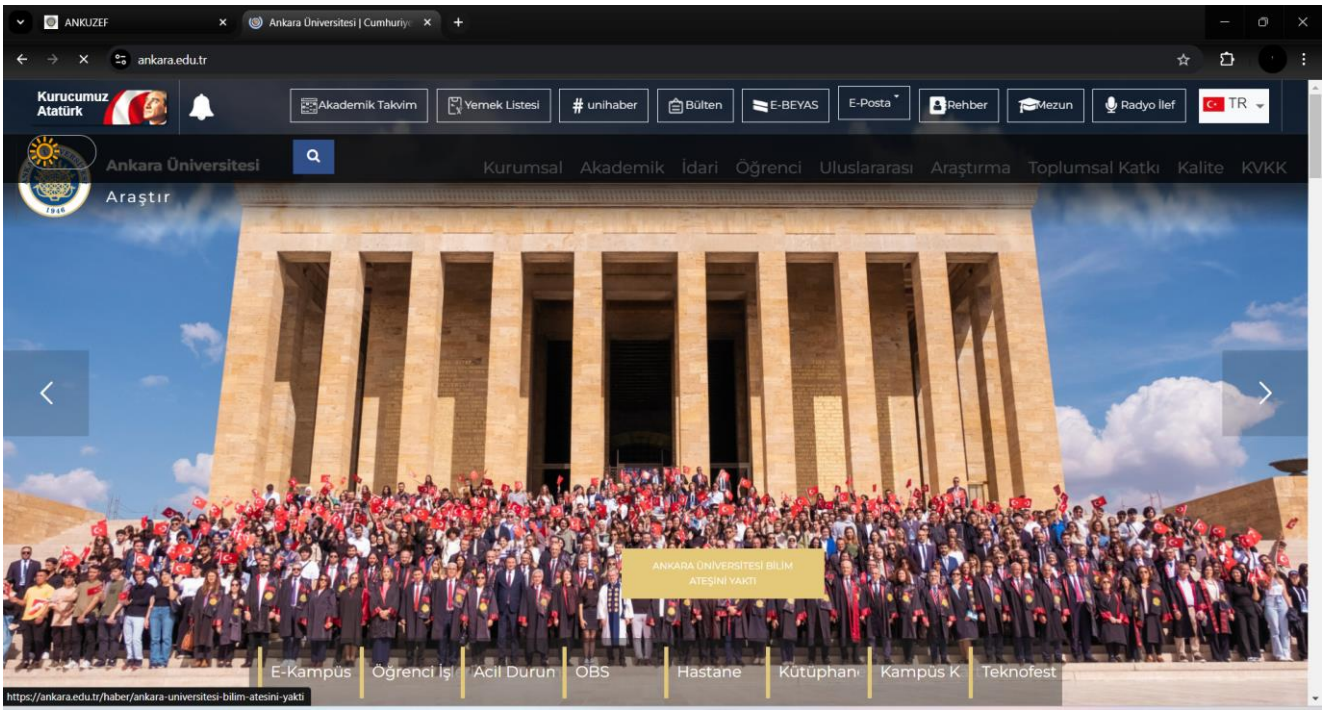
Rastgele seçtiğimiz üniversitelerin ip adresleri ve belli başlığı özelliklerine nasıl ulaştığımızı göstereceğim.

İlk olarak nmap uygulamasını yükleyerek bilgisayarımızdan cmd komut satırından

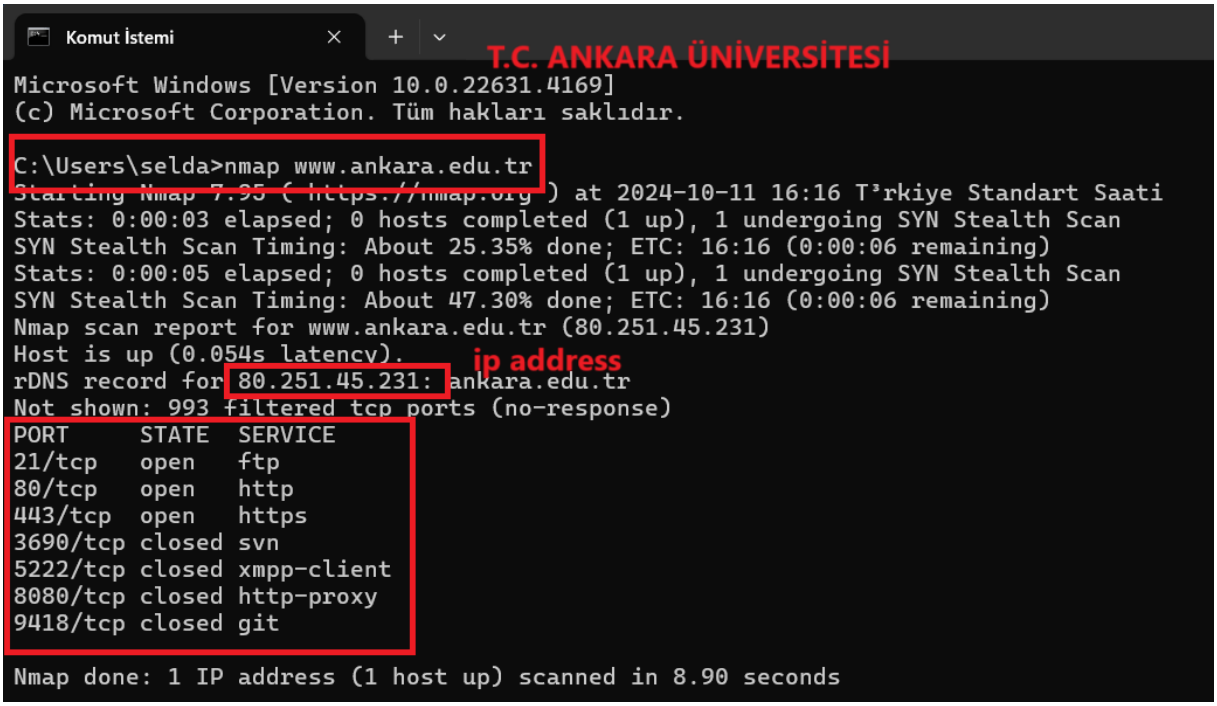
Nmap ve web sayfa url sini yazarak ip adresini buluyoruz.

1- T.C. ANKARA ÜNİVERSİTESİ



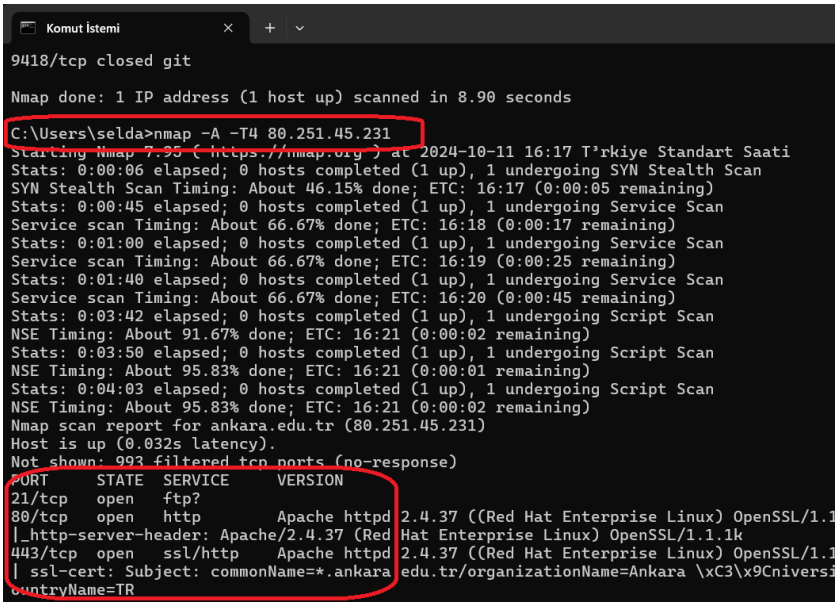
Şekil 1: ANKARA ÜNİVERSİTESİ WEB SAYFASI

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



Şekil 2: ANKARA ÜNİVERSİTESİ 1

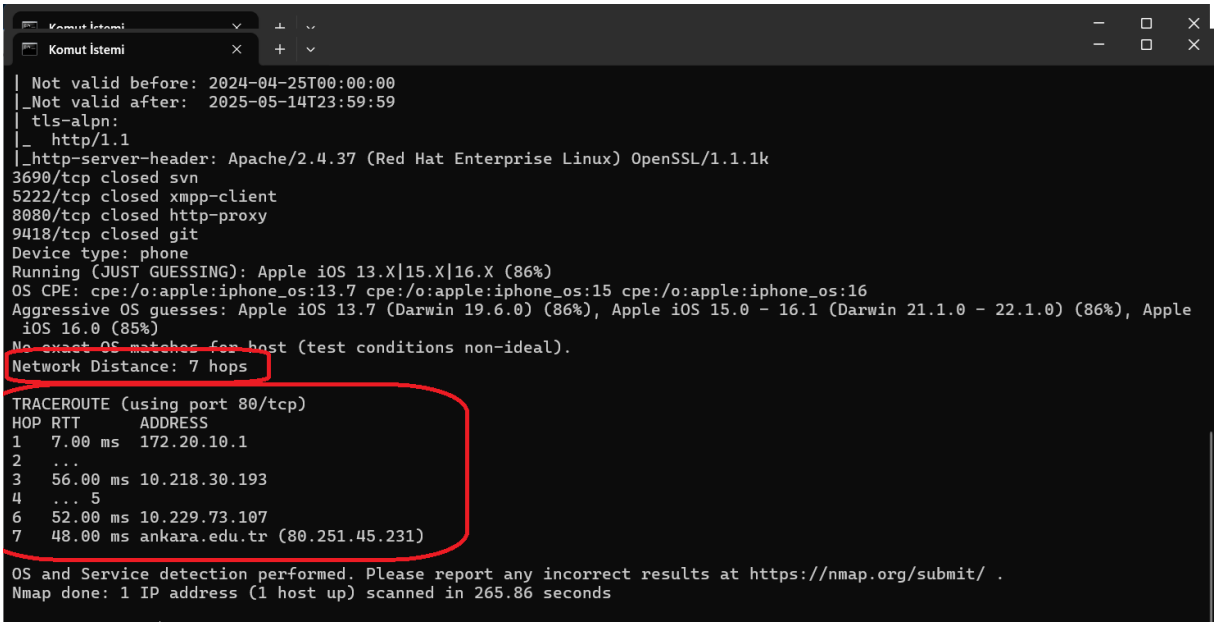
İlk olarak Ankara Üniversitesinin url adresini cmd üzerinde "nmap www.ankara.edu.tr" adresini girerek ip adresini kullanılan portları açık kapalı olduğu hangi servislerini kullanıdığını görebiliyoruz.



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.

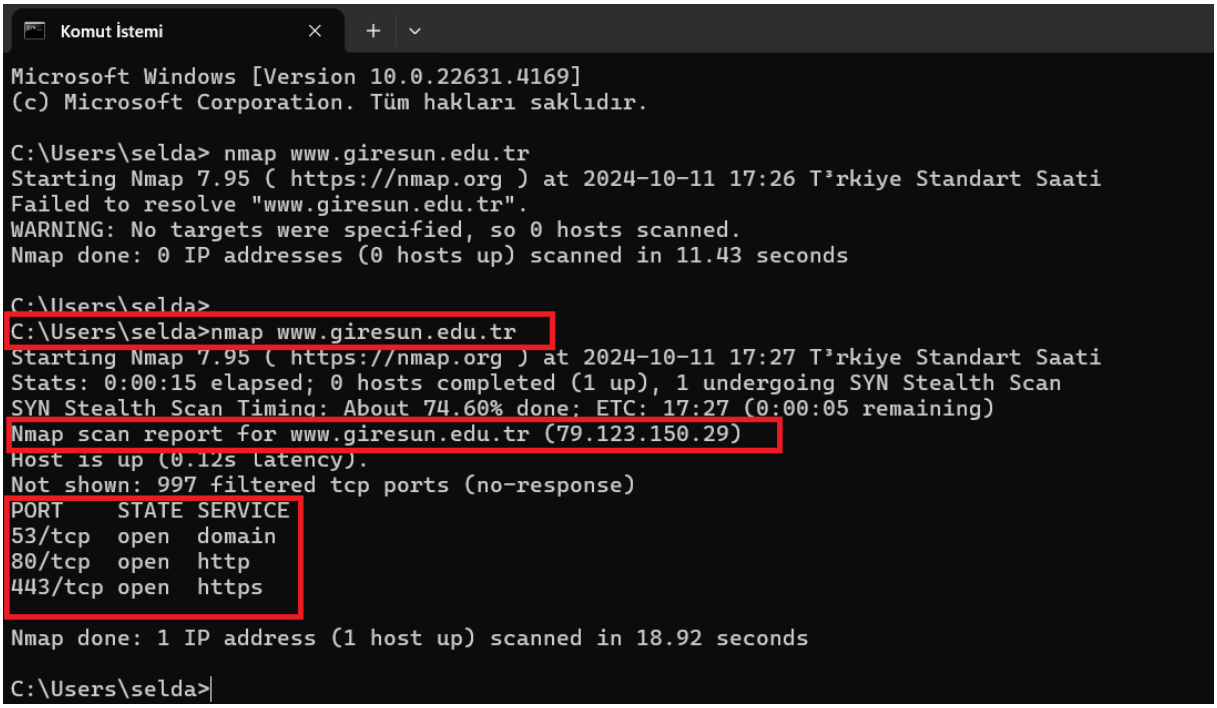


Şekil 4 : ANKARA ÜNİVERSİTESİ 3

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.

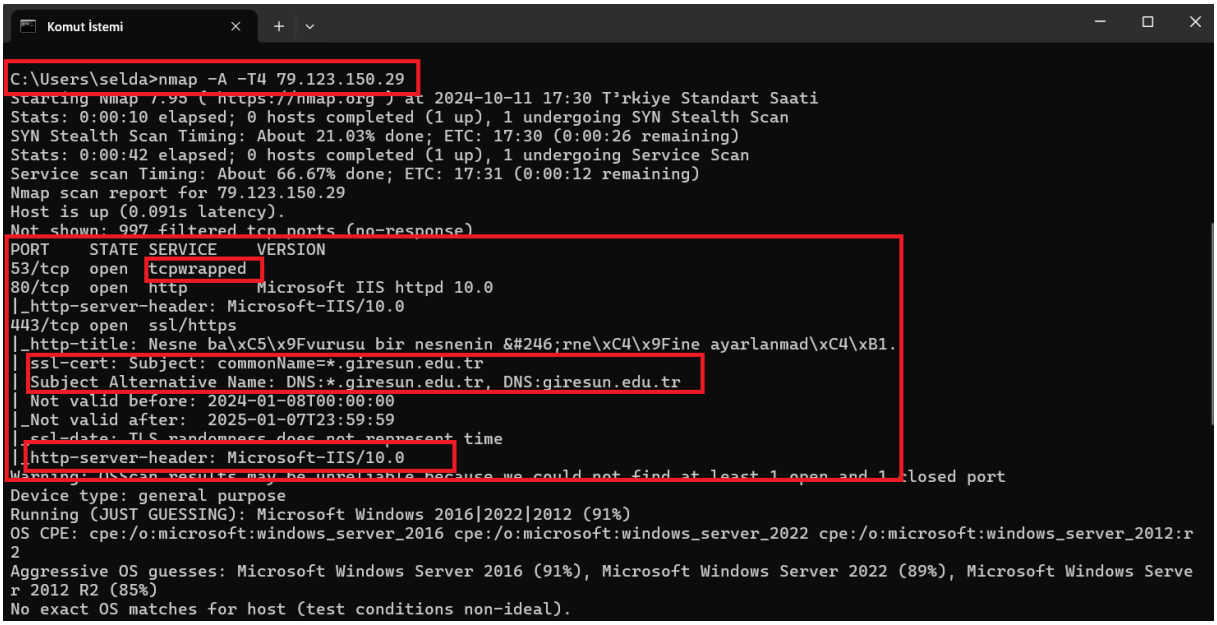
2- T.C. GİRESUN ÜNİVERSİTESİ

Şekil 5: GİRESUN ÜNİVERSİTESİ WEB SİTESİ



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 ulaşılıyor.

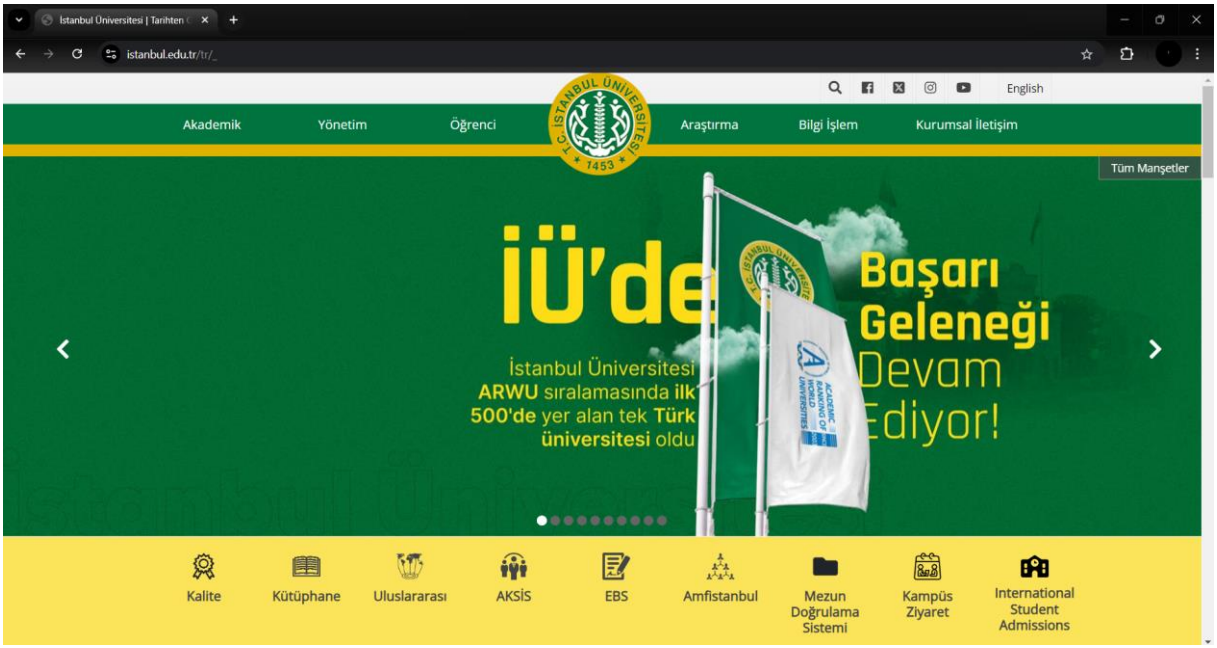


Şekil 7: GİRESUN ÜNİVERSİTESİ

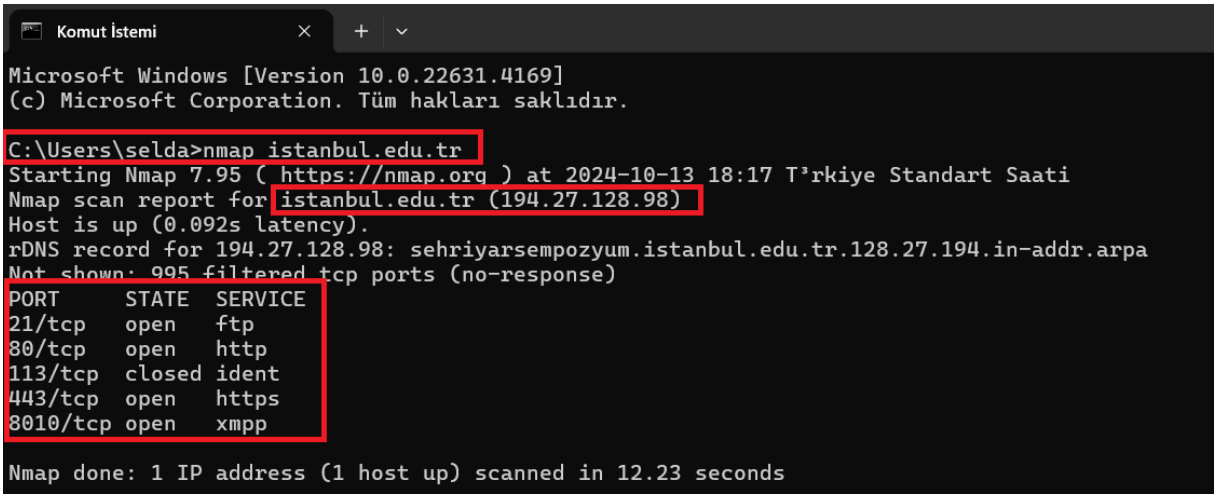
53 portundan Tcpwrapped kullanıldığını görüyoruz. Tcpwrapped : Linux veya BSD gibi işletim sistemi üzerindeki Internet Protokolü sunucularına filtrelenmiş ağ erişimi için kullanılır.

Microsoft – IIS sunucusu kullanılmaktadır.

3- T.C. İSTANBUL ÜNİVERSİTESİ



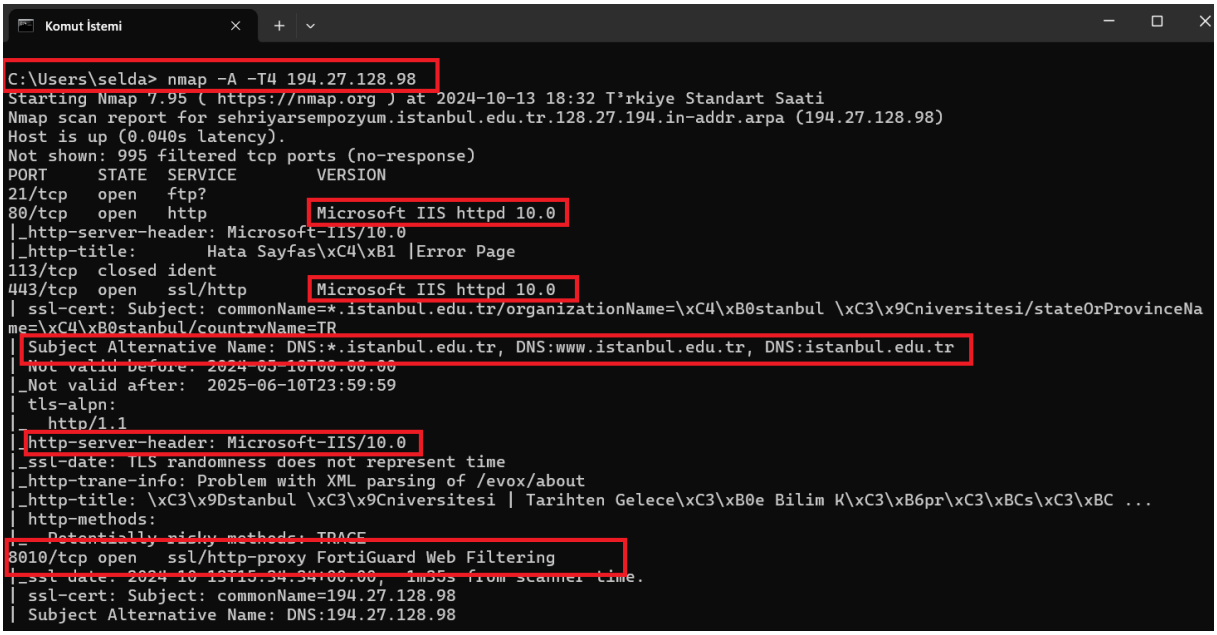
Şekil 8 : İstanbul Üniversitesi web sayfası



Şekil 9: istanbul üniversitesi

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

XMPP (*Extensible Messaging and Presence Protocol*, Türkçe anlam karışılığı : *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.



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 T³rkiye Standart Saati
Nmap scan report for ege.edu.tr (155.223.2.2)
Host is up (0.088s 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 T³rkiye 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     ISC BIND 9.9.4 (RedHat Enterprise Linux 7)
80/tcp   open   http       EgeWEB
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 302 Found
|     Date: Sun, 13 Oct 2024 15:55:41 GMT
|     Server: EgeWEB
|     Location: http://egeweb.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

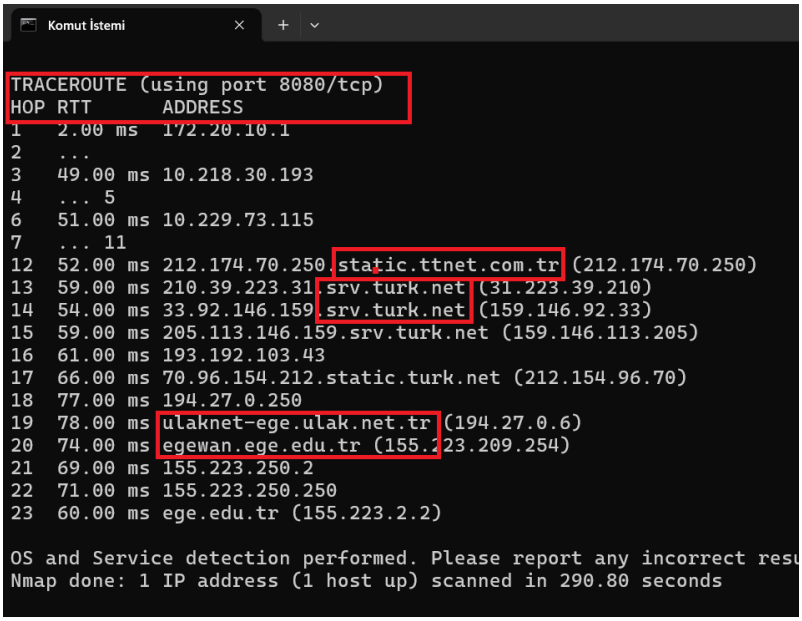
ISC BIND -> DNS sunucu yazılımını Linux 7 üzerinden kullanmakta.

Ayrıca EgeWEB isimli bir sunucuya da sahip olduğunu görüyoruz.

```
|     Server: EgeWEB
|     Set-Cookie: PHPSESSID=mh61crkio74hk6ljl8t6btgh21;
|     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
```

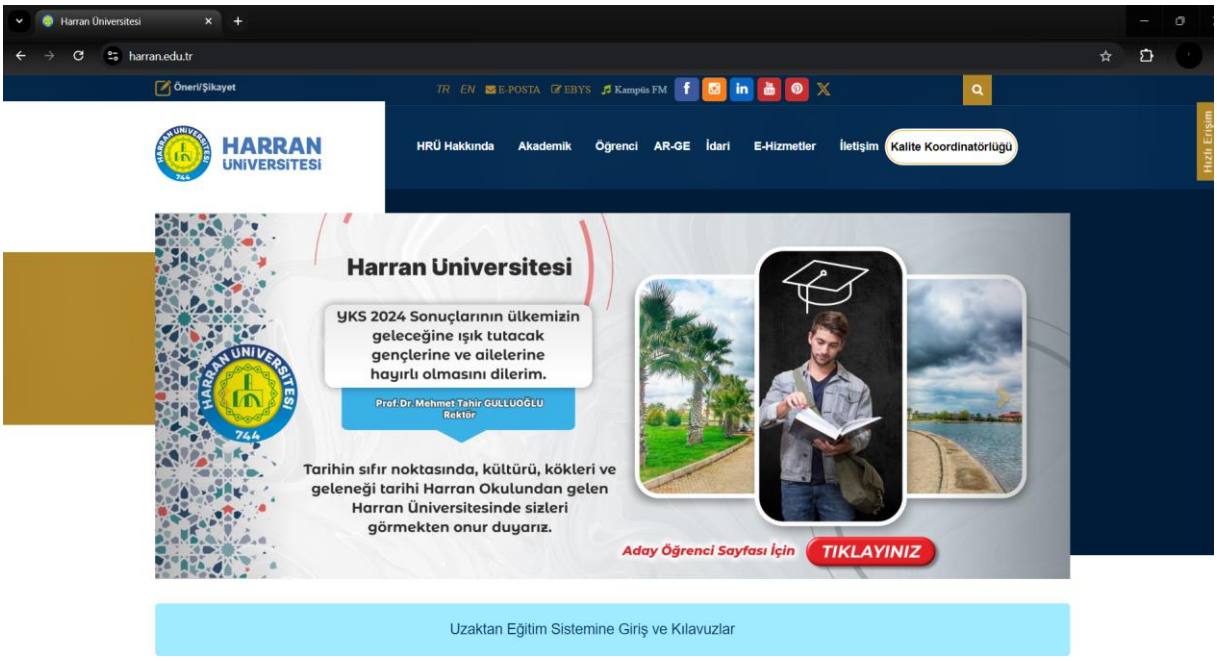
Şekil 14 : Ege Üniversitesi 2

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



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 çağrıların 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