Batuhan TORUK

Hafta 2

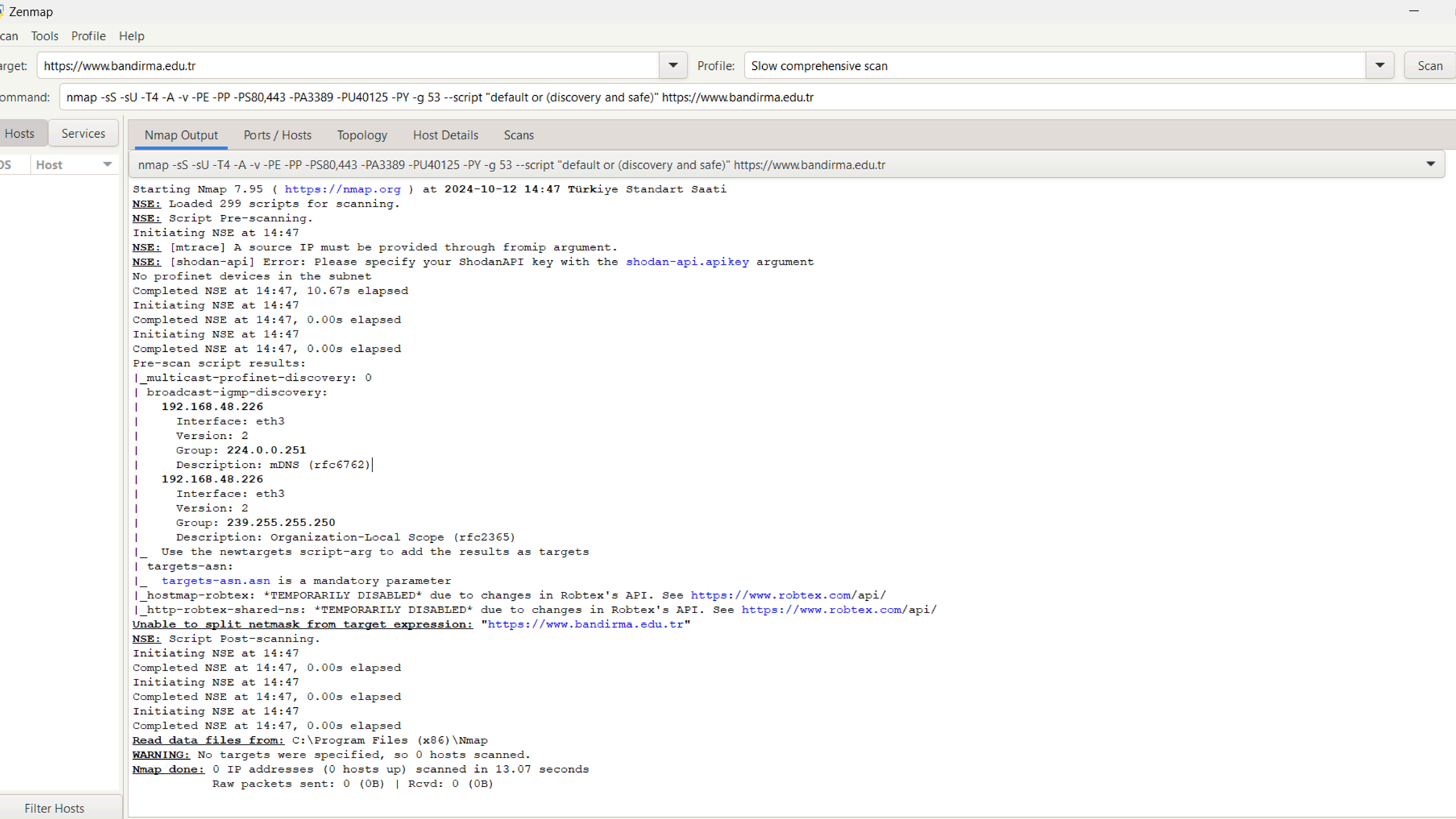
BANDIRMA ONYEDI EYLÜL

Kullanılan diller ve yazılımlar: html- javascript

Veri tabanı: asp.net

Web server: ııs 10.0 javascrpit

Frameworks:modernizr2.6.2 jQuery 1.10.2 jQueryuı



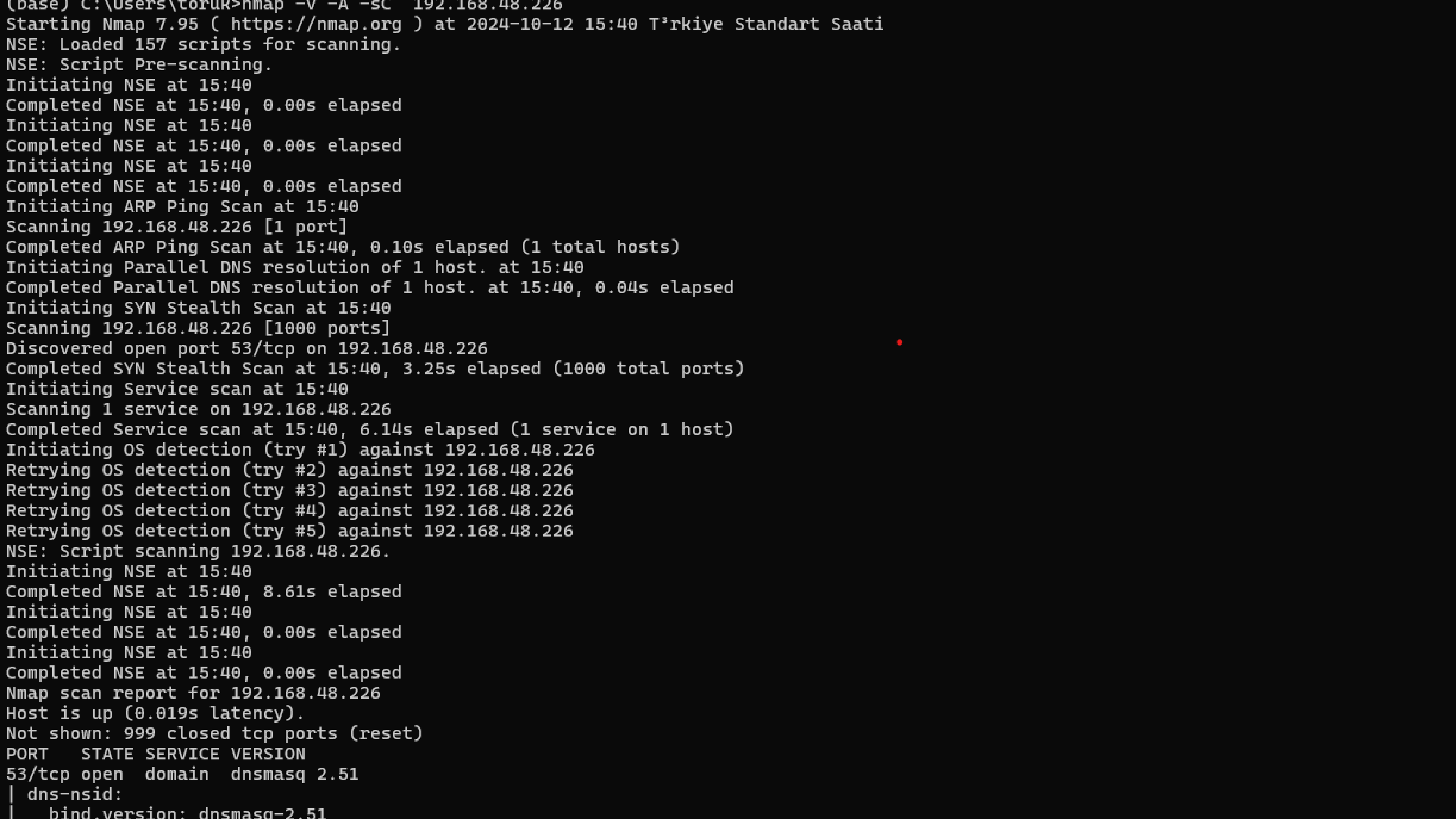
arget: https://www.bandirma.edu.tr

Profile: Slow comprehensive scan

ommand: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.bandirma.edu.tr

nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.bandirma.edu.tr

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 14:47 Türkiye Standart Saati
NSE: Loaded 299 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:47
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
No profinet devices in the subnet
Completed NSE at 14:47, 10.67s elapsed
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Pre-scan script results:
|_multicast-profinet-discovery: 0
| broadcast-igmp-discovery:
|   192.168.48.226
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.48.226
|     Interface: eth3
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Unable to split netmask from target expression: "https://www.bandirma.edu.tr"
NSE: Script Post-scanning.
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Initiating NSE at 14:47
Completed NSE at 14:47, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 13.07 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```

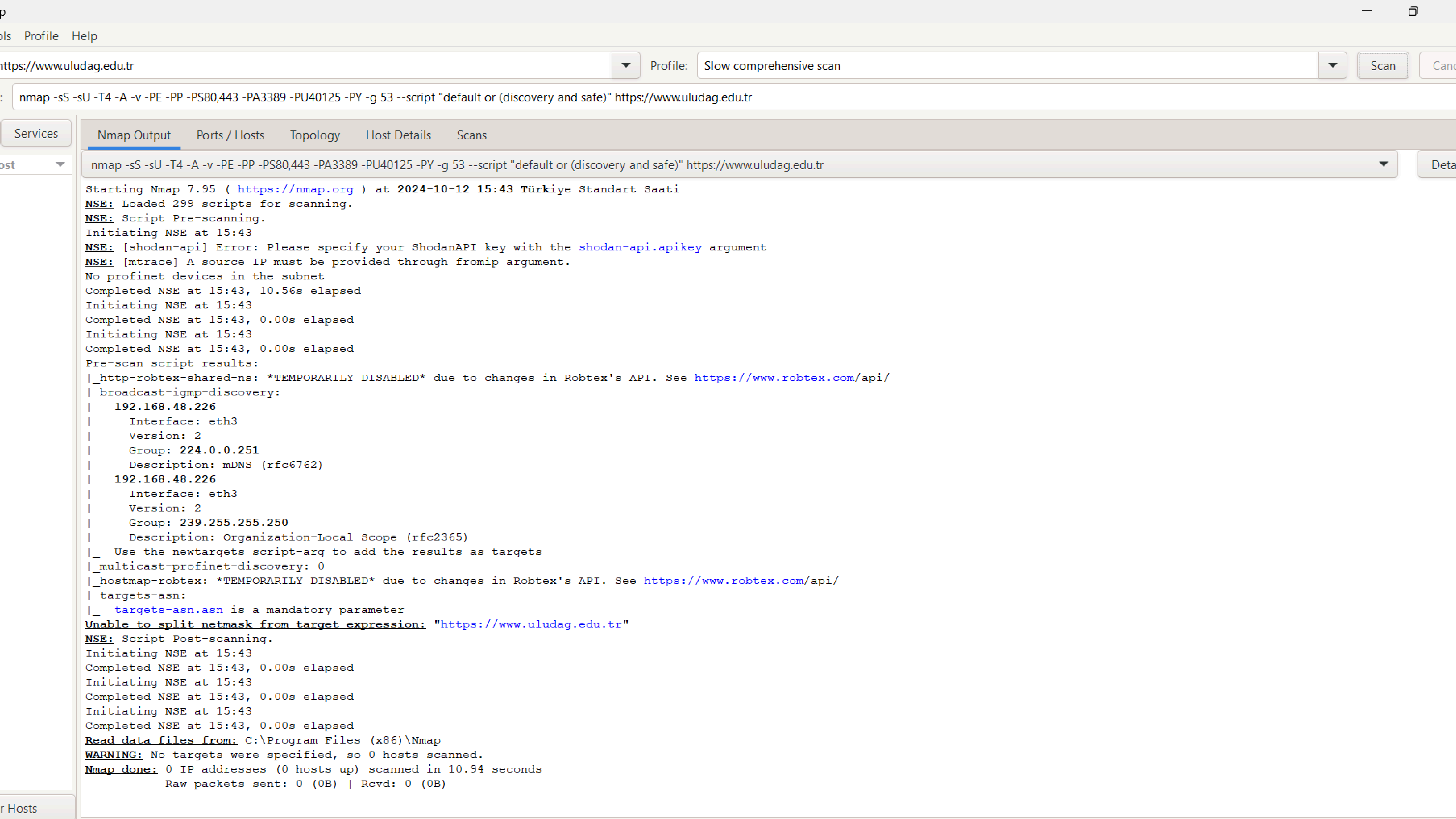


```
(base) C:\Users\toruk>nmap -V -A -sC  192.168.48.226
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 15:40 T³rkiye Standart Saati
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Initiating ARP Ping Scan at 15:40
Scanning 192.168.48.226 [1 port]
Completed ARP Ping Scan at 15:40, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:40
Completed Parallel DNS resolution of 1 host. at 15:40, 0.04s elapsed
Initiating SYN Stealth Scan at 15:40
Scanning 192.168.48.226 [1000 ports]
Discovered open port 53/tcp on 192.168.48.226
Completed SYN Stealth Scan at 15:40, 3.25s elapsed (1000 total ports)
Initiating Service scan at 15:40
Scanning 1 service on 192.168.48.226
Completed Service scan at 15:40, 6.14s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.48.226
Retrying OS detection (try #2) against 192.168.48.226
Retrying OS detection (try #3) against 192.168.48.226
Retrying OS detection (try #4) against 192.168.48.226
Retrying OS detection (try #5) against 192.168.48.226
NSE: Script scanning 192.168.48.226.
Initiating NSE at 15:40
Completed NSE at 15:40, 8.61s elapsed
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Initiating NSE at 15:40
Completed NSE at 15:40, 0.00s elapsed
Nmap scan report for 192.168.48.226
Host is up (0.019s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|   bind.version: dnsmasq-2.51
```

BURSA ULUDAĞ ÜNIVERSITESI

Kullanılan diller ve yazılımlar: html php javascript php 7.1.13

Dev tools: HTML5 Shiv

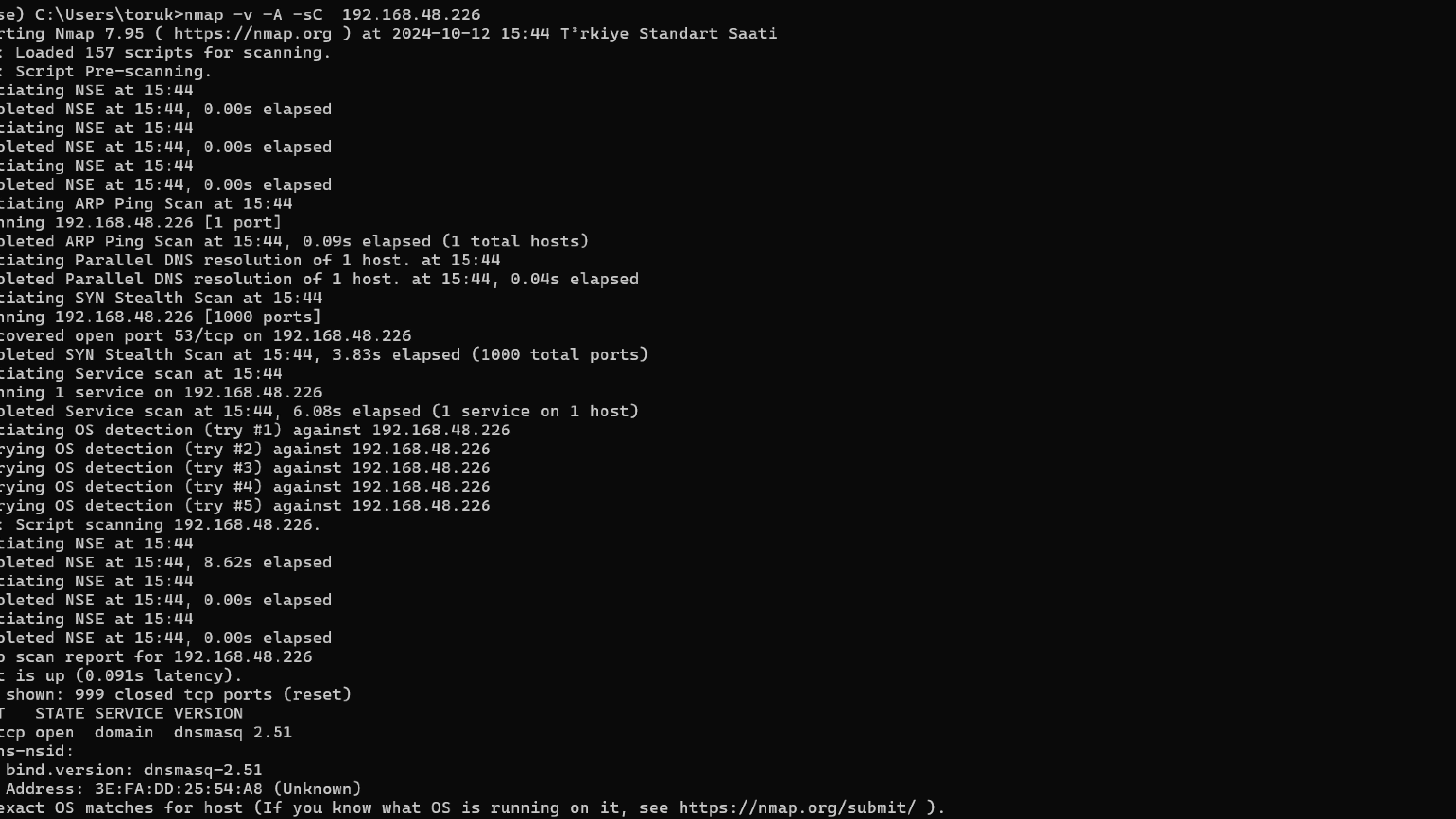


Target: ttps://www.uludag.edu.tr

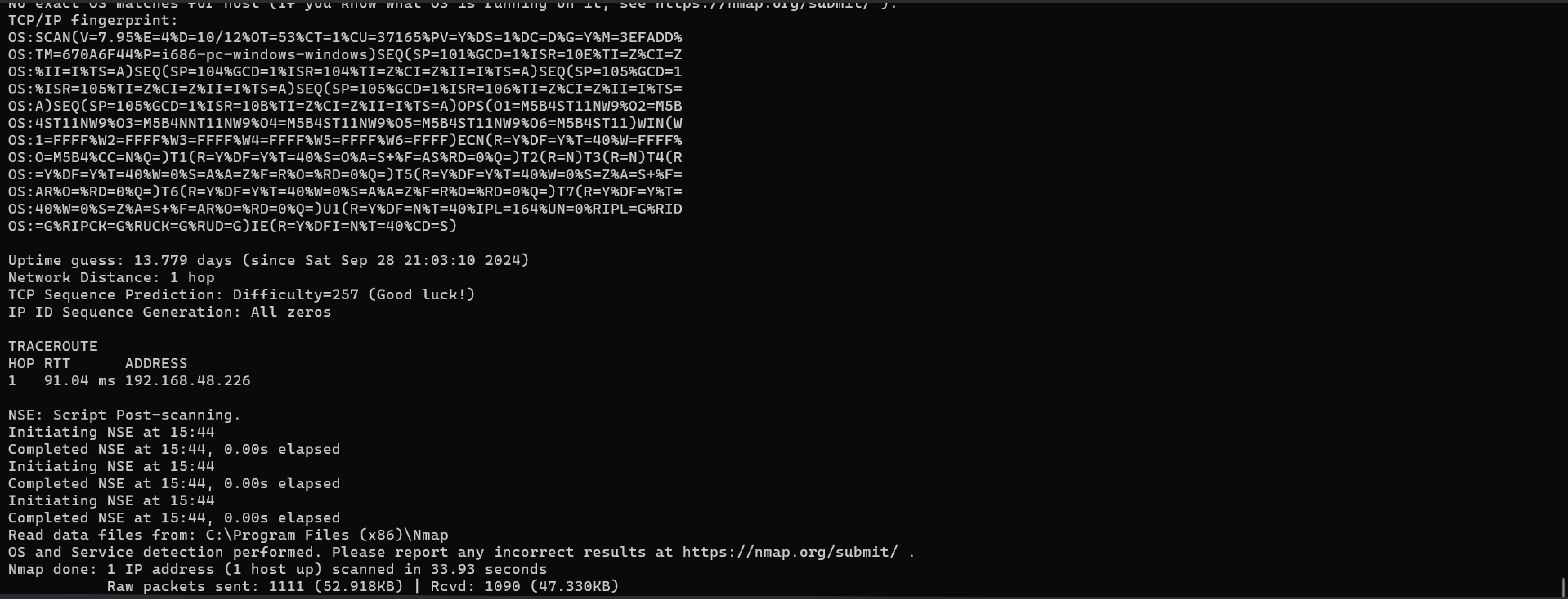
Profile: Slow comprehensive scan

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.uludag.edu.tr

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 15:43 Türkiye Standart Saati
NSE: Loaded 299 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:43
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [mtrace] A source IP must be provided through fromip argument.
No profinet devices in the subnet
Completed NSE at 15:43, 10.56s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Pre-scan script results:
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-igmp-discovery:
|   192.168.48.226
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.48.226
|     Interface: eth3
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
|_multicast-profinet-discovery: 0
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Unable to split netmask from target expression: "https://www.uludag.edu.tr"
NSE: Script Post-scanning.
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Initiating NSE at 15:43
Completed NSE at 15:43, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.94 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```



```
se) C:\Users\toruk>nmap -v -A -sC  192.168.48.226
rting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 15:44 T³rkiye Standart Saati
: Loaded 157 scripts for scanning.
: Script Pre-scanning.
tiating NSE at 15:44
pleted NSE at 15:44, 0.00s elapsed
tiating NSE at 15:44
pleted NSE at 15:44, 0.00s elapsed
tiating NSE at 15:44
pleted NSE at 15:44, 0.00s elapsed
tiating ARP Ping Scan at 15:44
nning 192.168.48.226 [1 port]
pleted ARP Ping Scan at 15:44, 0.09s elapsed (1 total hosts)
tiating Parallel DNS resolution of 1 host. at 15:44
pleted Parallel DNS resolution of 1 host. at 15:44, 0.04s elapsed
tiating SYN Stealth Scan at 15:44
nning 192.168.48.226 [1000 ports]
covered open port 53/tcp on 192.168.48.226
pleted SYN Stealth Scan at 15:44, 3.83s elapsed (1000 total ports)
tiating Service scan at 15:44
nning 1 service on 192.168.48.226
pleted Service scan at 15:44, 6.08s elapsed (1 service on 1 host)
tiating OS detection (try #1) against 192.168.48.226
rying OS detection (try #2) against 192.168.48.226
rying OS detection (try #3) against 192.168.48.226
rying OS detection (try #4) against 192.168.48.226
rying OS detection (try #5) against 192.168.48.226
: Script scanning 192.168.48.226.
tiating NSE at 15:44
pleted NSE at 15:44, 8.62s elapsed
tiating NSE at 15:44
pleted NSE at 15:44, 0.00s elapsed
tiating NSE at 15:44
pleted NSE at 15:44, 0.00s elapsed
p scan report for 192.168.48.226
t is up (0.091s latency).
 shown: 999 closed tcp ports (reset)
T   STATE SERVICE VERSION
tcp open  domain  dnsmasq 2.51
ns-nsid:
 bind.version: dnsmasq-2.51
 Address: 3E:FA:DD:25:54:A8 (Unknown)
exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
```



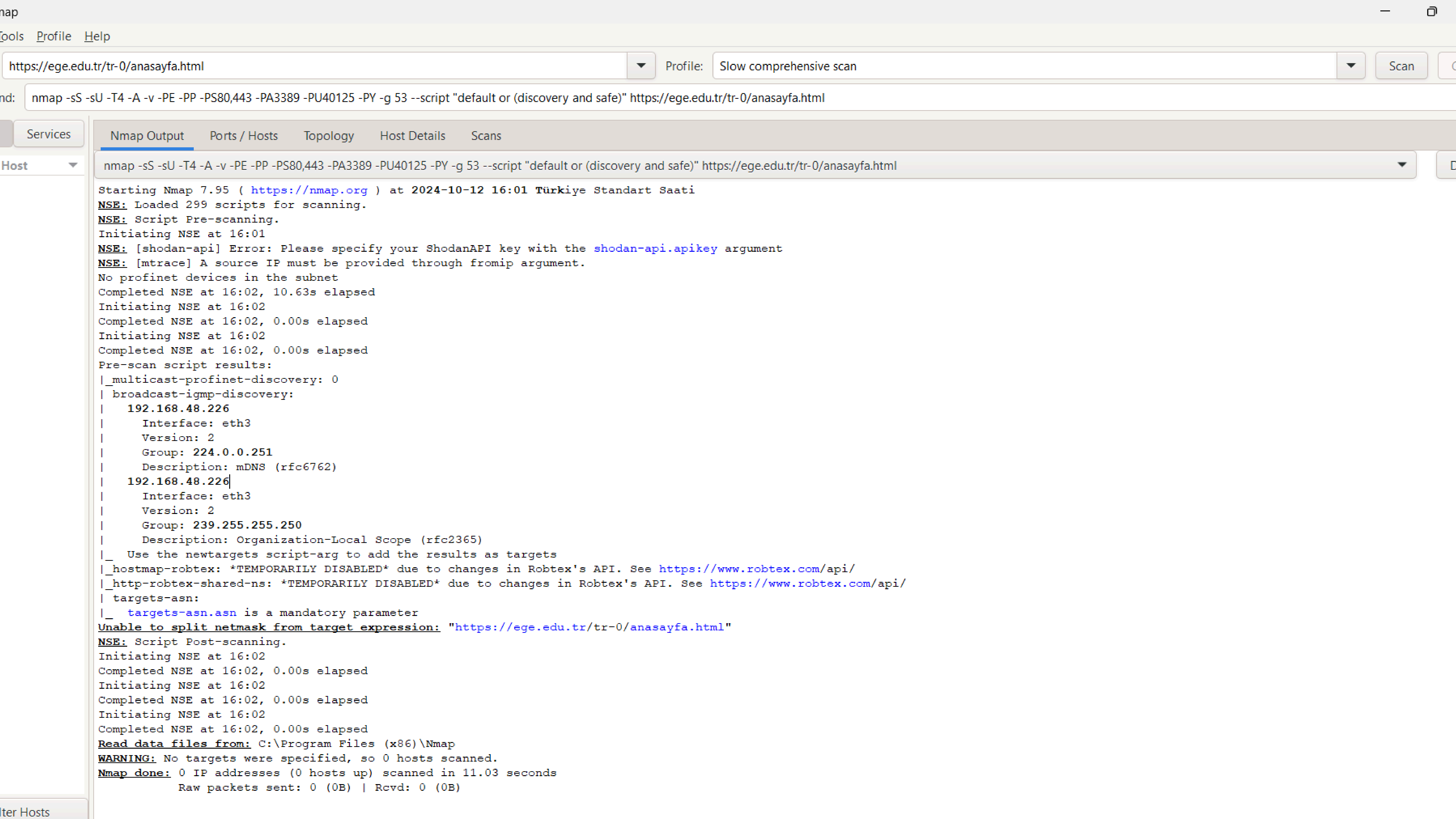
```
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=10/12%OT=53%CT=1%CU=37165%PV=Y%DS=1%DC=D%G=Y%M=3EFADD%
OS:TM=670A6F44%P=i686-pc-windows-windows)SEQ(SP=101%GCD=1%ISR=10E%TI=Z%CI=Z
OS:%II=I%TS=A)SEQ(SP=104%GCD=1%ISR=104%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=105%GCD=1
OS:%ISR=105%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=105%GCD=1%ISR=106%TI=Z%CI=Z%II=I%TS=
OS:A)SEQ(SP=105%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW9%O2=M5B
OS:4ST11NW9%O3=M5B4NNT11NW9%O4=M5B4ST11NW9%O5=M5B4ST11NW9%O6=M5B4ST11)WIN(W
OS:1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%
OS:O=M5B4%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R
OS:=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=
OS:AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=
OS:40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID
OS:=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 13.779 days (since Sat Sep 28 21:03:10 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1   91.04 ms 192.168.48.226

NSE: Script Post-scanning.
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Initiating NSE at 15:44
Completed NSE at 15:44, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 33.93 seconds
           Raw packets sent: 1111 (52.918KB) | Rcvd: 1090 (47.330KB)
```

EGE ÜNIVERSITESI

Kullanılan diller ve yazılımlar: javascript ASP.NET 4.0.30319

Dev tools: HTML5 Shiv

Obs: PHP 7.2.11 web sv Apache 2.4.27



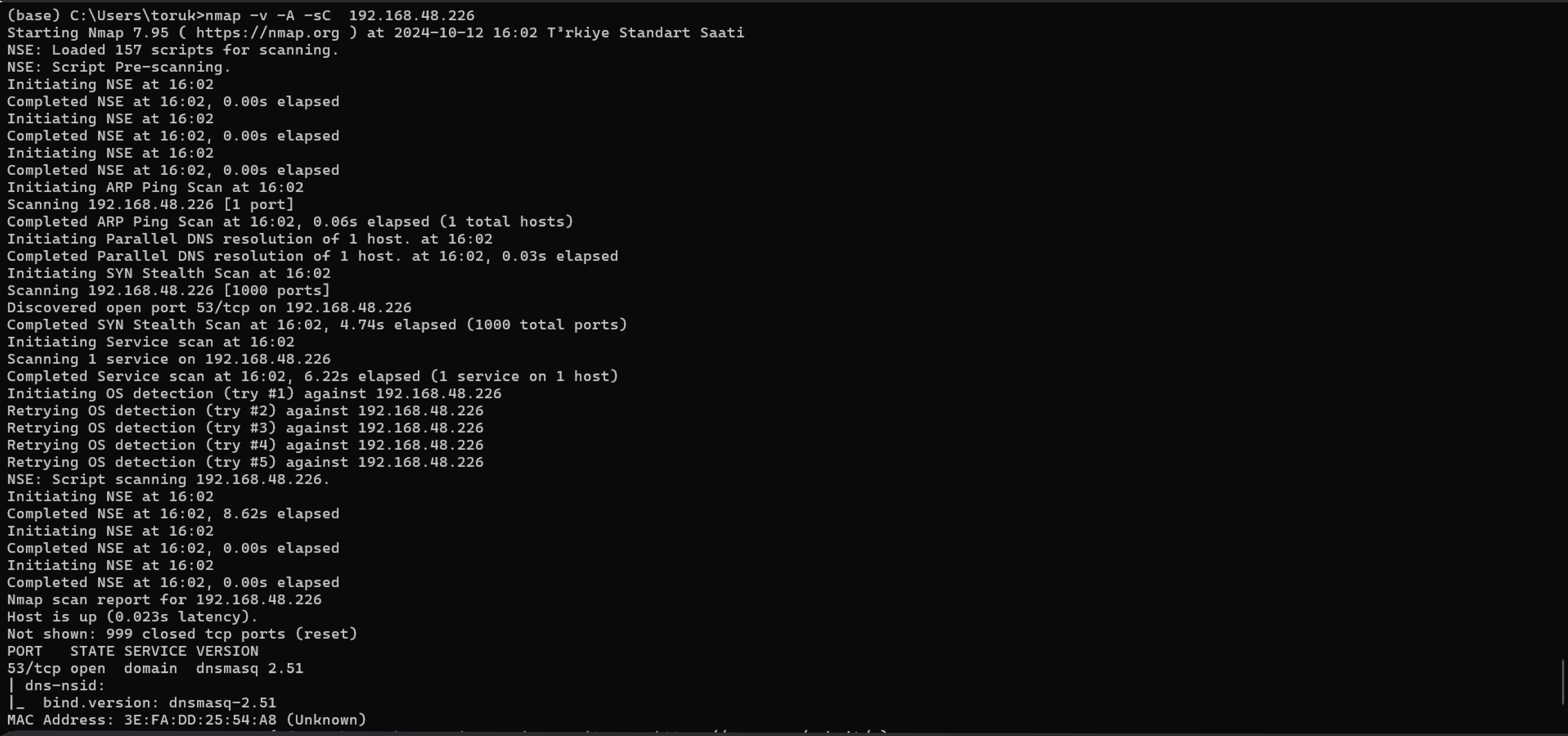
https://ege.edu.tr/tr-0/anasayfa.html

Profile: Slow comprehensive scan

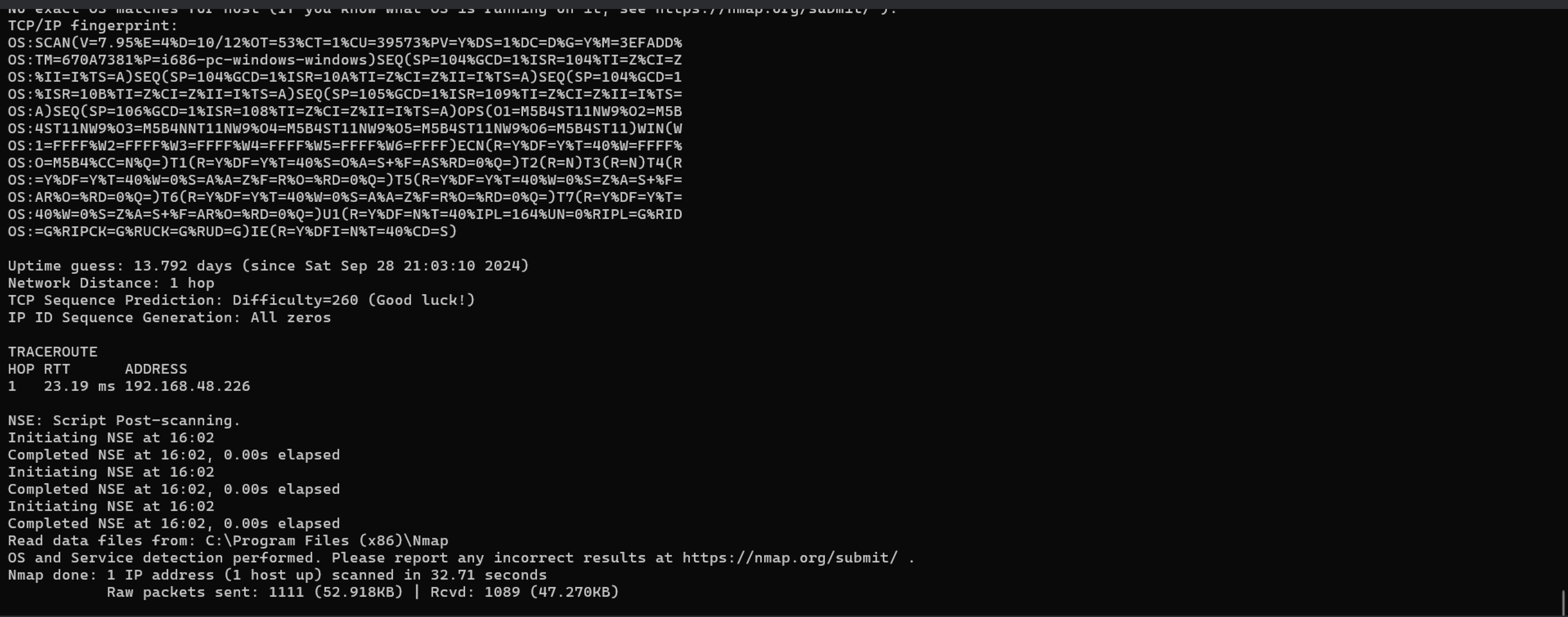
nd: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://ege.edu.tr/tr-0/anasayfa.html

```
nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://ege.edu.tr/tr-0/anasayfa.html
```

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 16:01 Türkiye Standart Saati
NSE: Loaded 299 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:01
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
NSE: [mtrace] A source IP must be provided through fromip argument.
No profinet devices in the subnet
Completed NSE at 16:02, 10.63s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Pre-scan script results:
|_multicast-profinet-discovery: 0
| broadcast-igmp-discovery:
|   192.168.48.226
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.48.226
|     Interface: eth3
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
Unable to split netmask from target expression: "https://ege.edu.tr/tr-0/anasayfa.html"
NSE: Script Post-scanning.
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 11.03 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```



```
(base) C:\Users\toruk>nmap -v -A -sC  192.168.48.226
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 16:02 T³rkiye Standart Saati
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating ARP Ping Scan at 16:02
Scanning 192.168.48.226 [1 port]
Completed ARP Ping Scan at 16:02, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:02
Completed Parallel DNS resolution of 1 host. at 16:02, 0.03s elapsed
Initiating SYN Stealth Scan at 16:02
Scanning 192.168.48.226 [1000 ports]
Discovered open port 53/tcp on 192.168.48.226
Completed SYN Stealth Scan at 16:02, 4.74s elapsed (1000 total ports)
Initiating Service scan at 16:02
Scanning 1 service on 192.168.48.226
Completed Service scan at 16:02, 6.22s elapsed (1 service on 1 host)
Initiating OS detection (try #1) against 192.168.48.226
Retrying OS detection (try #2) against 192.168.48.226
Retrying OS detection (try #3) against 192.168.48.226
Retrying OS detection (try #4) against 192.168.48.226
Retrying OS detection (try #5) against 192.168.48.226
NSE: Script scanning 192.168.48.226.
Initiating NSE at 16:02
Completed NSE at 16:02, 8.62s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Nmap scan report for 192.168.48.226
Host is up (0.023s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
53/tcp open  domain  dnsmasq 2.51
| dns-nsid:
|_  bind.version: dnsmasq-2.51
MAC Address: 3E:FA:DD:25:54:A8 (Unknown)
```



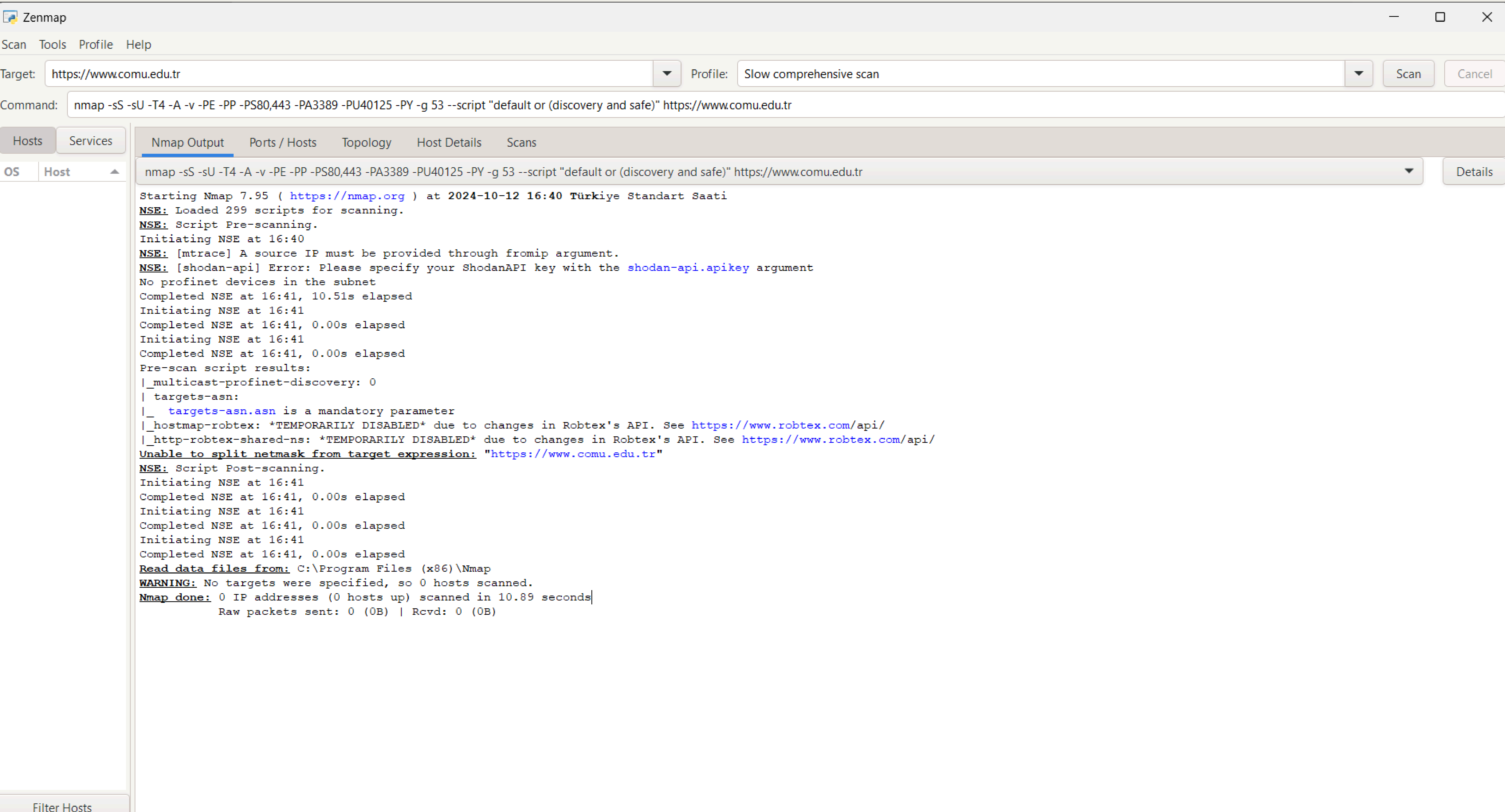
```
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=4%D=10/12%OT=53%CT=1%CU=39573%PV=Y%DS=1%DC=D%G=Y%M=3EFADD%
OS:TM=670A7381%P=i686-pc-windows-windows)SEQ(SP=104%GCD=1%ISR=104%TI=Z%CI=Z
OS:%II=I%TS=A)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=104%GCD=1
OS:%ISR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=105%GCD=1%ISR=109%TI=Z%CI=Z%II=I%TS=
OS:A)SEQ(SP=106%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M5B4ST11NW9%O2=M5B
OS:4ST11NW9%O3=M5B4NNT11NW9%O4=M5B4ST11NW9%O5=M5B4ST11NW9%O6=M5B4ST11)WIN(W
OS:1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)ECN(R=Y%DF=Y%T=40%W=FFFF%
OS:O=M5B4%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R
OS:=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=
OS:AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=
OS:40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID
OS:=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 13.792 days (since Sat Sep 28 21:03:10 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE
HOP RTT      ADDRESS
1   23.19 ms 192.168.48.226

NSE: Script Post-scanning.
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Initiating NSE at 16:02
Completed NSE at 16:02, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
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 32.71 seconds
           Raw packets sent: 1111 (52.918KB) | Rcvd: 1089 (47.270KB)
```

ÇANAKKALE 18 MART

Kullanılan diller ve yazılımlar: php html css Javascript

Frameworks: Respond JS HTML5 Shiv

Obs: ASP.NET 4.0.30319



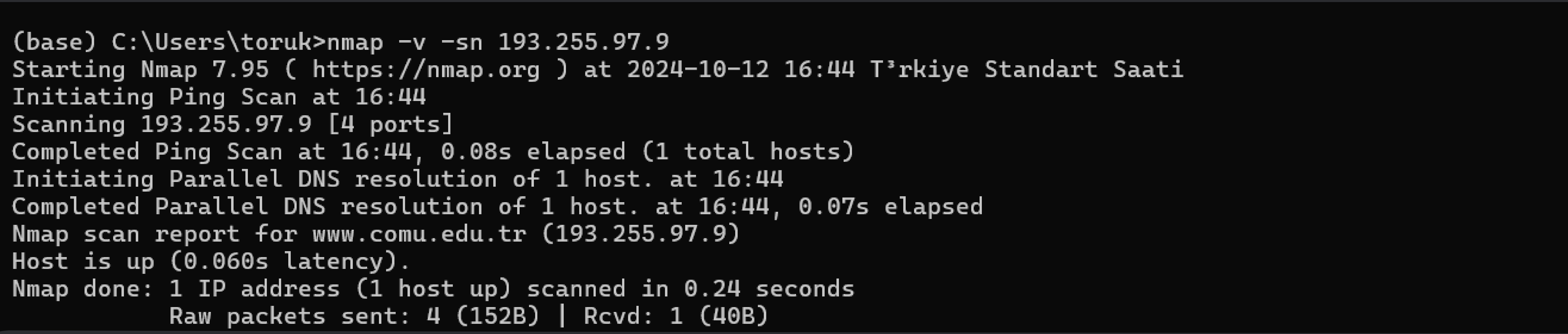
Target: https://www.comu.edu.tr

Profile: Slow comprehensive scan

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.comu.edu.tr

nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.comu.edu.tr

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 16:40 Türkiye Standart Saati
NSE: Loaded 299 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:40
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
No profinet devices in the subnet
Completed NSE at 16:41, 10.51s elapsed
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Pre-scan script results:
|_multicast-profinet-discovery: 0
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Unable to split netmask from target expression: "https://www.comu.edu.tr"
NSE: Script Post-scanning.
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Initiating NSE at 16:41
Completed NSE at 16:41, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.89 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```



```
(base) C:\Users\toruk>nmap -v -sn 193.255.97.9
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-12 16:44 T³rkiye Standart Saati
Initiating Ping Scan at 16:44
Scanning 193.255.97.9 [4 ports]
Completed Ping Scan at 16:44, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:44
Completed Parallel DNS resolution of 1 host. at 16:44, 0.07s elapsed
Nmap scan report for www.comu.edu.tr (193.255.97.9)
Host is up (0.060s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
           Raw packets sent: 4 (152B) | Rcvd: 1 (40B)
```

TRAKYA ÜNIVERSITESI

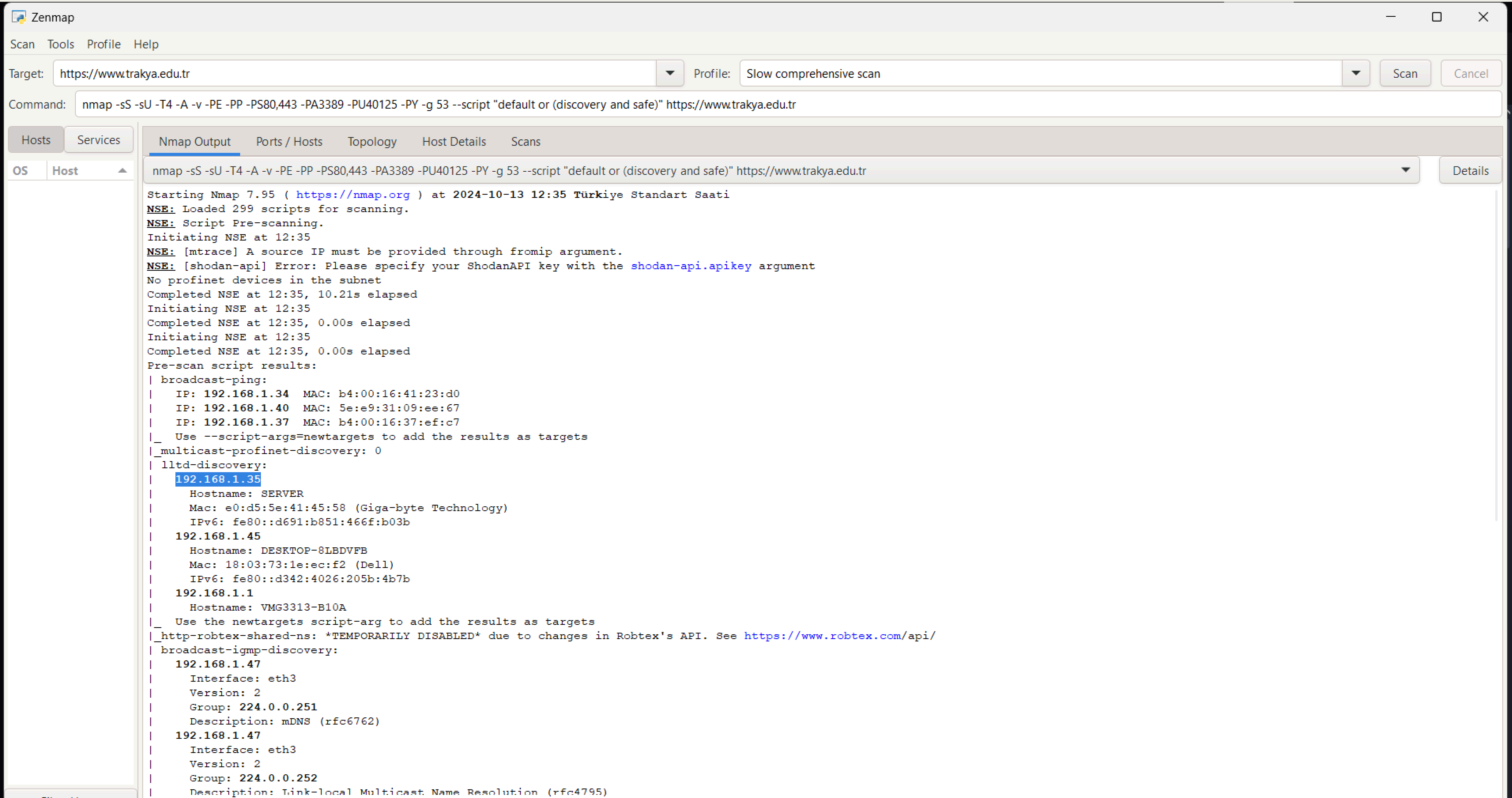
Kullanılan diller ve yazılımlar: HTML5 Shiv

Web Server: Apache 2.4.6

Frameworks: Respond JS HTML5 Shiv

Obs: PHP 5.6.40

web server extensions: OpenSSL 1.0.2k



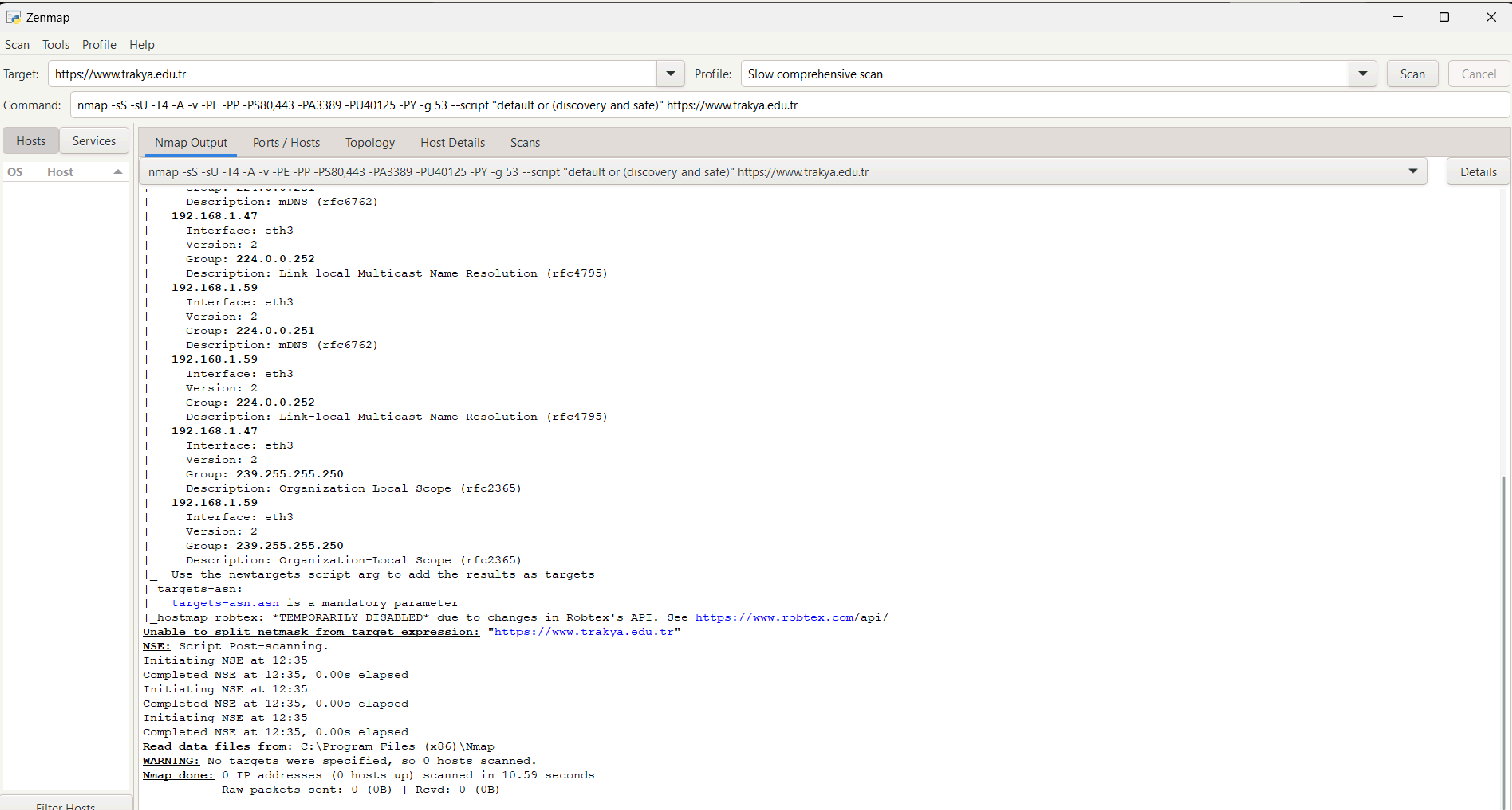
Target: https://www.trakya.edu.tr

Profile: Slow comprehensive scan

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.trakya.edu.tr

nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.trakya.edu.tr

```
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 12:35 Türkiye Standart Saati
NSE: Loaded 299 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:35
NSE: [mtrace] A source IP must be provided through fromip argument.
NSE: [shodan-api] Error: Please specify your ShodanAPI key with the shodan-api.apikey argument
No profinet devices in the subnet
Completed NSE at 12:35, 10.21s elapsed
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
Pre-scan script results:
| broadcast-ping:
|   IP: 192.168.1.34  MAC: b4:00:16:41:23:d0
|   IP: 192.168.1.40  MAC: 5e:e9:31:09:ee:67
|   IP: 192.168.1.37  MAC: b4:00:16:37:ef:c7
|_  Use --script-args=newtargets to add the results as targets
|_multicast-profinet-discovery: 0
| lltd-discovery:
|   192.168.1.35
|     Hostname: SERVER
|     Mac: e0:d5:5e:41:45:58 (Giga-byte Technology)
|     IPv6: fe80::d691:b851:466f:b03b
|   192.168.1.45
|     Hostname: DESKTOP-8LBDVFB
|     Mac: 18:03:73:1e:ec:f2 (Dell)
|     IPv6: fe80::d342:4026:205b:4b7b
|   192.168.1.1
|     Hostname: VMG3313-B10A
|_  Use the newtargets script-arg to add the results as targets
|_http-robtex-shared-ns: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
| broadcast-igmp-discovery:
|   192.168.1.47
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.1.47
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution (rfc4795)
```

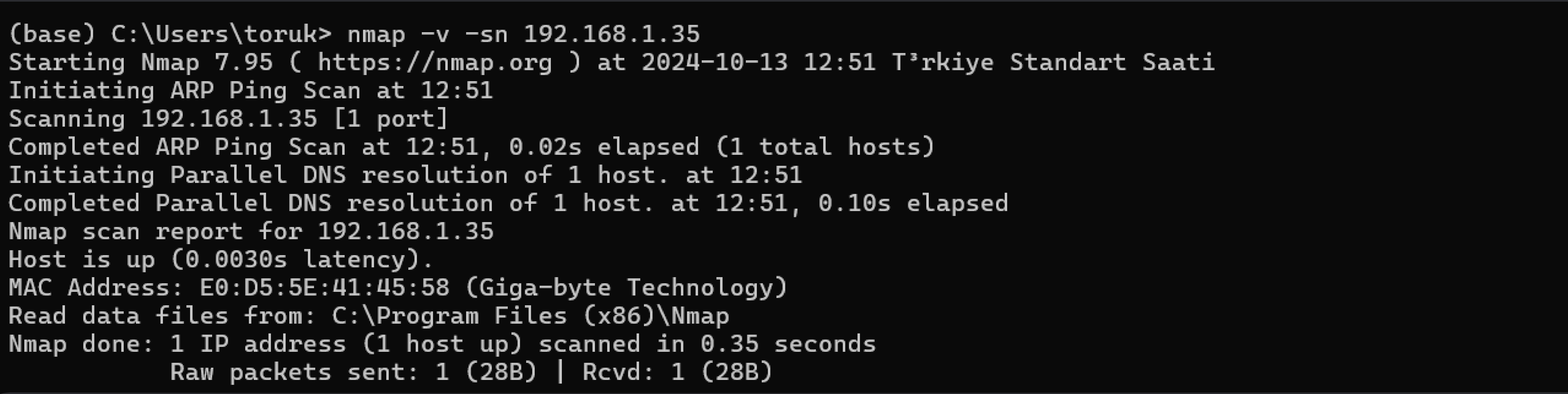


Target: https://www.trakya.edu.tr

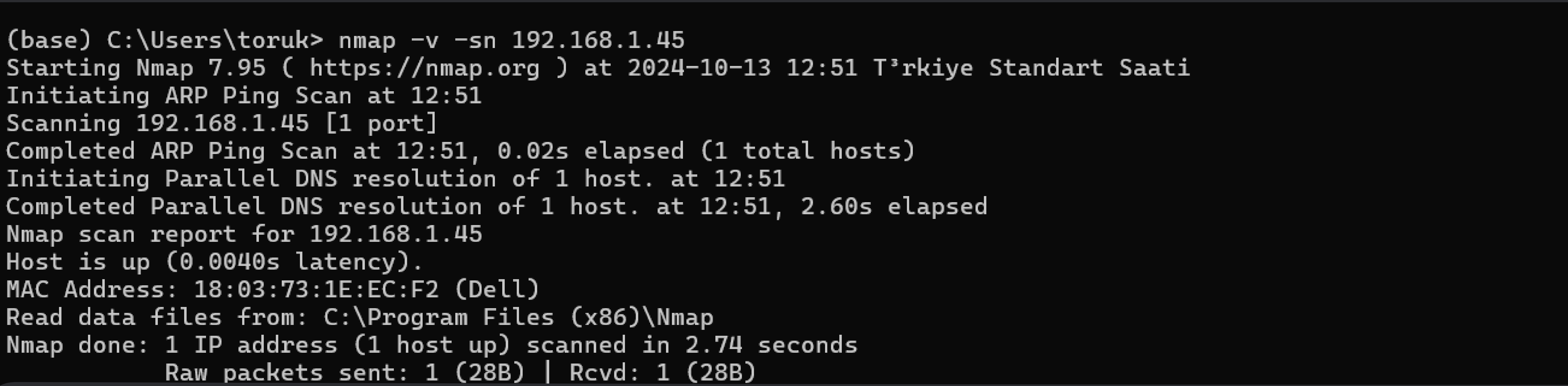
Profile: Slow comprehensive scan

Command: nmap -sS -sU -T4 -A -v -PE -PP -PS80,443 -PA3389 -PU40125 -PY -g 53 --script "default or (discovery and safe)" https://www.trakya.edu.tr

```
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.1.47
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution (rfc4795)
|   192.168.1.59
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.251
|     Description: mDNS (rfc6762)
|   192.168.1.59
|     Interface: eth3
|     Version: 2
|     Group: 224.0.0.252
|     Description: Link-local Multicast Name Resolution (rfc4795)
|   192.168.1.47
|     Interface: eth3
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|   192.168.1.59
|     Interface: eth3
|     Version: 2
|     Group: 239.255.255.250
|     Description: Organization-Local Scope (rfc2365)
|_  Use the newtargets script-arg to add the results as targets
| targets-asn:
|_  targets-asn.asn is a mandatory parameter
|_hostmap-robtex: *TEMPORARILY DISABLED* due to changes in Robtex's API. See https://www.robtex.com/api/
Unable to split netmask from target expression: "https://www.trakya.edu.tr"
NSE: Script Post-scanning.
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
Initiating NSE at 12:35
Completed NSE at 12:35, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 10.59 seconds
           Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
```



```
(base) C:\Users\toruk> nmap -v -sn 192.168.1.35
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 12:51 T³rkiye Standart Saati
Initiating ARP Ping Scan at 12:51
Scanning 192.168.1.35 [1 port]
Completed ARP Ping Scan at 12:51, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:51
Completed Parallel DNS resolution of 1 host. at 12:51, 0.10s elapsed
Nmap scan report for 192.168.1.35
Host is up (0.0030s latency).
MAC Address: E0:D5:5E:41:45:58 (Giga-byte Technology)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```



```
(base) C:\Users\toruk> nmap -v -sn 192.168.1.45
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-13 12:51 T³rkiye Standart Saati
Initiating ARP Ping Scan at 12:51
Scanning 192.168.1.45 [1 port]
Completed ARP Ping Scan at 12:51, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:51
Completed Parallel DNS resolution of 1 host. at 12:51, 2.60s elapsed
Nmap scan report for 192.168.1.45
Host is up (0.0040s latency).
MAC Address: 18:03:73:1E:EC:F2 (Dell)
Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 2.74 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```