



**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:

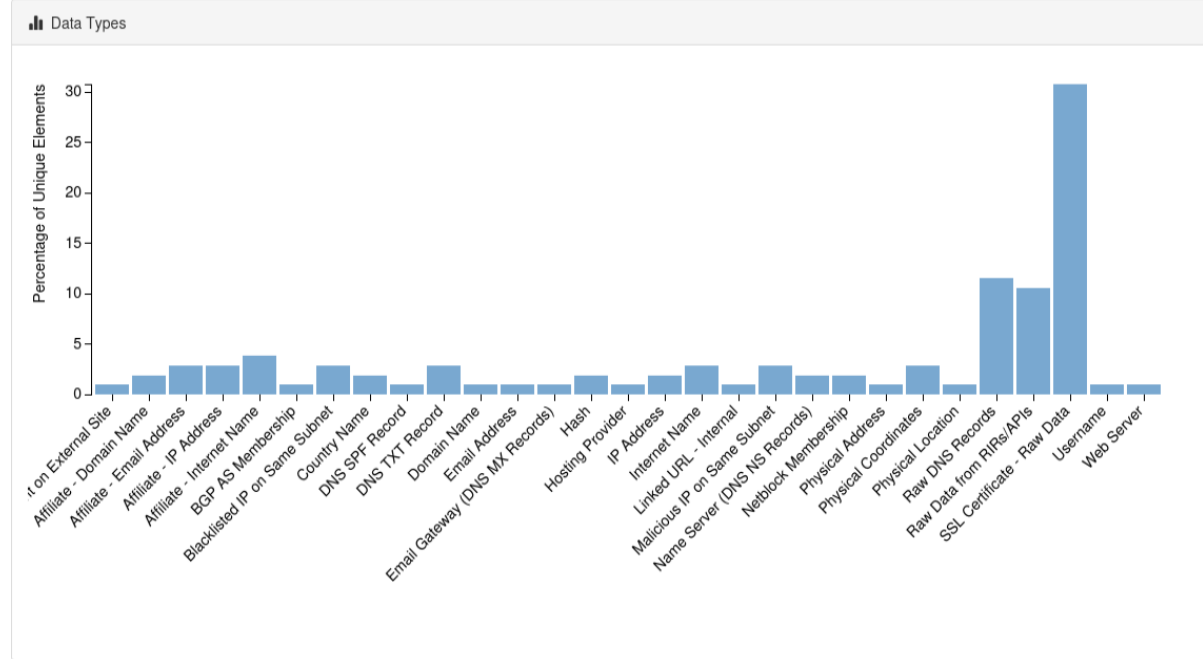
- Nmap ile detaylı ağ taraması

Sınırlar:

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

# Yabanavmalzemeleri.com 'un Pasif Bilgi Toplama :

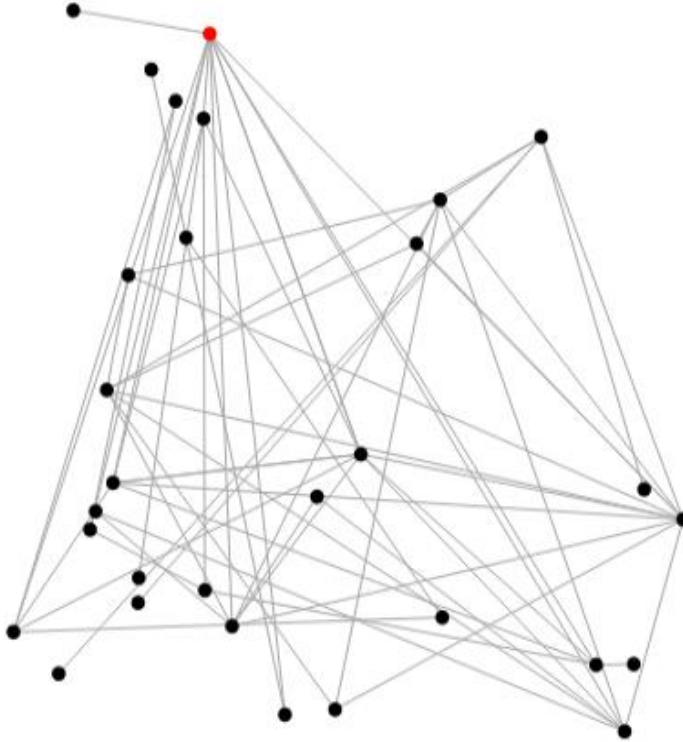
- GENEL BAKIŞ :  
Yabanavmalzemeleri.com Sitesindeki Veriler :



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 :

```
kali@kali:~$ whois yabanaymalzemeleri.com
Domain Name: YABANAYMALZEMELERI.COM
Registry Domain ID: 1543272212_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.metunic.com.tr
Registrar URL: http://metunic.com.tr
Updated Date: 2023-10-03T06:40:00Z
Creation Date: 2009-02-19T13:59:16Z
Registry Expiry Date: 2029-02-19T13:59:16Z
Registrar: ODTU Gelistirme Vakfi Bilgi Teknolojileri Sanayi Ve Ticaret Anonim Sirketi
Registrar IANA ID: 3871
Registrar Abuse Contact Email: abuseverisign@metunic.com.tr
Registrar Abuse Contact Phone: +90 312 5881186
Domain Status: clientTransferProhibited https://icann.org/epp/clientTransferProhibited
Name Server: NS1.MYIDEASOFT.COM
Name Server: NS2.MYIDEASOFT.COM
DNSSEC: unsigned
URL of the ICANN whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-02-03T18:31:18Z <<<

For more information on whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrant's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: yabanaymalzemeleri.com
Registry Domain ID: 1543272212_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.metunic.com.tr
Registrar URL: https://metunic.com.tr
Updated Date: 2023-10-03T06:40:00Z
Creation Date: 2009-02-19T13:59:16Z
Registrar Registration Expiration Date: 2029-02-19T13:59:00Z
Registrar: ODTU Gelistirme Vakfi Bilgi Teknolojileri Sanayi Ve Ticaret Anonim Sirketi
Registrar IANA ID: 3871
Registrar Abuse Contact Email: abuseverisign@metunic.com.tr
Registrar Abuse Contact Phone: +90 312 5881186
Domain Status: clientTransferProhibited https://www.icann.org/epp/clientTransferProhibited
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: SM ONLINE İLETİŞİM A.Ş.
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: REDACTED FOR PRIVACY
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: REDACTED FOR PRIVACY
Registrant Phone: REDACTED FOR PRIVACY
Registrant Email: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: SM ONLINE İLETİŞİM A.Ş.
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Email: REDACTED FOR PRIVACY
Tech Name: REDACTED FOR PRIVACY
Tech Organization: SM ONLINE İLETİŞİM A.Ş.
Tech Street: REDACTED FOR PRIVACY
Tech City: REDACTED FOR PRIVACY
Tech State/Province: REDACTED FOR PRIVACY
Tech Postal Code: REDACTED FOR PRIVACY
Tech Country: REDACTED FOR PRIVACY
Tech Phone: REDACTED FOR PRIVACY
Tech Email: REDACTED FOR PRIVACY
Name Server: ns1.myideasoft.com
Name Server: ns2.myideasoft.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-02-03T18:30:00Z <<<
```

Yukarıdaki resimlerde “yabanavmalzemeleri.com “ adlı sitenin whois 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 sınırlandırabilir.
- Kayıt Yaptıran ve WHOIS Sunucusu: ODTU Gelistirme Vakfı Bilgi Teknolojileri Sanayi Ve Ticaret Anonim Şirketi, 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 ONLINE 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 :

```
kali-linux-2023.4-virtualbox-amd64 [Calegyor] - Oracle VM VirtualBox
kali@kali:~$ dnsenum yabanavmalzemeleri.com
dnsenum VERSION:1.2.6

yabanavmalzemeleri.com

Host's addresses:
yabanavmalzemeleri.com.      112    IN    A     104.17.35.34
yabanavmalzemeleri.com.      112    IN    A     104.17.34.34

Name Servers:
ns1.myideasoft.com.          900    IN    A     185.122.12.181
ns2.myideasoft.com.          900    IN    A     185.122.12.182

Mail (MX) Servers:
mx.yabanavmalzemeleri.com.cust.a.hostedemail.com. 1826    IN    A     216.40.42.4

Trying Zone Transfers and getting Rnd versions:

Trying Zone Transfer for yabanavmalzemeleri.com on ns1.myideasoft.com ...
AXFR record query failed: NOTAUTH
Trying Zone Transfer for yabanavmalzemeleri.com on ns2.myideasoft.com ...
AXFR record query failed: NOTAUTH

Brute forcing with /usr/share/dnsenum/dns.txt:
mail.yabanavmalzemeleri.com.      14400  IN    CNAME ( 216.40.42.5
webmail.yabanavmalzemeleri.com.  14400  IN    CNAME ( 216.40.42.5
mail.yabanavmalzemeleri.com.cust.a.hostedemail.com. 3600    IN    A     216.40.42.5
www.yabanavmalzemeleri.com.       300    IN    CNAME yabanavmalzemeleri.com.
yabanavmalzemeleri.com.           18     IN    A     104.17.34.34
yabanavmalzemeleri.com.           18     IN    A     104.17.35.34

yabanavmalzemeleri.com class C netranges:
```

```
yabanavmalzemeleri.com class C netranges:
104.17.34.0/24
104.17.35.0/24

Performing reverse lookup on 512 IP addresses:
0 results out of 512 IP addresses.

yabanavmalzemeleri.com ip blocks:
done.
kali@kali:~$
```

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.



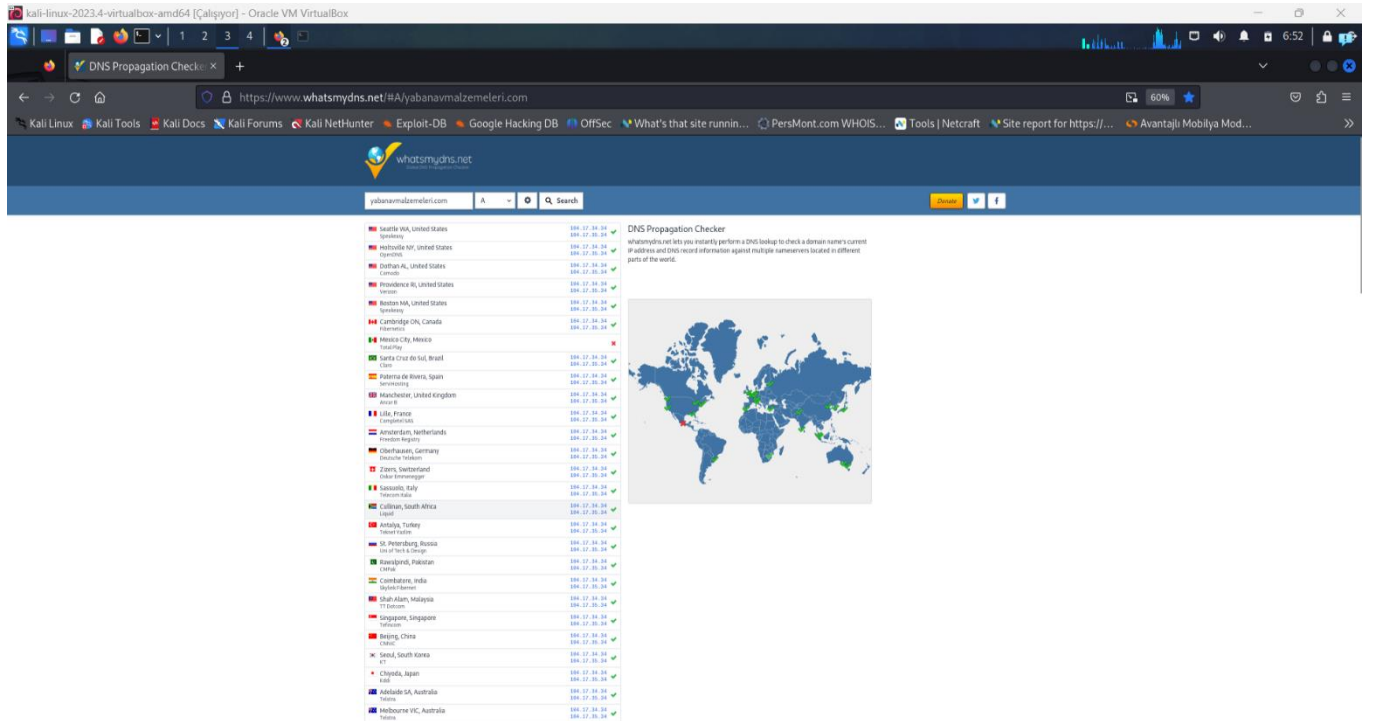
- Dns Kayıtları :

### 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 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	<a href="https://www.yabanavmalzemeleri.com">https://www.yabanavmalzemeleri.com</a>	Domain	<a href="https://www.yabanavmalzemeleri.com">yabanavmalzemeleri.com</a>
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 <a href="#">(VirusTotal ID)</a>	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](mailto:abuse@cloudflare.com)  
 OrgAbuseRef: <https://rdap.arin.net/registry/entity/ABUSE2916-ARIN>

OrgTechHandle: ADMIN2521-ARIN  
 OrgTechName: Admin  
 OrgTechPhone: +1-650-319-8930  
 OrgTechEmail: [r1r@cloudflare.com](mailto:r1r@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](mailto: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  
RNOCHandle: NOC  
RNOCHandle: +1-650-319-8930  
RNOCHandle: noc@cloudflare.com  
RNOCHandle: 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
+	mx	
+	ip4	185.122.12.0/24
+	ip4	185.122.13.0/24
+	ip4	216.40.44.0/24
+	ip4	64.99.140.1/24
-	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, kuralaların 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 <a href="#">↗</a>	Content delivery network and distributed domain name server service	<a href="http://www.speedtest.net">www.speedtest.net</a> , <a href="http://www.inspq.qc.ca">www.inspq.qc.ca</a> , <a href="http://www.ecosia.org">www.ecosia.org</a>

### 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 <a href="#">↗</a>	PHP is supported and/or running	<a href="http://www.northamericanweather.net">www.northamericanweather.net</a> , <a href="http://www.babnet.net">www.babnet.net</a> , <a href="http://www.w3schools.com">www.w3schools.com</a>
SSL <a href="#">↗</a>	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 <a href="#">↗</a>	Widely-supported programming language commonly used to power client-side dynamic content on websites	<a href="http://accounts.google.com">accounts.google.com</a> , <a href="http://l.facebook.com">l.facebook.com</a> , <a href="http://mail.yahoo.com">mail.yahoo.com</a>

### 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 href="#">↗</a>	A JavaScript library used to simplify the client-side scripting of HTML	<a href="http://www.amazon.ca">www.amazon.ca</a> , <a href="http://www.amazon.in">www.amazon.in</a> , <a href="http://www.xvideos.com">www.xvideos.com</a>

### 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 <a href="#">↗</a>	Content delivery network and distributed domain name server service	<a href="http://www.chess.com">www.chess.com</a> , <a href="http://www.coingecko.com">www.coingecko.com</a> , <a href="http://www.ilovepdf.com">www.ilovepdf.com</a>

### 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	<a href="http://www.essig-oel.de">www.essig-oel.de</a> , <a href="http://www.taosamuebles.com">www.taosamuebles.com</a> , <a href="http://www.arco.co.uk">www.arco.co.uk</a>

## Mobile Technologies

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

Technology	Description	Popular sites using this technology
Click to call <a href="#">🔗</a>	Markup language syntax intended for devices that can place calls (e.g. phones, VoIP, etc.)	<a href="http://www.nk.ca">www.nk.ca</a> , <a href="http://www.fxpro.com">www.fxpro.com</a> , <a href="http://aspen.eccouncil.org">aspen.eccouncil.org</a>

## 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 <a href="#">🔗</a>	Set of tools allowing webmasters to check indexing status and optimize visibility of their websites on Google	<a href="http://www.pinterest.com">www.pinterest.com</a> , <a href="http://www.disneyplus.com">www.disneyplus.com</a> , <a href="http://www.ebay.com">www.ebay.com</a>

## 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 <a href="#">🔗</a>	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 <a href="#">🔗</a>	Gzip HTTP Compression protocol	<a href="http://www.virustotal.com">www.virustotal.com</a> , <a href="http://www.wildberries.ru">www.wildberries.ru</a> , <a href="http://www.newsit.gr">www.newsit.gr</a>

## 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 <a href="#">🔗</a>	Browser MIME type sniffing is disabled	<a href="http://www.facebook.com">www.facebook.com</a> , <a href="http://www.linkedin.com">www.linkedin.com</a> , <a href="http://outlook.office.com">outlook.office.com</a>
Content Security Policy <a href="#">🔗</a>	Detect and mitigate attacks in the browser	<a href="http://www.deepl.com">www.deepl.com</a> , <a href="http://discord.com">discord.com</a> , <a href="http://twitter.com">twitter.com</a>
X-XSS-Protection Block <a href="#">🔗</a>	Block pages on which cross-site scripting is detected	<a href="http://www.binance.com">www.binance.com</a> , <a href="http://mail-redir.mention.com">mail-redir.mention.com</a> , <a href="http://mail.google.com">mail.google.com</a>

## 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 <a href="#">🔗</a>	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	<a href="http://learn.microsoft.com">learn.microsoft.com</a>

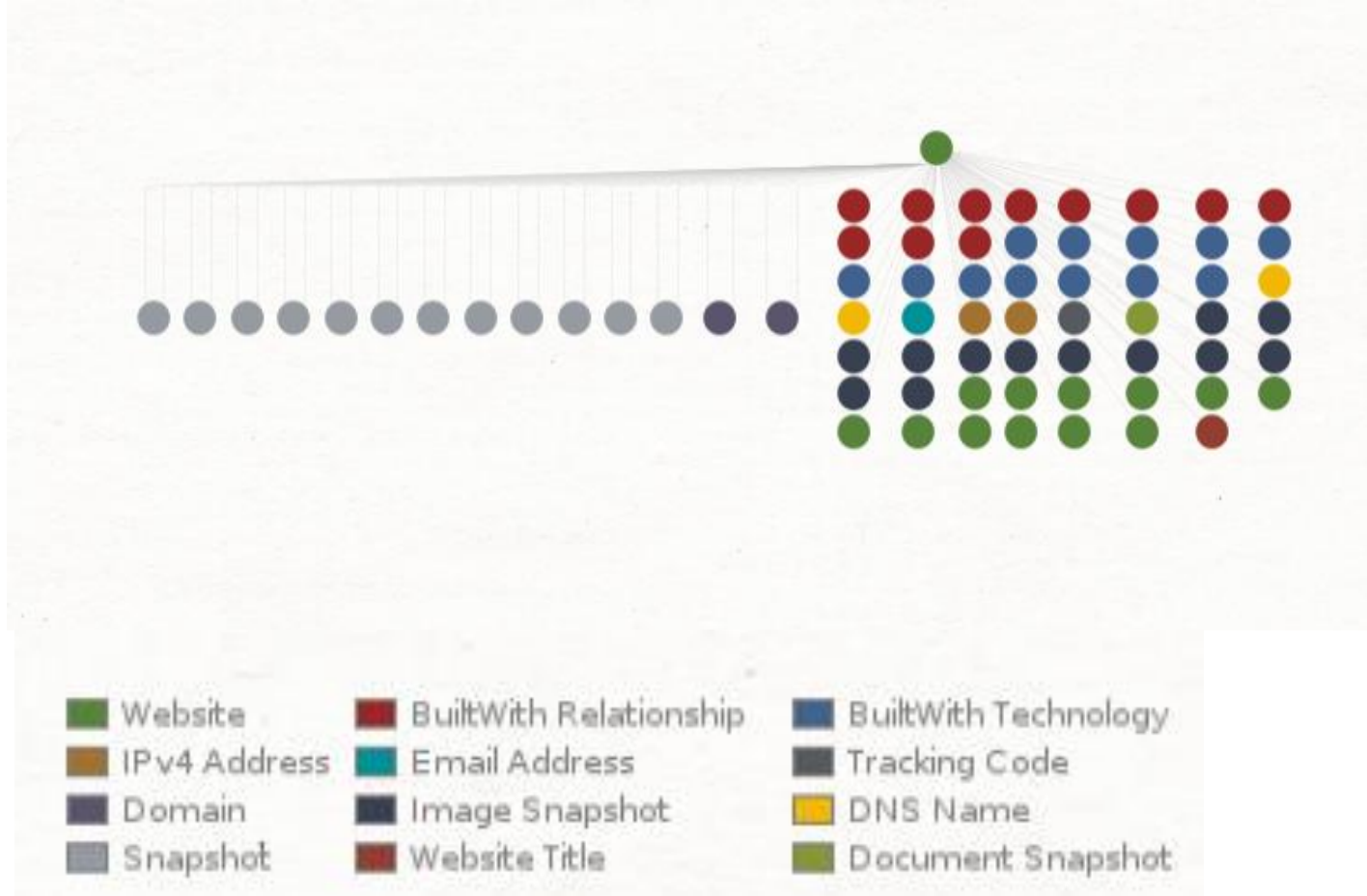
## CSS Usage

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).

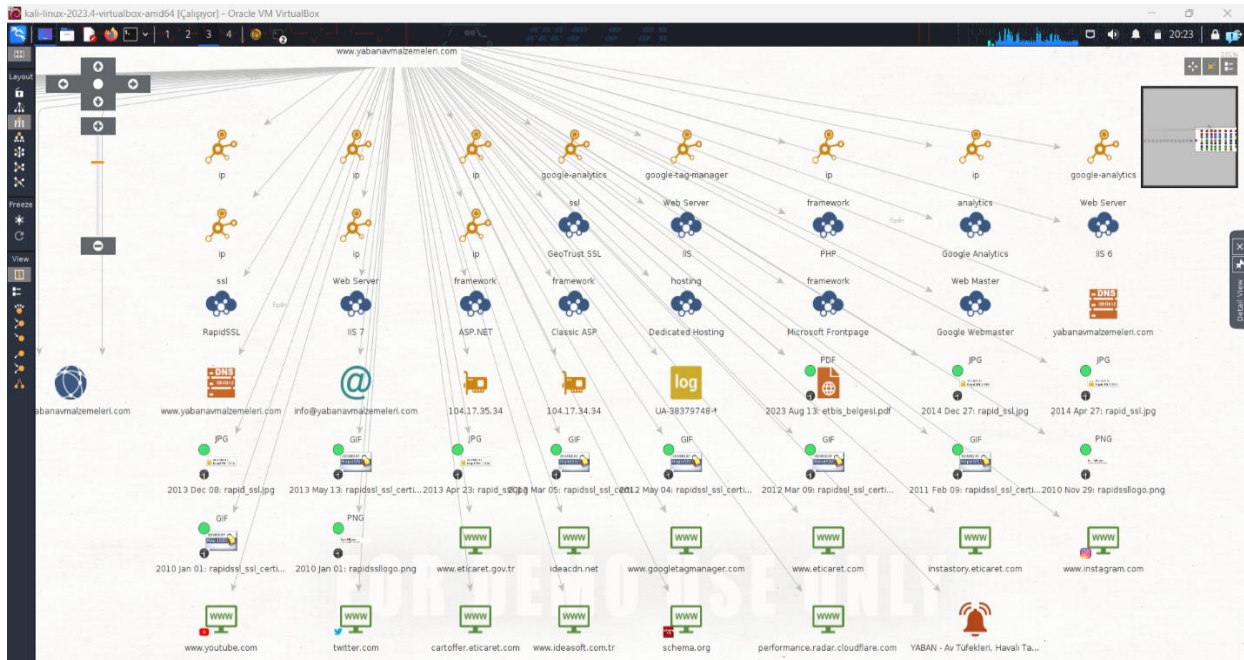
Technology	Description	Popular sites using this technology
Embedded <a href="#">🔗</a>	Styles defined within a webpage	<a href="http://www.amazon.es">www.amazon.es</a> , <a href="http://www.aliexpress.com">www.aliexpress.com</a> , <a href="http://www.portail-emploi.fr">www.portail-emploi.fr</a>
External <a href="#">🔗</a>	Styles defined within an external CSS file	<a href="http://www.instagram.com">www.instagram.com</a> , <a href="http://www.twitch.tv">www.twitch.tv</a> , <a href="http://www.netflix.com">www.netflix.com</a>

## 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
[kali@kali] (~)
$ sudo su
[sudo] password for kali:
[kali@kali] (/home/kali)
$ nmap -sV -O -A www.yabanavmalzemeleri.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 16:27 EST
Nmap scan report for www.yabanavmalzemeleri.com (104.17.35.34)
Host is up (0.0018s latency).
Other addresses for www.yabanavmalzemeleri.com (not scanned): 104.17.34.34
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  tcpwrapped
|_ http-server-header: cloudflare
|_ http-title: Did not follow redirect to https://www.yabanavmalzemeleri.com/
443/tcp    open  tcpwrapped
|_ http-server-header: cloudflare
|_ ssl-cert: Subject: commonName=yabanavmalzemeleri.com/organizationName=Cloud
|_ Subject Alternative Name: DNS:*.yabanavmalzemeleri.com, DNS:yabanavmalzem
|_ Not valid before: 2023-10-18T00:00:00
|_ Not valid after: 2024-10-17T23:59:59
|_ TLS-Alpn:
|_   H2
|_   http/1.1
|_ TLS-nextprotoneg:
|_   h2
|_ http/1.1
|_ ssl-date: TLS randomness does not represent time
8080/tcp    open  tcpwrapped
|_ http-server-header: cloudflare
Warning: OSscan results may be unreliable because we could not find at least
1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incom
lete
No OS matches for host
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.23 ms 104.17.35.34

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 25.20 seconds

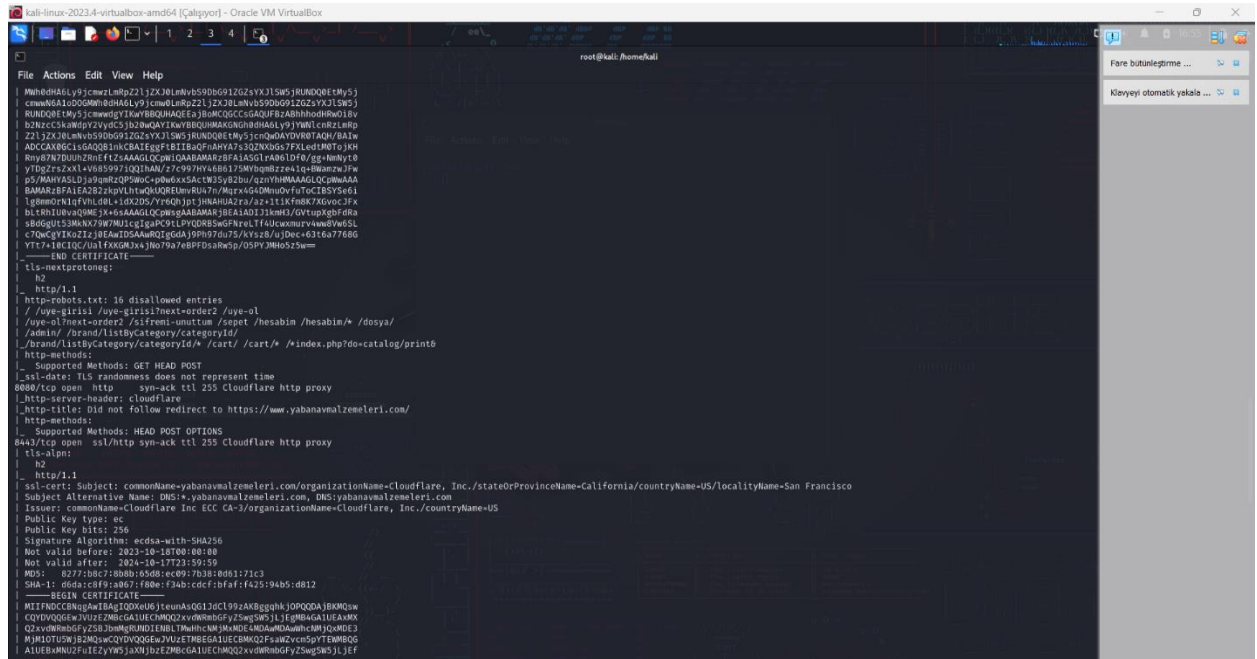
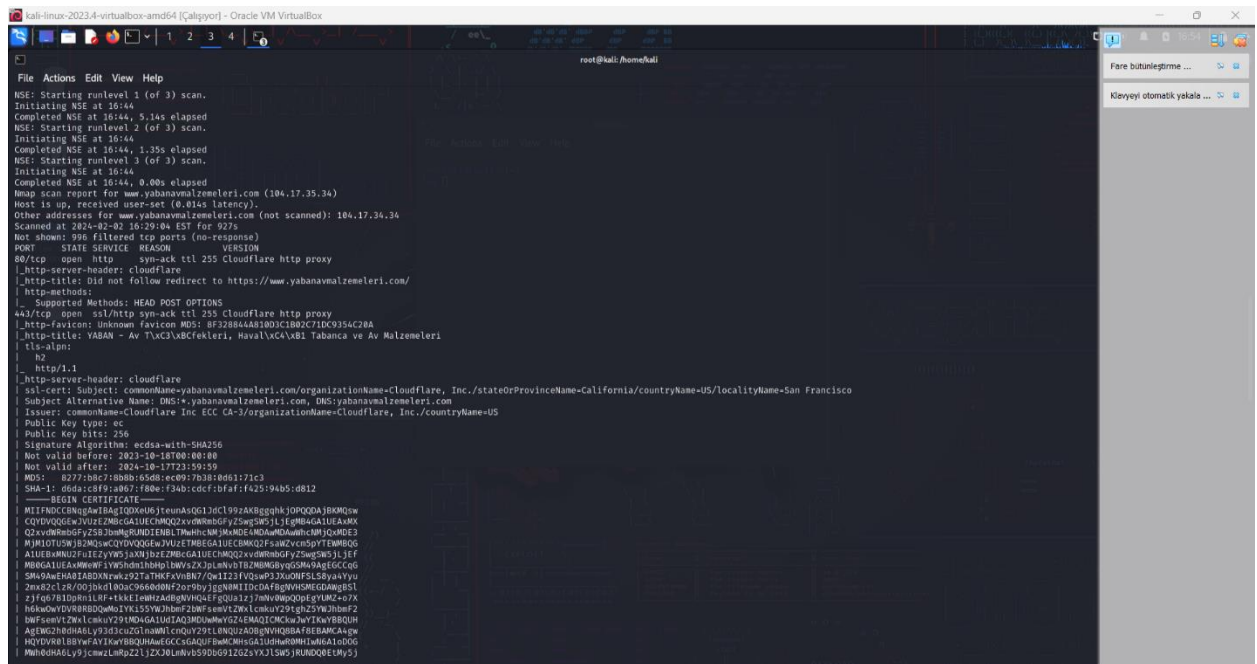
[kali@kali] (/home/kali)
$ nmap -sV -A -oA www.yabanavmalzemeleri.com --min-parallelism=50 --max-para
llelism=150 -PN -T2 -oA www.yabanavmalzemeleri.com
Host discovery disabled (-PN). All addresses will be marked 'up' and scan tim
es may be slower.
Warning: The -PN option is deprecated. Please use -Pn
```

```
kali-linux-2023.4-virtualbox-amd64 [Çalışıyor] - Oracle VM VirtualBox
root@kali: /home/kali

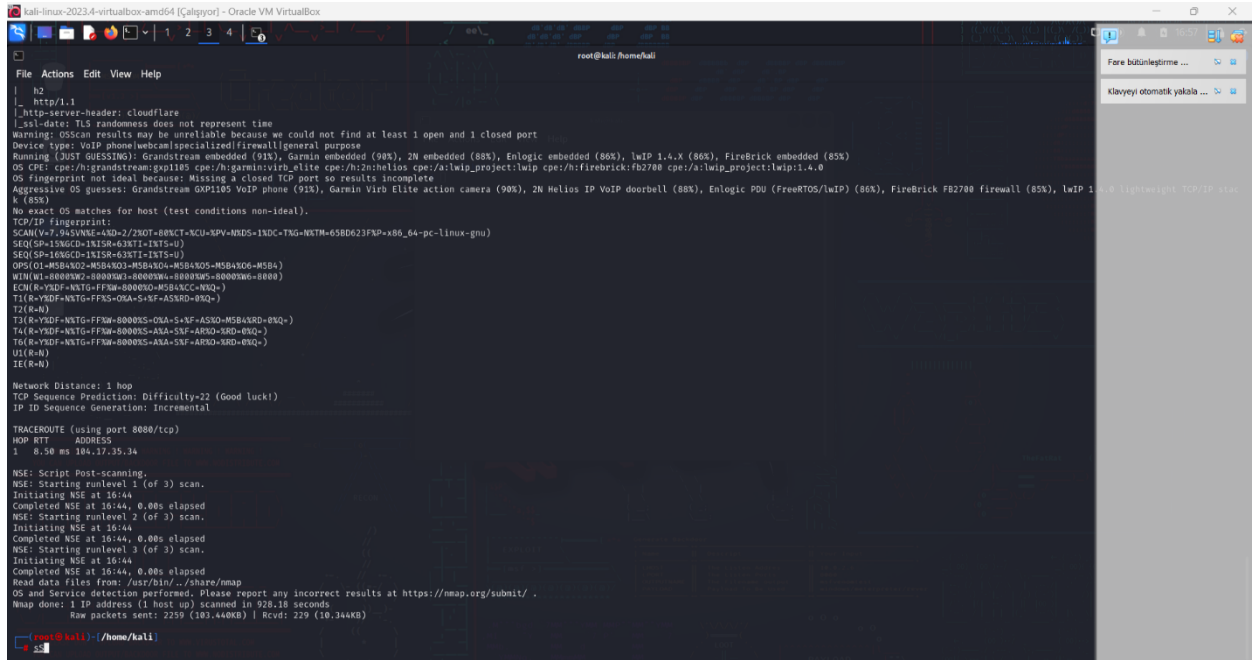
Warning: The -PN option is deprecated. Please use -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-02 16:29 EST
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 16:29
Completed NSE at 16:29, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 16:29
Completed NSE at 16:29, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 16:29
Completed NSE at 16:29, 0.00s elapsed
Warning: Hostname www.yabanavmalzemeleri.com resolves to 2 IPs. Using 104.17.
35.34.
Initiating SYN Stealth Scan at 16:29
Scanning www.yabanavmalzemeleri.com (104.17.35.34) [1000 ports]
Discovered open port 8080/tcp on 104.17.35.34
Discovered open port 80/tcp on 104.17.35.34
Discovered open port 443/tcp on 104.17.35.34
SYN Stealth Scan Timing: About 3.60% done; ETC: 16:43 (0:13:50 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 6.05% done; ETC: 16:43 (0:13:43 remaining)
SYN Stealth Scan Timing: About 11.50% done; ETC: 16:43 (0:12:57 remaining)
SYN Stealth Scan Timing: About 16.90% done; ETC: 16:43 (0:12:10 remaining)
Discovered open port 8443/tcp on 104.17.35.34
SYN Stealth Scan Timing: About 22.10% done; ETC: 16:43 (0:11:24 remaining)
SYN Stealth Scan Timing: About 27.20% done; ETC: 16:43 (0:10:40 remaining)
SYN Stealth Scan Timing: About 32.65% done; ETC: 16:43 (0:09:52 remaining)
SYN Stealth Scan Timing: About 37.75% done; ETC: 16:43 (0:09:07 remaining)
SYN Stealth Scan Timing: About 43.20% done; ETC: 16:43 (0:08:20 remaining)
SYN Stealth Scan Timing: About 48.25% done; ETC: 16:43 (0:07:36 remaining)
SYN Stealth Scan Timing: About 53.35% done; ETC: 16:43 (0:06:51 remaining)
SYN Stealth Scan Timing: About 58.45% done; ETC: 16:43 (0:06:06 remaining)
SYN Stealth Scan Timing: About 63.55% done; ETC: 16:43 (0:05:21 remaining)
SYN Stealth Scan Timing: About 68.70% done; ETC: 16:43 (0:04:36 remaining)
SYN Stealth Scan Timing: About 73.75% done; ETC: 16:43 (0:03:51 remaining)
SYN Stealth Scan Timing: About 78.85% done; ETC: 16:43 (0:03:06 remaining)
SYN Stealth Scan Timing: About 83.95% done; ETC: 16:43 (0:02:21 remaining)
SYN Stealth Scan Timing: About 89.05% done; ETC: 16:43 (0:01:37 remaining)
SYN Stealth Scan Timing: About 94.20% done; ETC: 16:43 (0:00:51 remaining)
Completed SYN Stealth Scan at 16:43, 881.85s elapsed (1000 total ports)
Initiating Service scan at 16:43
Scanning 4 services on www.yabanavmalzemeleri.com (104.17.35.34)
Completed Service scan at 16:43, 12.16s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against www.yabanavmalzemeleri.com (104.17.35.34)
Retrying OS detection (try #2) against www.yabanavmalzemeleri.com (104.17.35.34)
Initiating Traceroute at 16:44
Completed Traceroute at 16:44, 0.88s elapsed
NSE: Script scanning 104.17.35.34.
NSE: Starting runlevel 1 (of 3) scan.
```



## BLG424 Ağ Güvenliği ve Şifrelemeye Giriş



## 18



- 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.