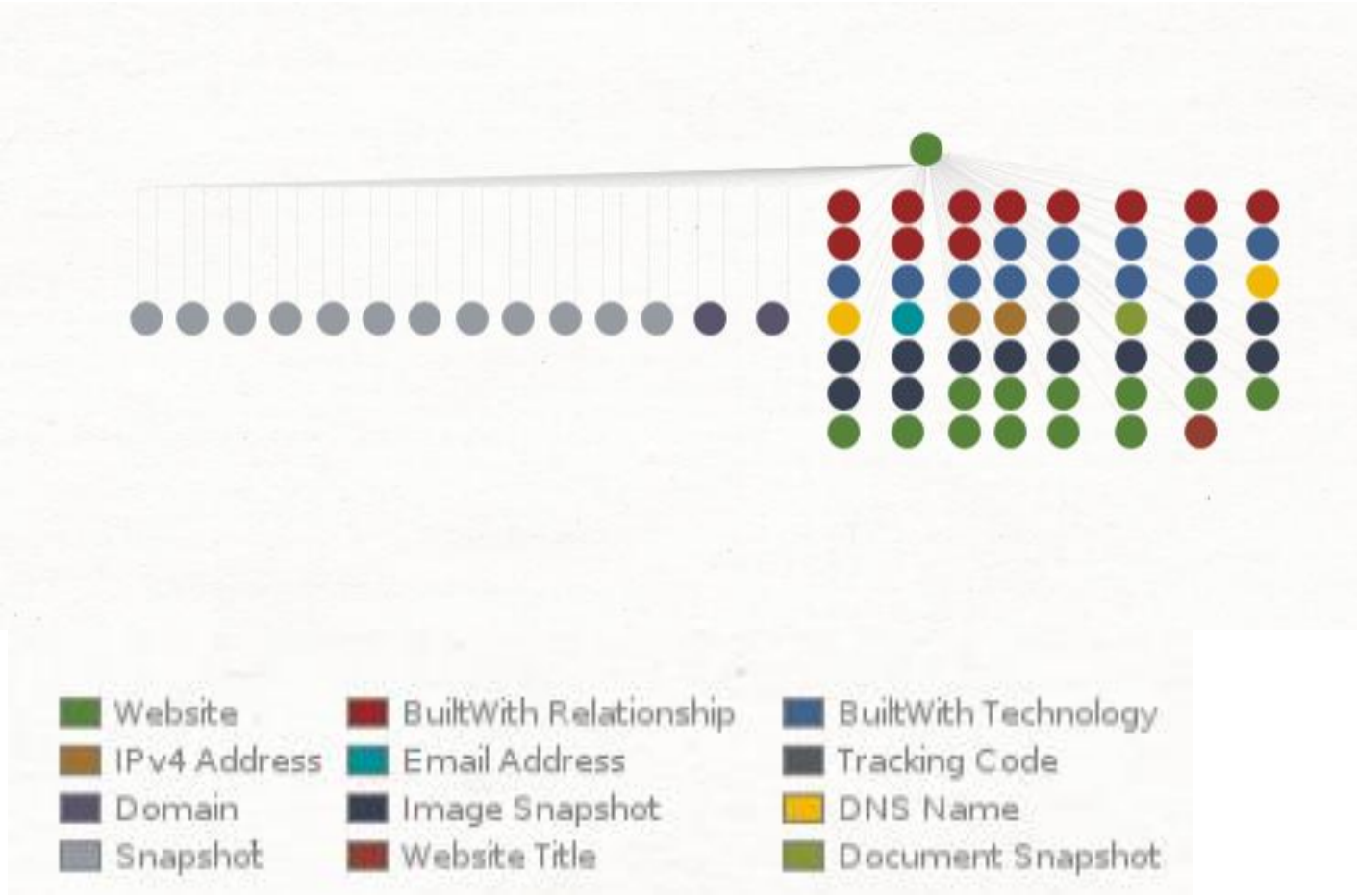
## CSS Usage

Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

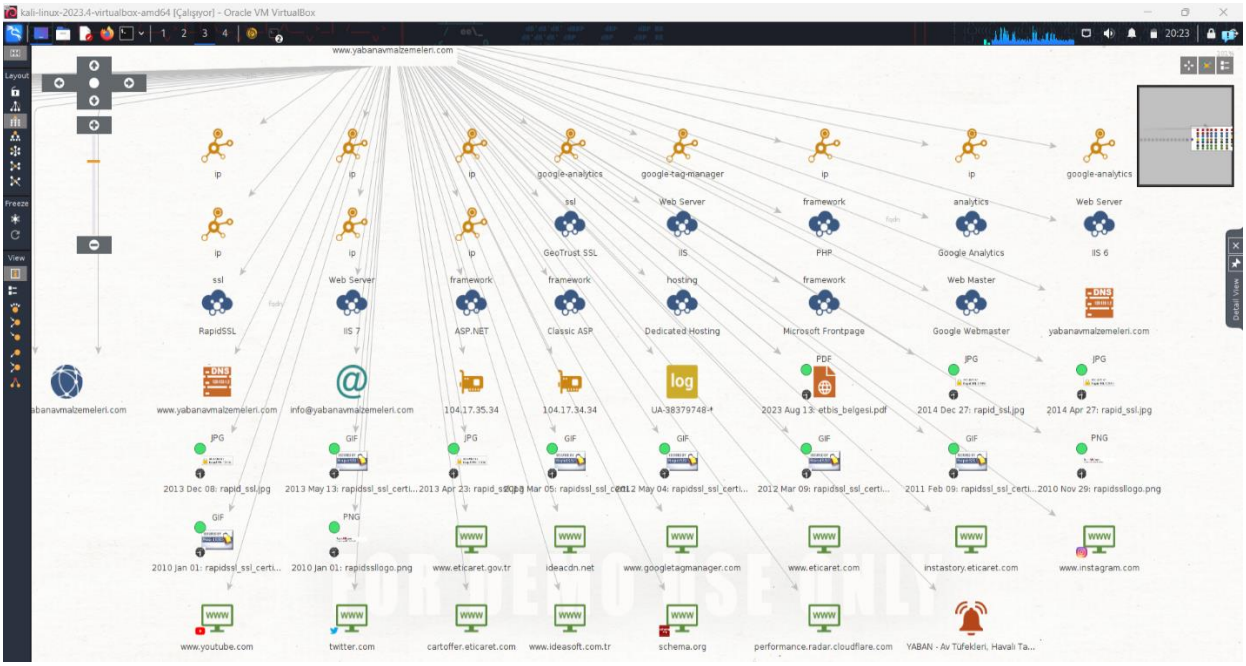
| Technology | Description | Popular sites using this technology |
|---|---|---|
| Embedded | Styles defined within a webpage | www.amazon.es, www.aliexpress.com, www.portail-emploi.fr |
| External | Styles defined within an external CSS file | www.instagram.com, www.twitch.tv, www.netflix.com |

# Yabanavmalzemeleri.com ‘un Ağ Yapısı

- Genel Görünüm :

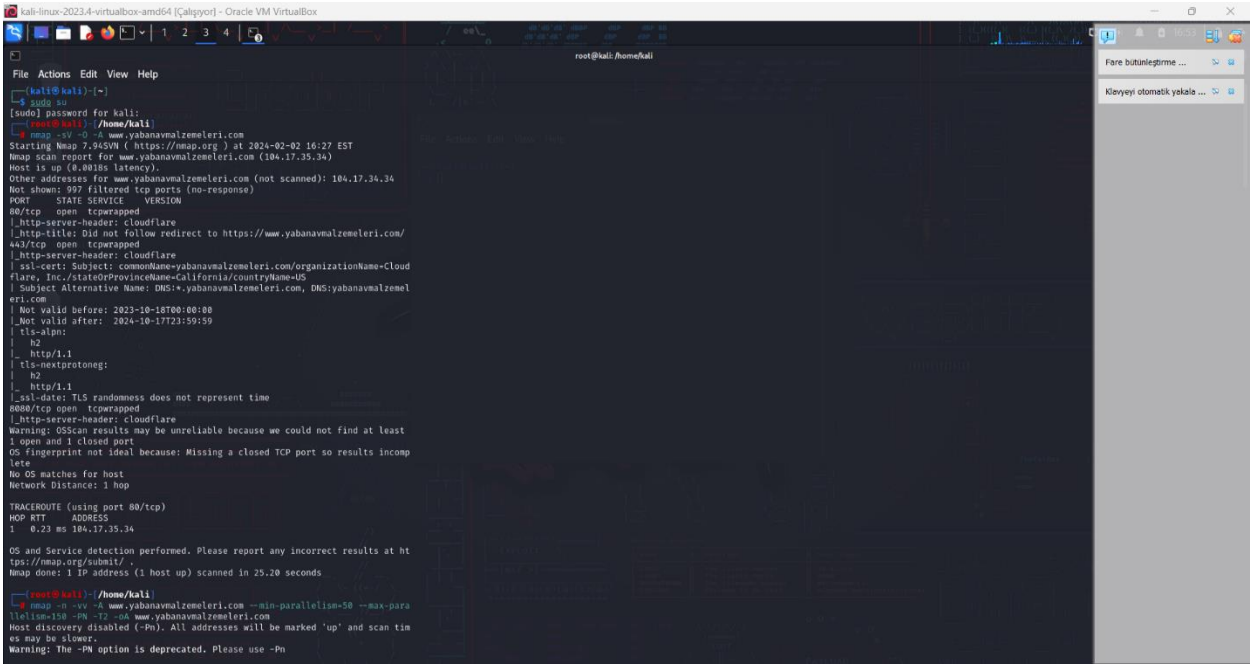


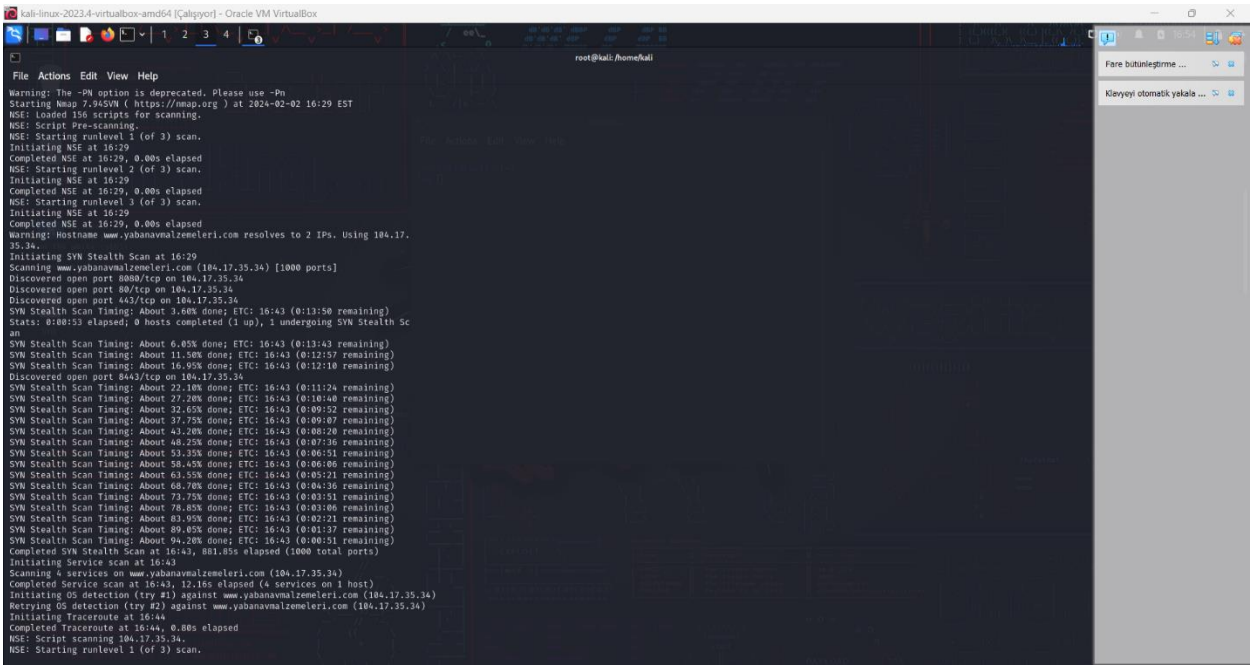
- Detaylı Görünüm :

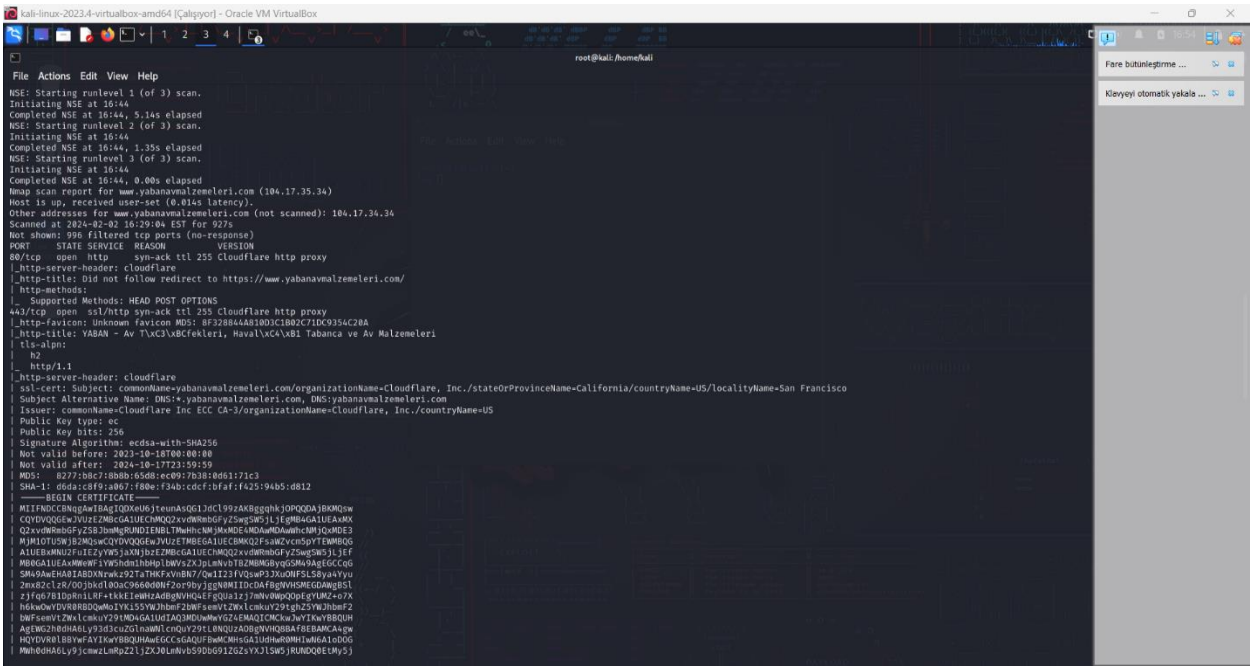


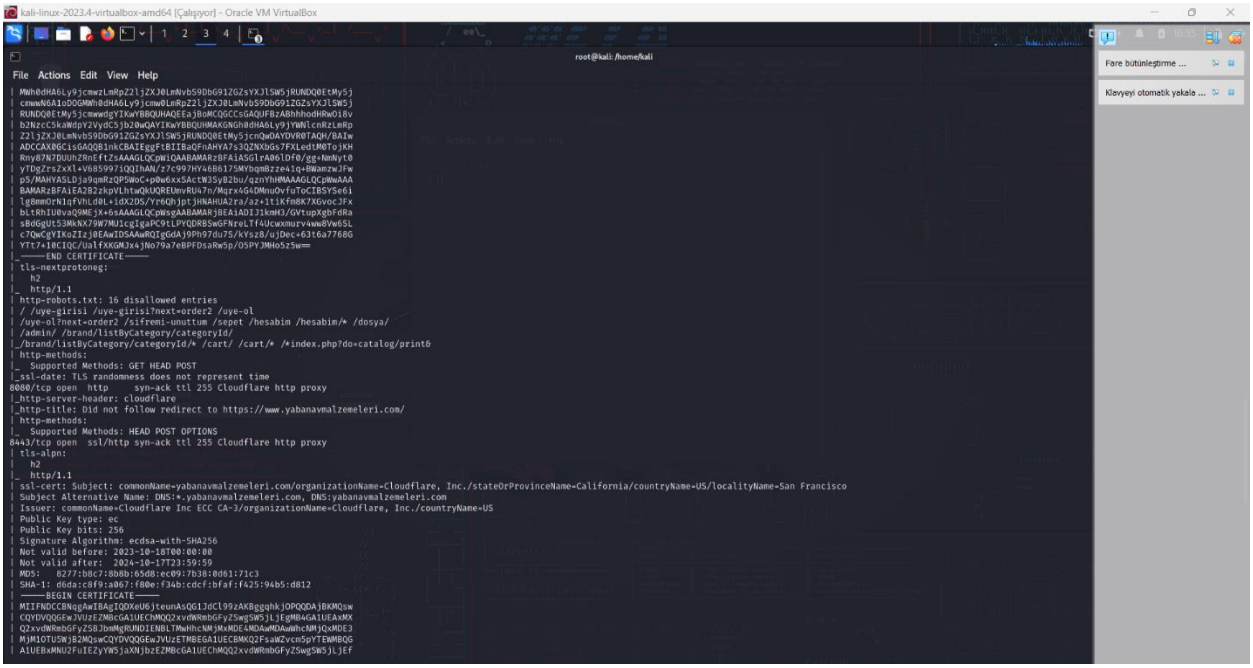

# Yabanavmalzemeleri.com ‘un Aktif Taraması :

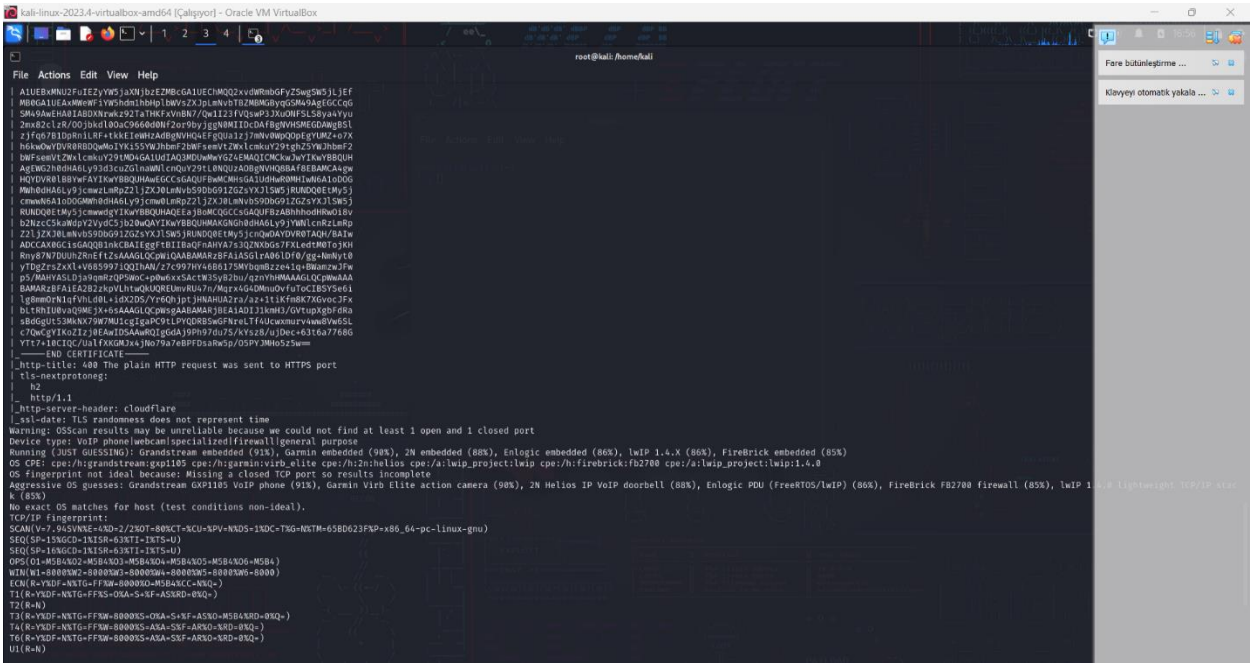
- Nmap taraması

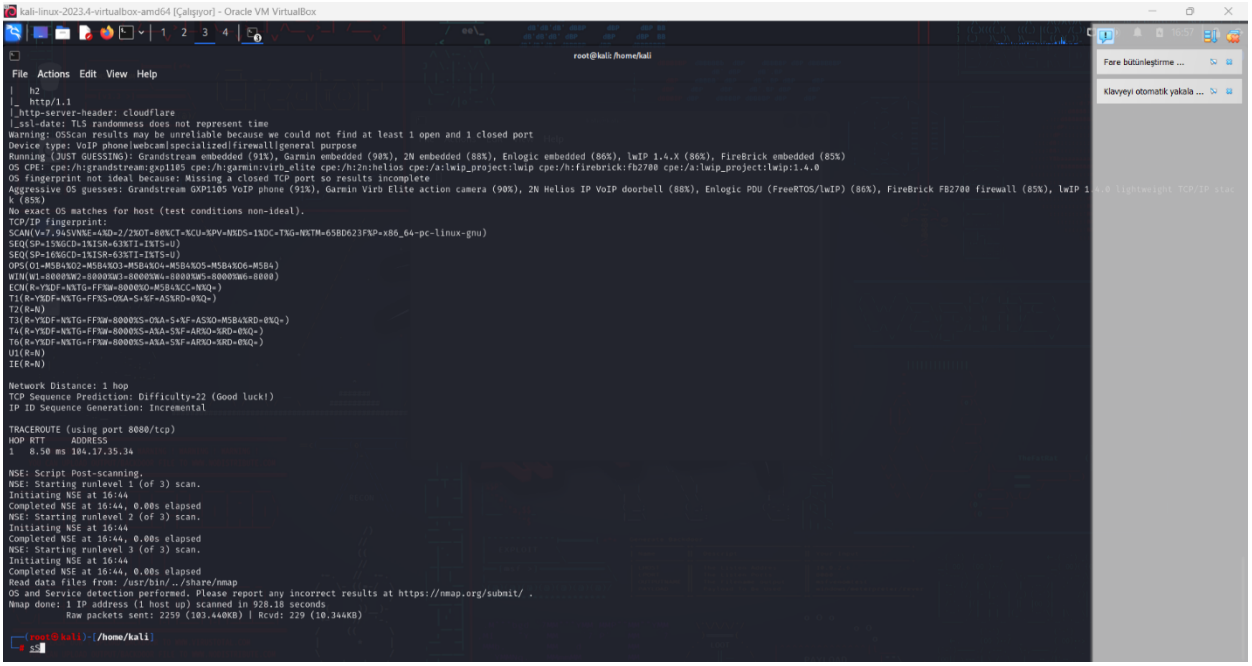



kali-linux-2023.4-virtualbox-amd64 [Çalışıyor] - Oracle VM VirtualBox
root@kali: /home/kali
File Actions Edit View Help
Fare bütünleştirme ...
Klavyeyi otomatik yakala ...


kali-linux-2023.4-virtualbox-amd64 [Çalışıyor] - Oracle VM VirtualBox
root@kali: /home/kali
File Actions Edit View Help
Fare bütünleştirme ...
Klavyeyi otomatik yakala ...




Yukarıdaki resimlerde nmap taraması yapılmıştır. Yapılan Tarama Sonrasında ulaşılan bilgiler şöyledir :

- Port Durumları:

80/tcp: Açık, "http" servisi kullanılıyor. Cloudflare üzerinden bir HTTP proxy görülmekte. Ancak bu port üzerinde yapılan HTTP isteği, HTTPS portuna yönlendiriliyor.
443/tcp: Açık, "ssl/http" servisi kullanılıyor. Cloudflare üzerinden bir HTTP proxy görülmekte.
8080/tcp: Açık, "http" servisi kullanılıyor. Cloudflare üzerinden bir HTTP proxy görülmekte.
8443/tcp: Açık, "ssl/http" servisi kullanılıyor. Cloudflare üzerinden bir HTTP proxy görülmekte.

- SSL/TLS Sertifikası:

Sertifika, "yabanavmalzemeleri.com" alan adına ve Cloudflare tarafından sağlanmış gibi görünüyor. Sertifika, 2023-10-18 tarihinden başlayarak ve 2024-10-17 tarihine kadar geçerli.

- HTTP Sunucu Bilgileri:

HTTP başlıkları, sunucunun Cloudflare tarafından barındırıldığını gösteriyor.

- OS ve Servis Algılama:

Host, VoIP telefon, webcam, firewall gibi cihazları içeren genel bir amaçlı bir işletim sistemine sahip gibi görünüyor. Ancak, bir kapalı TCP portu bulunamadığı için OS tespiti kesin değil.

- Web Uygulama Bilgileri:

Ana web uygulamasının HTTPS kullanması gerektiği, ancak bazı isteklerin HTTP üzerinden yapıldığı görülüyor.
"robots.txt" dosyası, belirli dizinlere ve sayfalara erişimde kısıtlamalar içermekte.

- Hizmet Algılama ve Versiyon Bilgileri:

4 farklı servis algılanmış: HTTP, HTTPS, HTTP alternatifi (8080/tcp) ve HTTPS alternatifi (8443/tcp).
HTTP başlıkları ve içerikleri incelendi. HTTPS portu için sunucu başlıkları, "YABAN - Av Tüfekleri, Havalı Tabanca ve Av Malzemeleri" ifadesini içeriyor.