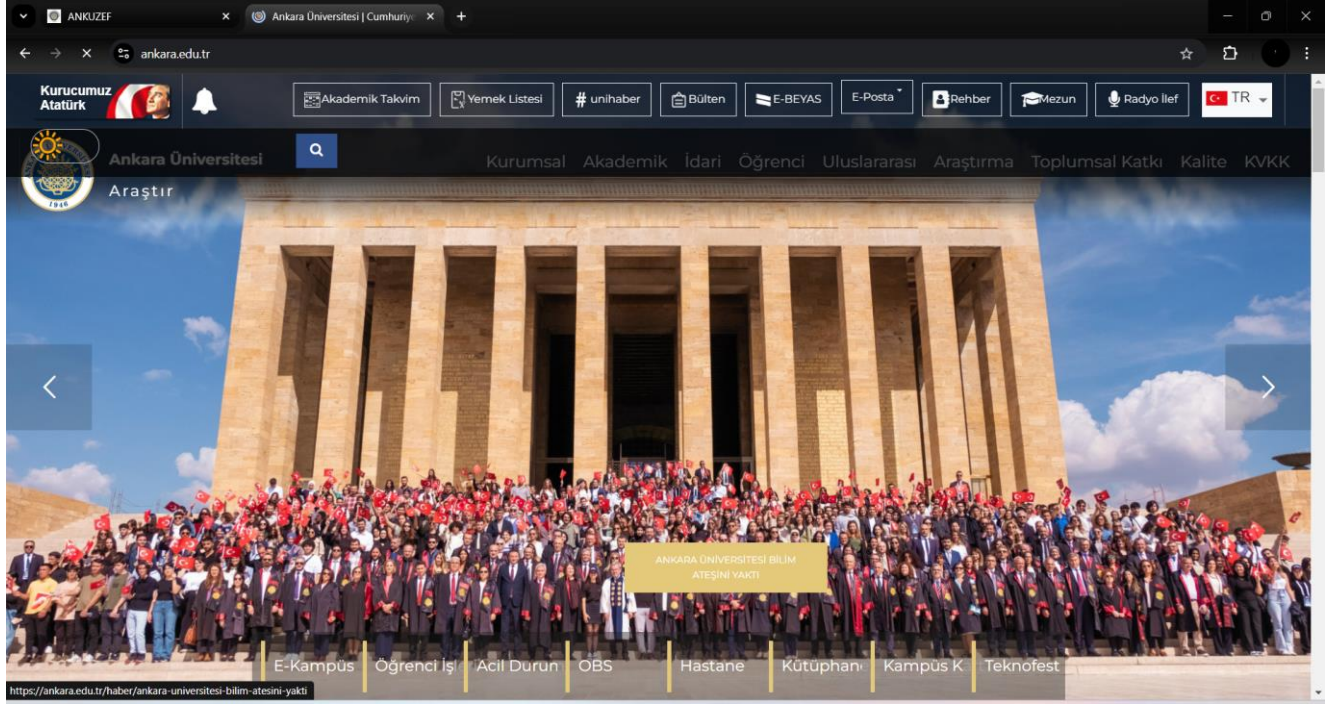


Rastgele seçtiğimiz üniversitelerin ip adresleri ve belli başlı özelliklerine nasıl ulaştığımızı göstereceğim.

İlk olarak nmap uygulamasını yükleyerek bilgisayarımızdan cmd komut satırından

Nmap ve web sayfa url sini yazarak ip adresini buluyoruz.

1- T.C. ANKARA ÜNİVERSİTESİ



Şekil 1: ANKARA ÜNİVERSİTESİ WEB SAYFASI

NMAP UYGULAMASI VE CMD ÜZERİNDEN ANKARA ÜNİVERSİTESİNİN BELLİ BAŞLI VERİLERİNE ULAŞACAĞIZ.

```
Komut İstemi
T.C. ANKARA ÜNİVERSİTESİ
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\selda>nmap www.ankara.edu.tr
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 16:16 T'rkiye Standart Saati
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 25.35% done; ETC: 16:16 (0:00:06 remaining)
Stats: 0:00:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 47.30% done; ETC: 16:16 (0:00:06 remaining)
Nmap scan report for www.ankara.edu.tr (80.251.45.231)
Host is up (0.054s latency).
rDNS record for 80.251.45.231: ankara.edu.tr
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
3690/tcp  closed svn
5222/tcp  closed xmpp-client
8080/tcp  closed http-proxy
9418/tcp  closed git

Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds
```

Şekil 2: ANKARA ÜNİVERSİTESİ 1

İlk olarak Ankara Üniversitesinin url adresini cmd üzerinde “nmap www.ankara.edu.tr” adresini girerek ip adresini kullanılan portları açık kapalı olduğu hangi servislerini kullandığını görebiliyoruz.

```
Komut İstemi
9418/tcp closed git

Nmap done: 1 IP address (1 host up) scanned in 8.90 seconds

C:\Users\selda>nmap -A -T4 80.251.45.231
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 16:17 T'rkiye Standart Saati
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.15% done; ETC: 16:17 (0:00:05 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:18 (0:00:17 remaining)
Stats: 0:01:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:19 (0:00:25 remaining)
Stats: 0:01:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 16:20 (0:00:45 remaining)
Stats: 0:03:42 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 91.67% done; ETC: 16:21 (0:00:02 remaining)
Stats: 0:03:50 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 16:21 (0:00:01 remaining)
Stats: 0:04:03 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 95.83% done; ETC: 16:21 (0:00:02 remaining)
Nmap scan report for ankara.edu.tr (80.251.45.231)
Host is up (0.032s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
80/tcp    open  http         Apache httpd 2.4.37 ((Red Hat Enterprise Linux) OpenSSL/1.1.1k)
|_http-server-header: Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k
443/tcp   open  ssl/http     Apache httpd 2.4.37 ((Red Hat Enterprise Linux) OpenSSL/1.1.1k)
|_ssl-cert: Subject: commonName=*.ankara.edu.tr/organizationName=Ankara \xC3\x9Cniversitesi
countryName=TR
```

Şekil 3: ANKARA ÜNİVERSİTESİ 2

Öğrendiğimiz ip adresini girerek daha da detaylı bilgilere ulaşıyoruz.

80/tcp portunun açık ve http servisiyle Apache web sunucusu kullanılarak yapıldığını görüyoruz.

```
Komut İstemi
Komut İstemi

| Not valid before: 2024-04-25T00:00:00
|_Not valid after: 2025-05-14T23:59:59
|_tls-alpn:
|_ http/1.1
|_http-server-header: Apache/2.4.37 (Red Hat Enterprise Linux) OpenSSL/1.1.1k
3690/tcp closed svn
5222/tcp closed xmpp-client
8080/tcp closed http-proxy
9418/tcp closed git
Device type: phone
Running (JUST GUESSING): Apple iOS 13.X|15.X|16.X (86%)
OS CPE: cpe:/o:apple:iphone_os:13.7 cpe:/o:apple:iphone_os:15 cpe:/o:apple:iphone_os:16
Aggressive OS guesses: Apple iOS 13.7 (Darwin 19.6.0) (86%), Apple iOS 15.0 - 16.1 (Darwin 21.1.0 - 22.1.0) (86%), Apple
iOS 16.0 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 7 hops

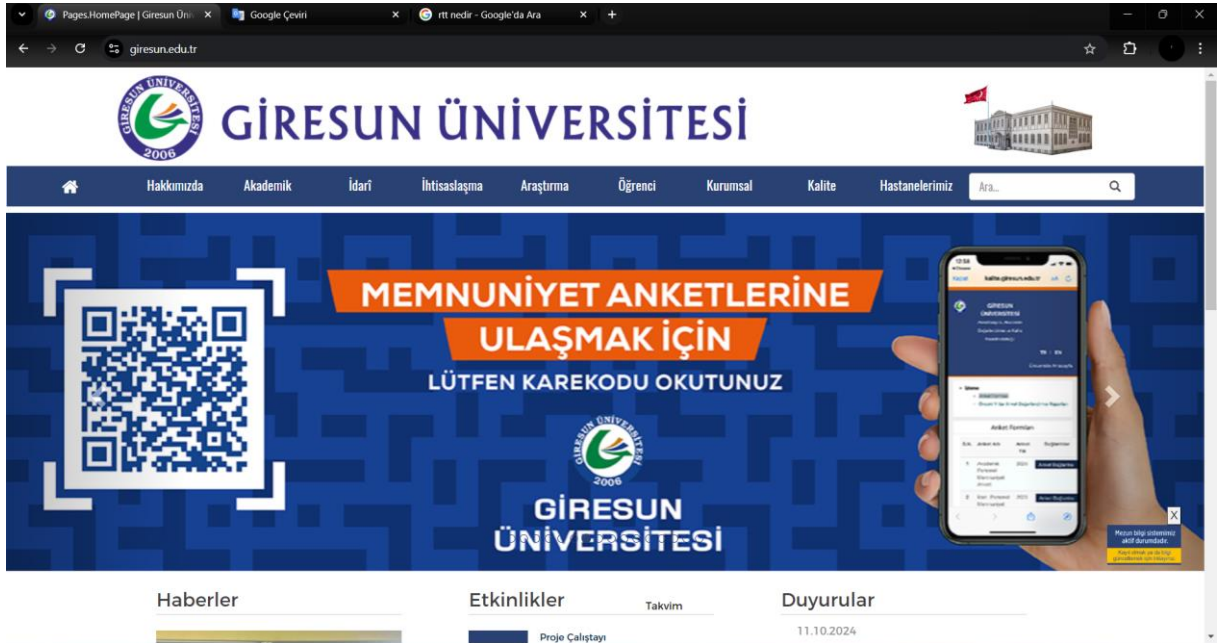
TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 7.00 ms 172.20.10.1
2 ...
3 56.00 ms 10.218.30.193
4 ... 5
5 52.00 ms 10.229.73.107
6 48.00 ms ankara.edu.tr (80.251.45.231)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 265.86 seconds
```

Şekil 4 : ANKARA ÜNİVERSİTESİ 3

Round trip time (RTT) yani gidiş-dönüş süresi, verilerin bir başlangıç noktasından (tarayıcı) ayrılıp aynı noktaya geri dönmesi için geçen süreyi milisaniye cinsinden ölçer. Hangi ip den kaç milisaniye de ulaştığını gözlemleyebiliriz.

2- T.C. GİRESUN ÜNİVERSİTESİ



Şekil 5: GİRESUN ÜNİVERSİTESİ WEB SİTESİ

```
Komut İstemi
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\selda> nmap www.giresun.edu.tr
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 17:26 T'rkiye Standart Saati
Failed to resolve "www.giresun.edu.tr".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 11.43 seconds

C:\Users\selda>
C:\Users\selda>nmap www.giresun.edu.tr
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-11 17:27 T'rkiye Standart Saati
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 74.60% done; ETC: 17:27 (0:00:05 remaining)
Nmap scan report for www.giresun.edu.tr (79.123.150.29)
Host is up (0.12s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 18.92 seconds
C:\Users\selda>
```

Şekil 6: GİRESUN ÜNİVERSİTESİ 1

İlk olarak Giresun Üniversitesinin url adresini cmd üzerinde “nmap www.giresun.edu.tr” adresini girerek ip adresini kullanılan portları açık kapalı olduğu hangi servislerini kullanıldığını görebiliyoruz. Ankara’dan farklı olarak 53/tcp portunun açık olduğunu görüyoruz. Bilgisayarımızdan browser'a bir internet sitesi çağırdığınızda önce 53 portundan o sitenin IP'sini buluyor, daha sonrada HTTP veya HTTPS üzerinden siteye ulaşıyor.

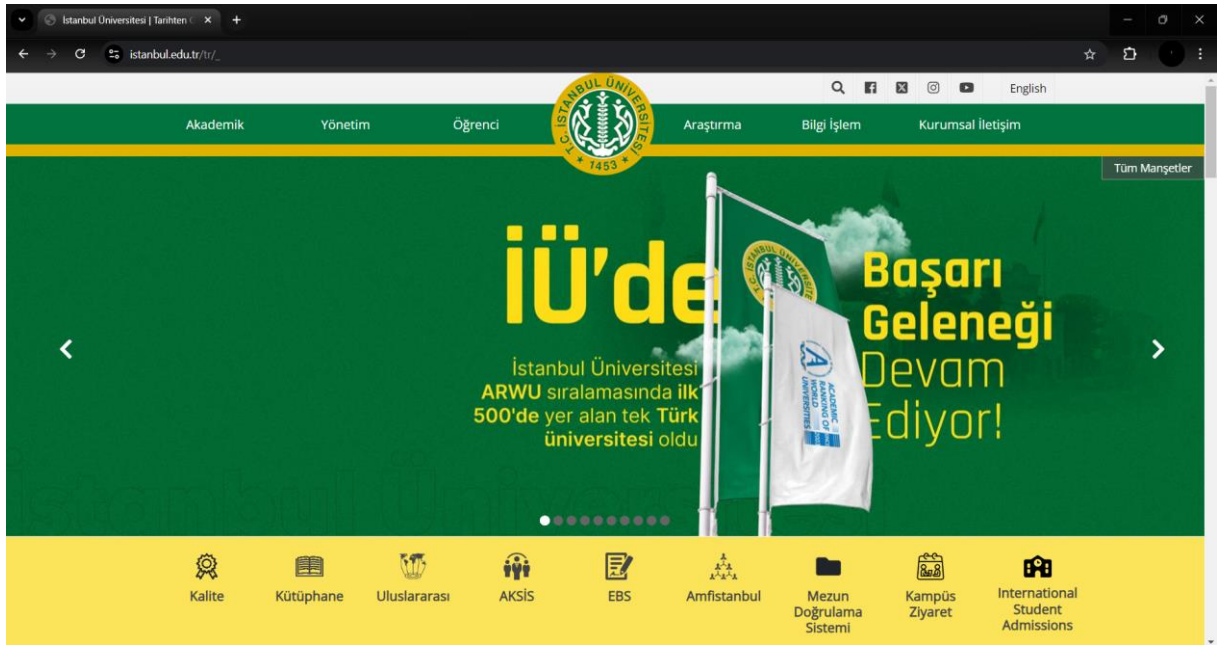
```
Komut İstemi
C:\Users\selda>nmap -A -T4 79.123.150.29
Starting nmap 7.95 ( https://nmap.org ) at 2024-10-11 17:30 T'rkiye Standart Saati
Stats: 0:00:10 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 21.03% done; ETC: 17:30 (0:00:26 remaining)
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 17:31 (0:00:12 remaining)
Nmap scan report for 79.123.150.29
Host is up (0.091s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
53/tcp    open  tcpwrapped
80/tcp    open  http      Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
443/tcp   open  ssl/https
|_http-title: Nesne ba\xC5\x9Fvurusu bir nesnenin &#246;rne\xC4\x9Fine ayarlanmad\xC4\xB1.
|_ssl-cert: Subject: commonName=*.giresun.edu.tr
|_ Subject Alternative Name: DNS:*.giresun.edu.tr, DNS:giresun.edu.tr
|_ Not valid before: 2024-01-08T00:00:00
|_ Not valid after: 2025-01-07T23:59:59
|_ ssl-date: TLS randomness does not represent time
|_http-server-header: Microsoft-IIS/10.0
Warning: SSLScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2016|2022|2012 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2022 cpe:/o:microsoft:windows_server_2012:r
2
Aggressive OS guesses: Microsoft Windows Server 2016 (91%), Microsoft Windows Server 2022 (89%), Microsoft Windows Serve
r 2012 R2 (85%)
No exact OS matches for host (test conditions non-ideal).
```

Şekil 7: GİRESUN ÜNİVERSİTESİ

53 portundan Tcpwrapped kullanıldığını görüyoruz. Tcpwrapped : Linux veya BSD gibi işletim sistemi üzerindeki Internet Protokolü sunucularına filtrelenmiş ağ erişimi için kullanılır.

Microsoft – IIS sunucusu kullanılmaktadır.

3- T.C. İSTANBUL ÜNİVERSİTESİ



Şekil 8 : İstanbul Üniversitesi web sayfası

```
Komut İstemi
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. Tüm hakları saklıdır.

C:\Users\selda>nmap istanbul.edu.tr
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 18:17 Türkiye Standart Saati
Nmap scan report for istanbul.edu.tr (194.27.128.98)
Host is up (0.092s latency).
rDNS record for 194.27.128.98: sehriyarsempozyum.istanbul.edu.tr.128.27.194.in-addr.arpa
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
8010/tcp  open  xmpp

Nmap done: 1 IP address (1 host up) scanned in 12.23 seconds
```

Şekil 9: istanbul üniversitesi

Burda diğer portlardan farklı olarak 8010 tcp portunu xmpp protokolünü görüyoruz.

XMPP (*Extensible Messaging and Presence Protocol*, Türkçe anlam karışıklığı : *Genişletilebilir Mesajlaşma ve Varlık Protokolü*), daha önceki adıyla Jabber, Internet'teki iki ucun herhangi bir yapısal bilgiyi birbirleri arasında karşılıklı ve neredeyse eş zamanlı aktarmalarına olanak sağlayan açık bir XML protokol ve teknolojileri bütünüdür.


```
Komut İstemi
C:\Users\selda> nmap -A -T4 194.27.128.98
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 18:32 T'rkiye Standart Saati
Nmap scan report for sehriyarsempozyum.istanbul.edu.tr.128.27.194.in-addr.arpa (194.27.128.98)
Host is up (0.040s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp?
80/tcp    open  http              Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Hata Sayfası\xC4\xB1 |Error Page
113/tcp   closed ident
443/tcp   open  ssl/http          Microsoft IIS httpd 10.0
|_ssl-cert: Subject: commonName=*.istanbul.edu.tr/organizationName=\xC4\xB0stanbul \xC3\x9Cniversitesi/stateOrProvinceName=\xC4\xB0stanbul/countryName=TR
|_Subject Alternative Name: DNS:*.istanbul.edu.tr, DNS:www.istanbul.edu.tr, DNS:istanbul.edu.tr
|_Not valid before: 2024-05-10T00:00:00
|_Not valid after: 2025-06-10T23:59:59
|_tls-alpn:
|_http/1.1
|_http-server-header: Microsoft-IIS/10.0
|_ssl-date: TLS randomness does not represent time
|_http-trane-info: Problem with XML parsing of /evox/about
|_http-title: \xC3\x9Dstanbul \xC3\x9Cniversitesi | Tarihten Gelece\xC3\xB0e Bilim K\xC3\xB6pr\xC3\xBCs\xC3\xBC ...
|_http-methods:
|_Potentially risky methods: TRACE
8010/tcp  open  ssl/http-proxy FortiGuard Web Filtering
|_ssl-date: 2024-10-13T15:34:34+00:00, 1m35s from scanner time.
|_ssl-cert: Subject: commonName=194.27.128.98
|_Subject Alternative Name: DNS:194.27.128.98
```

Şekil 10 : İstanbul Üniversitesi 2

Sunucu Microsoft – IIS kullanıldığını görüyoruz.

4- T.C. EGE ÜNİVERSİTESİ



Şekil 11: Ege Üniversitesi web sayfası

```
C:\Users\selda> nmap ege.edu.tr
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 18:50 T'rkiye Standart Saati
Nmap scan report for ege.edu.tr (155.223.2.2)
Host is up (0.038s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
8080/tcp   closed http-proxy

Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
```

Şekil 12: Ege Üniversitesi

Yine aynı şekilde 8080 portunun kapalı olduğu Proxy kullanıldığını görüyoruz.

```
Komut İstemi
C:\Users\selda> nmap -A -T4 155.223.2.2
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 18:56 T'rkiye Standart Saati
Stats: 0:04:14 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.75% done; ETC: 19:00 (0:00:02 remaining)
Nmap scan report for ege.edu.tr (155.223.2.2)
Host is up (0.038s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp?
53/tcp    open  domain
80/tcp    open  http         ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
           EgeWEB
|_ fingerprint-strings:
|_   FourOhFourRequest:
|_     HTTP/1.1 302 Found
|_     Date: Sun, 13 Oct 2024 15:55:41 GMT
|_     Server: EgeWEB
|_     Location: http://egweb.ege.edu.tr/errors/err404.php
|_     Content-Length: 226
|_     Connection: close
|_     Content-Type: text/html; charset=iso-8859-1
|_     <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
|_     <html><head>
|_     <title>302 Found</title>
|_     </head><body>
```

Şekil 13: Ege Üniversitesi

ISC BIND -> DNS sunucu yazılımını Linux 7 üzerinden kullanmakta.

Ayrıca EgeWEB isimli bir sunucuya da sahip olduğunu görüyoruz.

```
Date: Sun, 13 Oct 2024 15:55:42 GMT
Server: EgeWEB
Set-Cookie: PHPSESSID=mh61crkio74hk6jl8t6btgh21;
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-validate
Pragma: no-cache
X-Powered-By: ASP.NET 2.0
Access-Control-Allow-Origin: *.ege.edu.tr
```

Şekil 14 : Ege Üniversitesi 2

Açık kaynaklı web sayfası geliştirmek için kullanılan ASP.NET 2.0 kullandığını da görüyoruz.

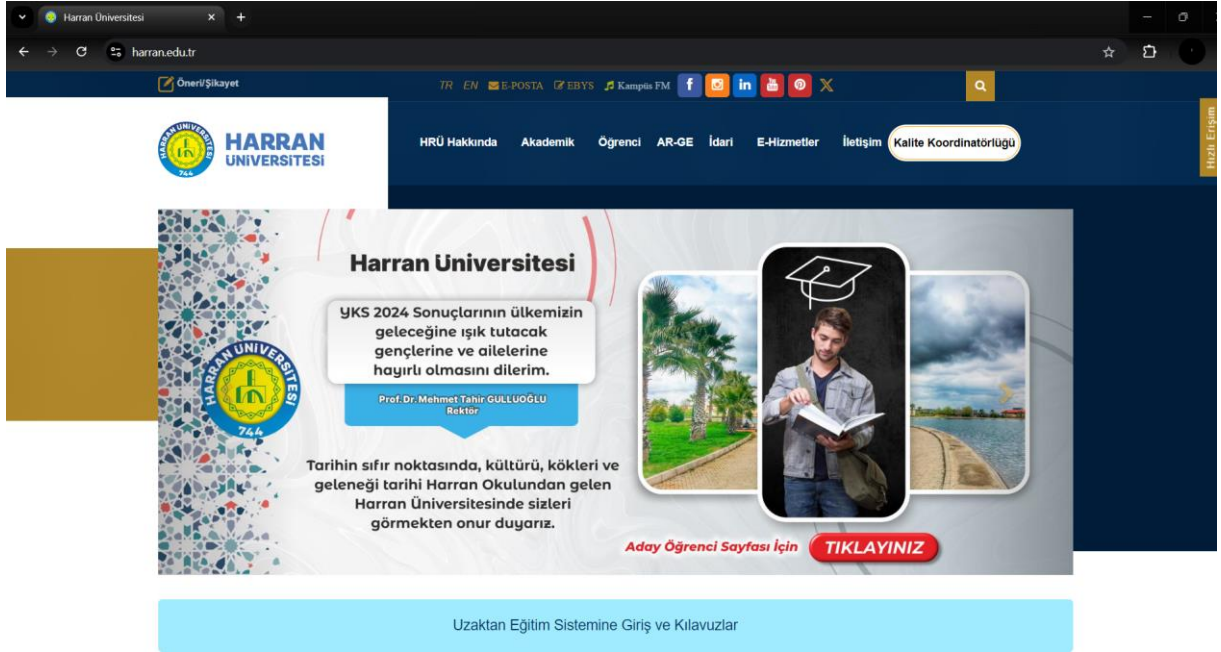
```
Komut İstemi

TRACEROUTE (using port 8080/tcp)
HOP RTT ADDRESS
1 2.00 ms 172.20.10.1
2 ...
3 49.00 ms 10.218.30.193
4 ... 5
6 51.00 ms 10.229.73.115
7 ... 11
12 52.00 ms 212.174.70.250 static.ttnet.com.tr (212.174.70.250)
13 59.00 ms 210.39.223.31 srv.turk.net (31.223.39.210)
14 54.00 ms 33.92.146.159 srv.turk.net (159.146.92.33)
15 59.00 ms 205.113.146.159 srv.turk.net (159.146.113.205)
16 61.00 ms 193.192.103.43
17 66.00 ms 70.96.154.212 static.turk.net (212.154.96.70)
18 77.00 ms 194.27.0.250
19 78.00 ms ulaknet-ege.ulak.net.tr (194.27.0.6)
20 74.00 ms egewan.ege.edu.tr (155.223.209.254)
21 69.00 ms 155.223.250.2
22 71.00 ms 155.223.250.250
23 60.00 ms ege.edu.tr (155.223.2.2)

OS and Service detection performed. Please report any incorrect results.
Nmap done: 1 IP address (1 host up) scanned in 290.80 seconds
```

Şekil 15 : Ege Üniversitesi 3

5- T.C. HARRAN ÜNİVERSİTESİ



Şekil 16: Harran Üniversitesi web sayfası


```

C:\Users\selda> nmap harran.edu.tr
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 19:20 T³rkiye Standart
Nmap scan report for harran.edu.tr (193.140.254.163)
Host is up (0.13s latency).
rDNS record for 193.140.254.163: www.harran.edu.tr
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 19.73 seconds

```

Şekil 17: Harran Üniversitesi 1

```

Komut İstemi
Nmap done: 1 IP address (1 host up) scanned in 19.73 seconds
C:\Users\selda>nmap -A -T4 193.140.254.163
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 19:34 T³rkiye Standart Saati
Nmap scan report for www.harran.edu.tr (193.140.254.163)
Host is up (0.035s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
80/tcp    open  http    Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
443/tcp   open  ssl/http Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
|_ssl-cert: Subject: commonName=*.harran.edu.tr
|_Subject Alternative Name: DNS:*.harran.edu.tr, DNS:harran.edu.tr
|_Not valid before: 2024-05-06T00:00:00
|_Not valid after: 2025-06-06T23:59:59
|_http-methods:
|_Potentially risky methods: TRACE
8080/tcp   open  http    Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0

```

Şekil 18 : Harran Üniversitesi 2

Microsoft-HTTPAPI/2.0

Her bir çağrı için ayrı bir istek açılması ve tek tek yanıtlanması yerine tek bir istekte tüm çağrılarının iletilmesi ve karşı sunucunun cevaplamasını sağlıyor, bu özellik de sitenizde herhangi bir optimizasyon yapmasanız dahi HTTP/2 protokolü sayesinde web sitenizin daha hızlı yüklenmesini sağlamaktadır.

```

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   2.00 ms   172.20.10.1
2   ...
3   68.00 ms  10.218.30.193
4   ... 5
6   69.00 ms  10.229.73.115
7   71.00 ms  www.harran.edu.tr (193.140.254.163)

OS and Service detection performed. Please report any in
Nmap done: 1 IP address (1 host up) scanned in 324.08 se

```

Şekil 19 : Harran Üniversitesi 3