

## Nmap Nedir?

Nmap, ağ tarama ve zayıf tespiti için kullanılan açık kaynaklı bir araçtır. Bu araç birçok sisteme yönelik taramaları gerçekleştirerek esnek, hızlı ve anlamlı bir şekilde sonuç üretmektedir. Sistemlerin açık olup olmadığını, açık olan sistemlerin portlarını durumları, hangi servislerin çalıştığı ve kullanılan işletim sistemi gibi birçok bilgiyi verebilmektedir. Nmap ile tespit edilen servislerin güvenlik açığı barındırıp barındırmadığı ve kullanılan servisler hakkında bilgi elde edilebilir. Ayrıca içerisinde barındırmış olduğu scriptler ile hedef sisteme yönelik tarama gerçekleştirildiğinde hedef sistem hakkında detaylı bilgi ve güvenlik açığı olup olmamasına yönelik sonuç üretmektedir. Nmap aracı, alanının en iyi araçları arasında yer almaktadır.

## NMAP TARAMA AŞAMALARI

Nmap uygulaması kullanılarak taramanın başarılı bir şekilde sonuçlanması için belirli aşamalar takip edilerek tarama işlemleri yapılmalıdır.

### Tarama Öncesi Scriptlerin Kullanılması

Nmap aracı, taranacak ağ hakkında bilgi toplamak için scriptler barındırır. Örneğin, ağ servislerinden bilgi almak için broadcast sorgularını kullanan dhcp-discover ve broadcast-dns-service-discover gibi scriptler kullanılmaktadır.

### Hedef Numaralandırma

Nmap, hedef numaralandırma işlemlerinde DNS, IP adresleri, CIDR değerleri gibi host belirteçlerini tespit etmektedir. Hedef hostları belirlemek için –iR parametresi kullanılabilir.

### Host Keşif İşlemleri

Nmap'te host keşif işlemleri genellikle bir makinenin aktif olup olmadığını tespit etmek için yapılmaktadır. Nmap varsayılan olarak önce host keşfi yapar ve sonra port taramasına başlar. Eğer port taraması yapmadan sadece host keşif işlemi yapılmak isteniyorsa –sn parametresi kullanılır. Host keşif işleminin yapılması istenmiyorsa –Pn parametresi kullanılabilir. –Pn parametresinin kullanılması ile hostlara ping atılmaz. Böylelikle host keşfi yapılmaz.

### Reverse-DNS Resolution

Nmap, ping taraması ile tarayıp belirdiği aktif makinelere yönelik Reverse-DNS çözümleme işlemi gerçekleştirilmektedir. Reverse-DNS çözümlemesi, –R parametresi ile yapılır. Normal şartlarda yalnızca açık makinelere yapılır.

## Port Taraması

Port taraması, Nmap aracının ana işlevlerinden biridir. Aktif olan bir sistemin portlarına istek atarak, portların açık veya kapalı olma durumunu tespit eder.

## Versiyon Tespiti

Tespit edilen açık portlarda hangi servisin çalıştığını tespiti için kullanılır. Nmap aracı içerisinde barındırmış olduğu problemler ve 6500'den fazla servis imzası ile portlarda bulunan servisleri karşılaştırıp tespit etmektedir. Bu işlem `-sV` parametresi kullanılarak gerçekleştirilmektedir.

## İşletim Sistemi Tespiti

Nmap ile açık olan makinelere yönelik işletim sistemi tespiti yapılmaktadır. Nmap içerisinde bulunan bir veritabanında işletim sistemlerinin yanıtları bulunmaktadır. Nmap oluşturmuş olduğu problemleri makinelere göndererek makinelerden gelen yanıtları veritabanında bulunan yanıtlarla karşılaştırılmaktadır. Böylelikle kullanılan işletim sistemi bilgisi elde edilmektedir. Nmap aracı üzerinde bu işlem `-O` parametresi kullanılarak gerçekleştirilmektedir.

## Traceroute İşlemi

Nmap, `-traceroute` parametresi ile her hedef için paketlerin hangi yoldan geçtiğini tespit edebilir.

## Script Taraması

Nmap içerisinde, Nmap Script Engine(NSE) adı verilen bir yapı bulunmaktadır. Bu yapı içerisinde birçok script bulunur. Bu scriptler kullanılarak hedefe yönelik bilgi toplama ve güvenlik açığı tespit etme gibi birçok işlem gerçekleştirilebilmektedir. NSE, lua programlama dili ve ağ üzerinde bilgi toplama için tasarlanmış standart bir kütüphane tarafından desteklenmektedir. Bu scriptler genellikle tespit edilen her host üzerinde bulunan her bir port için bir kere çalıştırılmaktadır. `-script` veya `-sC` parametreleri kullanarak Nmap üzerindeki script'ler çalıştırılabilir.

## Çıktı Alma

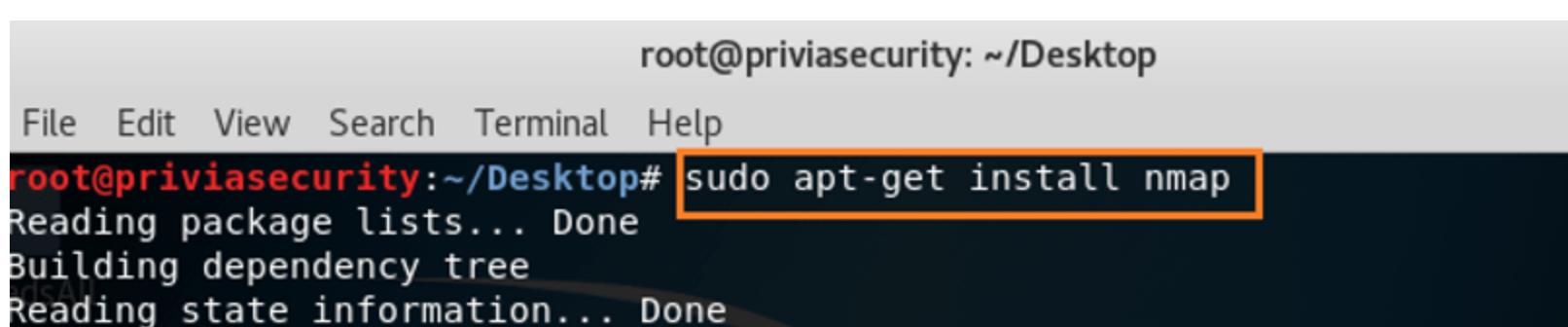
Nmap, tarama işlemleri sonucunda elde ettiği bilgileri ekrana basar. Bu sonuçlar farklı dosya formatlarında kaydedilebilir.

## Nmap Kurulumu

### Linux (Debian/Ubuntu) Ortamı

Terminal'de “`sudo apt-get install nmap`” komutu çalıştırıldığında Nmap yüklenmeye başlayacaktır. Ayrıca `nmap`, sitesinden `.rpm` veya `.deb` uzantılı `setup` dosyaları indirilerek kurulabilir.

Şekil 2.1.1 – Linux Ortamında Kurulum



```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
root@priviasecurity:~/Desktop# sudo apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

Şekil 2.1.1'de gösterildiği gibi “`sudo apt-get install nmap`” komutu ile kolay bir şekilde kurulum gerçekleştirilebilir.

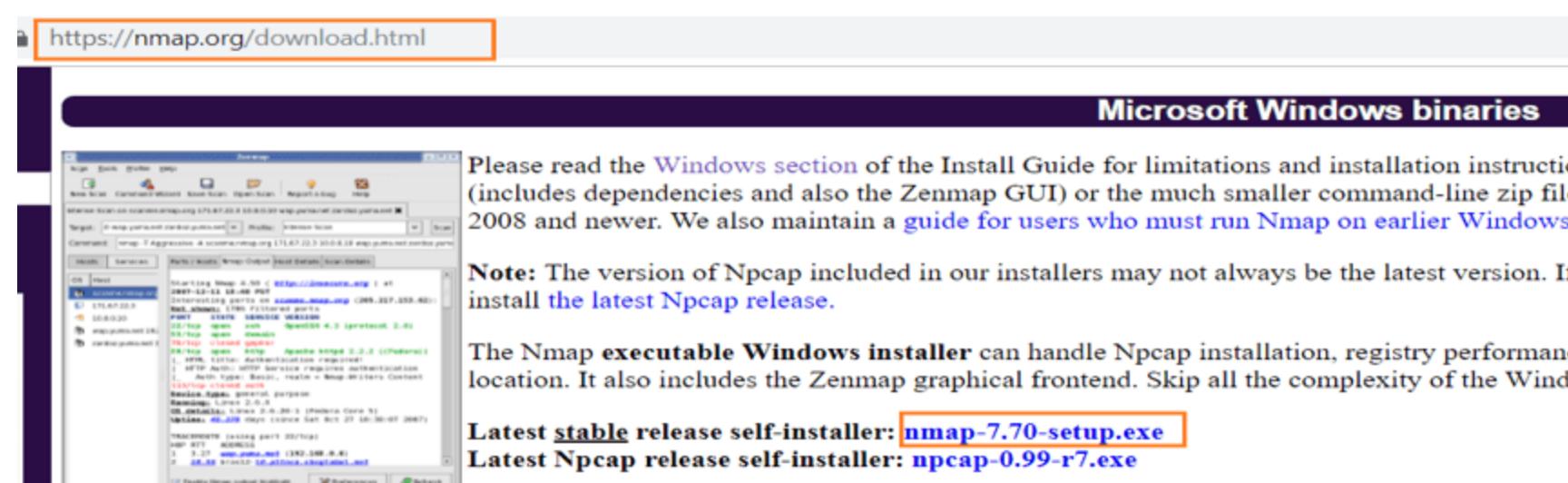
```
root@priviasecurity: ~
File Edit View Search Terminal Help

root@priviasecurity:~# nmap --help
Nmap 7.50 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude file>: Exclude list from file
```

## Windows Ortamı

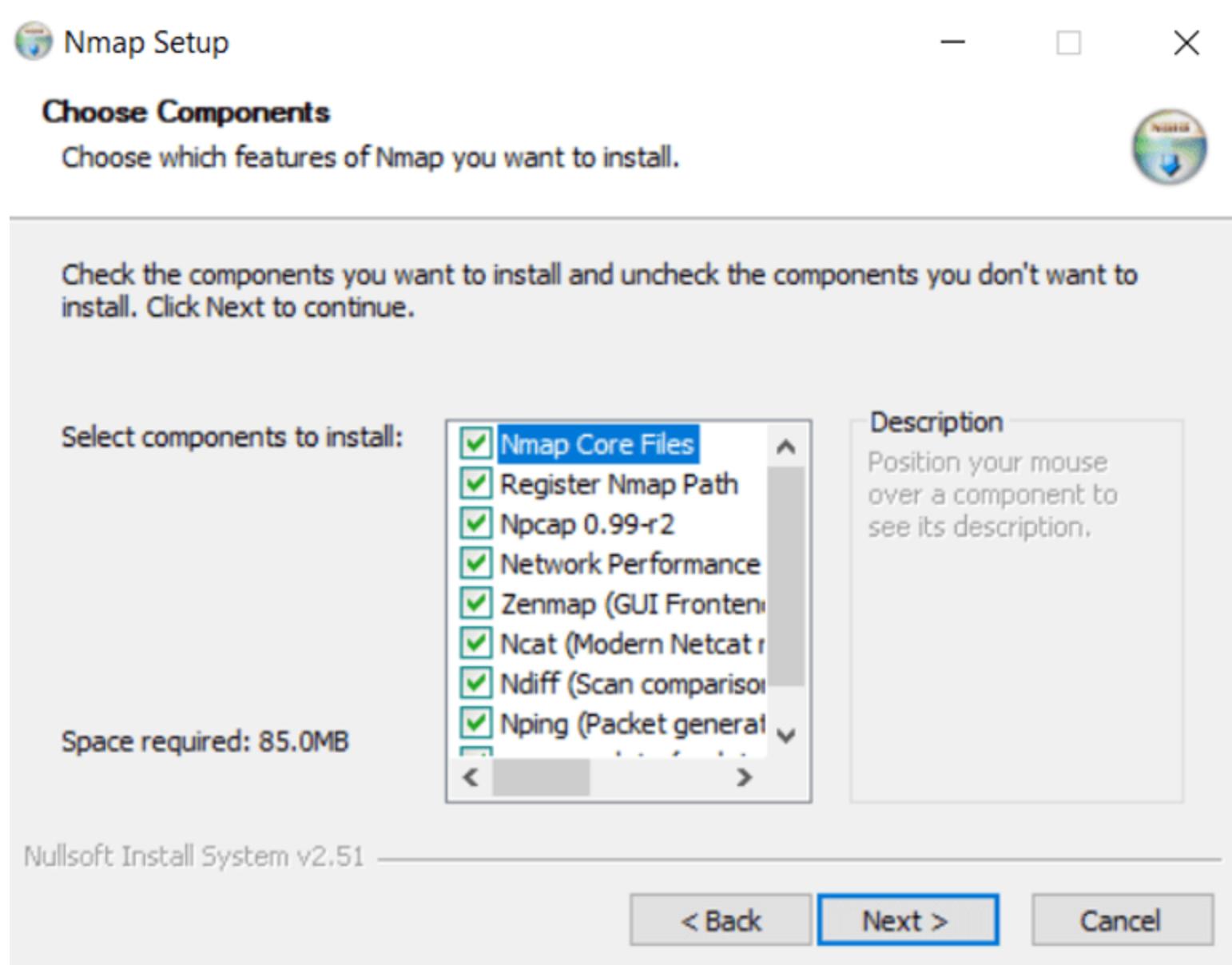
Nmap aracının Windows ortamındaki kurulumunu sağlamak için <https://nmap.org/download.html> uzantılı sayfasından aşağıda gösterileceği gibi indirme işlemi gerçekleştirilecektir.

Şekil 2.2.1 – Windows Ortamı için İndirme İşlemi



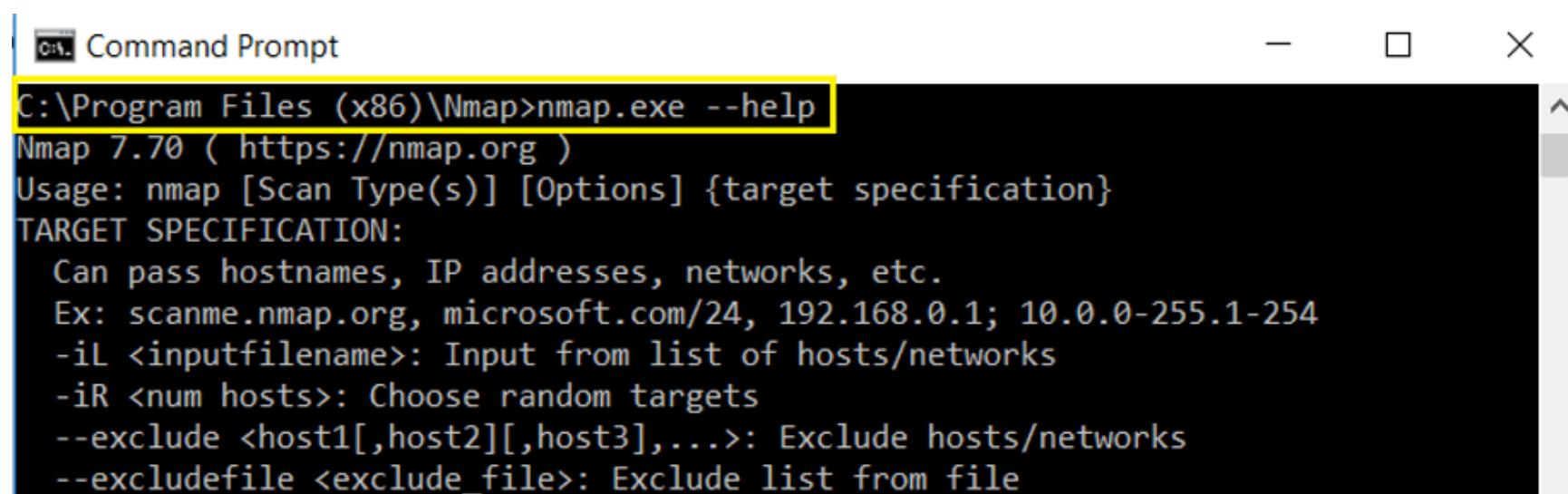
Daha sonra indirilen .exe uzantılı nmap setup'ı yönetici olarak çalıştırılmaktadır.

Şekil 2.2.2 – Windows Kurulum Gösterimi



Kurulum işlemi bittikten sonra **Program Files(x86)\Nmap** dizinin altındaki **nmap.exe** uygulaması çalıştırılabilir. Ayrıca bu kurulumla birlikte Nmap'in grafik kullanıcı arayüzlü hali olan **zenmap** uygulaması da yüklenecektir.

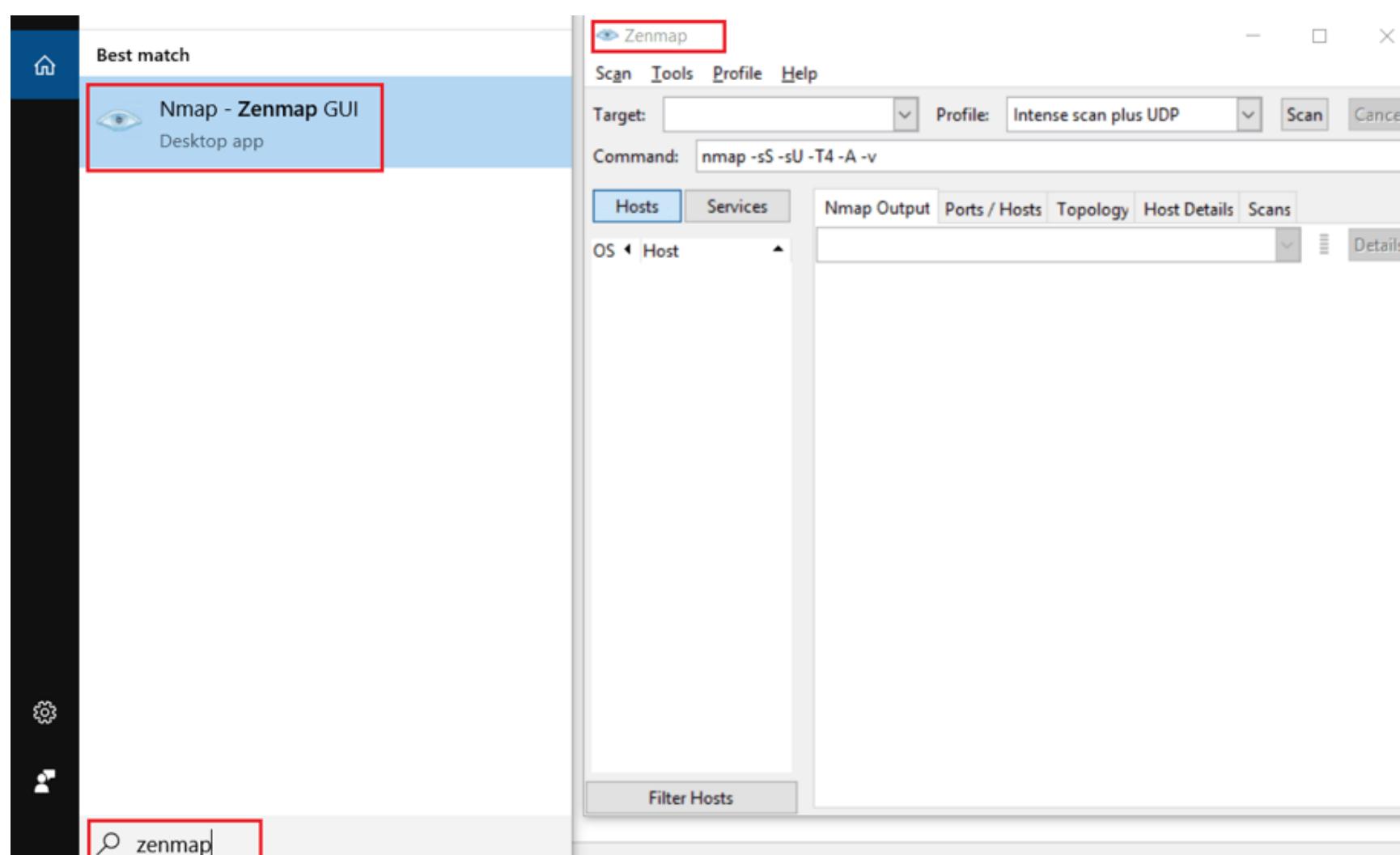
Şekil 2.2.3 – Command Prompt Ekranında Nmap



```
C:\Program Files (x86)\Nmap>nmap.exe --help
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

Şekil 2.2.3'te Command Prompt ekranı üzerinde nmap.exe çalıştırılmıştır.

Şekil 2.2.4 – Windows Ortamında ZenMap Uygulamasının Çalıştırılması



Şekil 2.2.3 ve Şekil 2.2.4'te gösterildiği gibi Nmap ve Zenmap araçları Linux ortamında da mevcuttur. Terminal üzerinden **nmap** ve **zenmap** komutu çalıştırılarak görüntülenebilir.

## Host Keşif İşlemleri

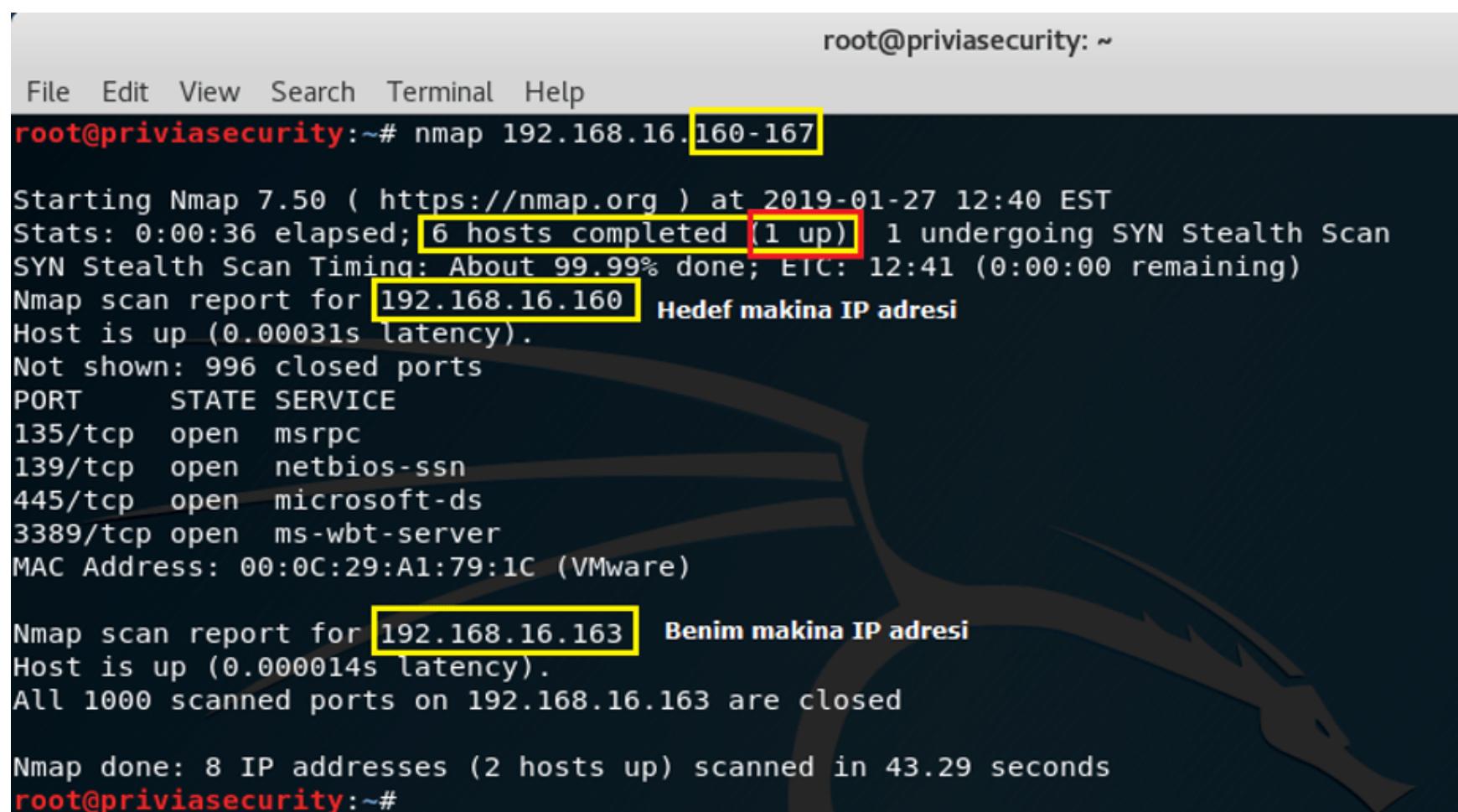
Host keşfi, ağda bulunan sistemlere ping atılarak gerçekleştirilir. Fakat bu işlemler geniş ağlara yönelik yapıldığında veya var olan ağ üzerinde ICMP paketlerine yönelik cevap vermeyen bazı makineler olduğunda farklı yöntemler kullanılarak host keşfi yapılabilir. Hedef ağ üzerinde ping atmadan tarama işlemleri gerçekleştirilebilir. Ayrıca TCP, SYN/ACK, UDP gibi protoller isteğe bağlı olarak kullanılabilir. Bu protollerin amacı, türüne göre protoller gönderildikten sonra, alınan yanıt doğrultusunda verilen IP adresine sahip makinenin gerçekten açık olup olmadığını tespit etmektir.

## Hedef Hostları ve Ağları Belirlemek

Hedef hostları belirlemek için Nmap'e hedef ağın IP adresi veya Hostname bilgisi girilmelidir. Bir IP adresinin yerine IP adresi aralığı verilebilir. Ayrıca, Nmap uygulaması CIDR adreslemeyi desteklemektedir. CIDR, ip adresinden veya hostname'den sonra gelen /24, /18 vb. değerlerdir. Bu değerler sonucunda Nmap uygulaması kendi içerisinde bunu işlemlerini yaparak kaç hostun taraması gerektiğini hesaplayıp otomatik olarak tarama işlemini gerçekleştirmektedir.

Örneğin, 192.168.10.0/24 IP adresini girdiğimizde 256 tane hostu taramaktadır. Ayrıca hostname adını belirterek tarama aynı şekilde gerçekleştirilmektedir. Örneğin, priviasecurity.com/24 diyerek de bir tarama başlatılabilir.

Şekil 3.1 – Örnek Host Keşif Sorgusu



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap 192.168.16.160-167

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 12:40 EST
Stats: 0:00:36 elapsed; 6 hosts completed (1 up) 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:41 (0:00:00 remaining)
Nmap scan report for 192.168.16.160  Hedef makina IP adresi
Host is up (0.00031s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap scan report for 192.168.16.163  Benim makina IP adresi
Host is up (0.000014s latency).
All 1000 scanned ports on 192.168.16.163 are closed

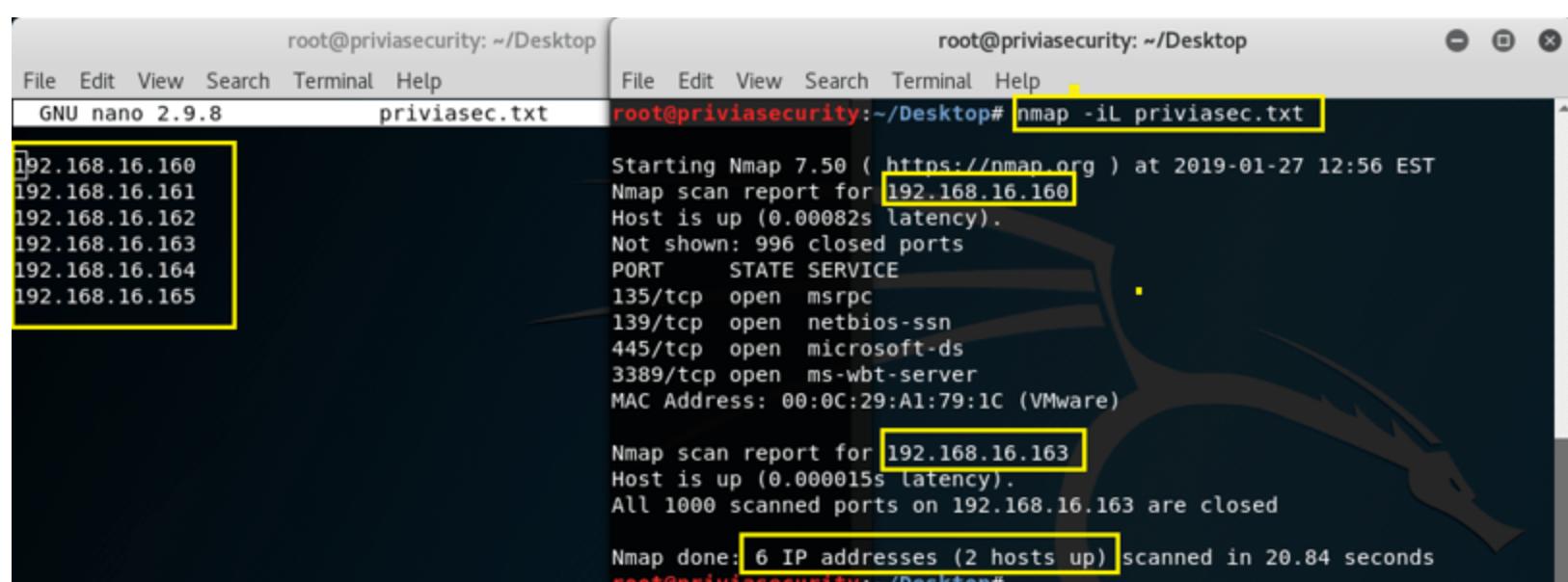
Nmap done: 8 IP addresses (2 hosts up) scanned in 43.29 seconds
root@priviasecurity:~#
```

Şekil 3.1'de gösterildiği gibi nmap uygulaması üzerinden bir IP aralığı verilmektedir. Bu tarama sonucunda verilen IP aralığında da tarama gerçekleştirilmektedir.

## IP Listesi Belirtmek

Bu tür tarama işlemleri genellikle geniş ağ taramalarında gerçekleştirilmektedir. Verilen yüzlerce veya binlerce IP adresini bir dosyaya kaydettikten sonra –iL parametresi kullanılarak tarama işlemleri başlatılabilir.

Şekil 3.1.1 – Nmap Uygulaması ile Liste Taraması Gerçekleştirmek



```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
GNU nano 2.9.8      priviasec.txt
root@priviasecurity:~/Desktop# nmap -iL priviasec.txt

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 12:56 EST
Nmap scan report for 192.168.16.160
Host is up (0.00082s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap scan report for 192.168.16.163
Host is up (0.000015s latency).
All 1000 scanned ports on 192.168.16.163 are closed

Nmap done: 6 IP addresses (2 hosts up) scanned in 20.84 seconds
root@priviasecurity:~/Desktop#
```

Şekil 3.1.1'de gösterildiği gibi nmap komutundan sonra –iL parametresi kullanılarak içerisinde IP adresleri bulunan bir dosya belirtilir ve tarama işlemi gerçekleştirilir.

## Rastgele Hedef Seçmek

Nmap aracı ile rastgele IP adreslerinin taraması için –iR parametresi kullanılarak yapılmaktadır.

## Kapsam Dışı Hedefleri Belirlemek

Genellikle gözden kaçan durumlardan biri olan kapsam dışı hedefleri belirleme işlemleri, riskli işlemleri önlemektedir. Tarama yapılacak ağda, taranması istenmeyen IP adresleri –exclude parametresi ile belirtilir. Birçok IP adresi olduğu durumlarda, IP adresleri bir dosyaya kaydedildikten sonra –excludefile parametresi ile bu işlemler gerçekleştirilmektedir.

```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
root@priviasecurity:~/Desktop# nmap 192.168.16.160-167 --exclude 192.168.16.161,192.168.16.163
Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 13:31 EST
Nmap scan report for 192.168.16.160
Host is up (0.00053s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 6 IP addresses (1 host up) scanned in 4.48 seconds
root@priviasecurity:~/Desktop# nmap 192.168.16.160-167 --exclude 192.168.16.161,192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 13:32 EST
Nmap scan report for 192.168.16.163
Host is up (0.000040s latency).
All 1000 scanned ports on 192.168.16.163 are closed

Nmap done: 6 IP addresses (1 host up) scanned in 2.30 seconds
root@priviasecurity:~/Desktop#
```

Şekil 3.1.3'de gösterildiği gibi **--exclude** parametresinden sonra belirtilen IP adresleri tarama dışında tutulmaktadır. Ayrıca taranması istenmeyen IP adresleri birden fazla olduğunda **--excludefile** parametresi kullanılabilir.

Şekil 3.14'te, taranacak bir ağıdaki IP adreslerinin listelenmesi için **-sL** parametresi kullanılır.

Şekil 3.1.4 – Nmap ile **-sL** Parametresinin Kullanılması

```
root@priviasecurity: ~/Desktop
File Edit View Search Terminal Help
root@priviasecurity:~/Desktop# nmap -sL 192.168.16.160/29
Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 14:02 EST
Nmap scan report for 192.168.16.160
Nmap scan report for 192.168.16.161
Nmap scan report for 192.168.16.162
Nmap scan report for 192.168.16.163
Nmap scan report for 192.168.16.164
Nmap scan report for 192.168.16.165
Nmap scan report for 192.168.16.166
Nmap scan report for 192.168.16.167
Nmap done: 8 IP addresses (0 hosts up) scanned in 0.13 seconds
root@priviasecurity:~/Desktop#
```

Eğer birbirinden farklı hedeflerin IP adresleri veya hostnameleri taranmak istenirse IP adresleri arasında boşluk bırakılarak tarama işlemi gerçekleştirilebilir. Şekil 3.1.5'de gösterilmiştir.

Şekil 3.1.5 – Nmap ile Farklı Hedeflerin Bir Anda Taranması

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap priviasecurity.com 192.168.16.160 192.168.16.163

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-27 15:55 EST
Nmap scan report for priviasecurity.com (104.18.41.10)
Host is up (0.023s latency).
Other addresses for priviasecurity.com (not scanned): 104.18.40.10 2606:4700:30::6812:290a 2606:4700:30::6812:280a
Not shown: 998 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 192.168.16.160
Host is up (0.00058s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap scan report for 192.168.16.163
Host is up (0.000038s latency).
All 1000 scanned ports on 192.168.16.163 are closed

Nmap done: 3 IP addresses (3 hosts up) scanned in 110.22 seconds
root@priviasecurity:~#
```

## Hedef Kuruluşun IP Adresinin Bulunması

Genellikle bir taramadan önce ana domain bilgisi verilmektedir. Verilen domain adresinin IP bilgileri üzerinden tarama işlemleri gerçekleştirilebilir.

### DNS Bilgilerinin Elde Edilmesi

DNS'in birincil amacı, domain adlarını IP adreslerine çözümlemektir. Bu nedenle DNS bilgilerini araştırılması gerekmektedir. Şekil 3.2.1'de gösterilmiştir.

Şekil 3.2.1 – DNS Kayıt Türlerinin Sorgulanması

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# host -t ns priviasecurity.com
priviasecurity.com name server uma.ns.cloudflare.com.
priviasecurity.com name server phil.ns.cloudflare.com.
root@priviasecurity:~# host -t a priviasecurity.com
priviasecurity.com has address 104.18.40.10
priviasecurity.com has address 104.18.41.10
root@priviasecurity:~# host -t aaaa priviasecurity.com
priviasecurity.com has IPv6 address 2606:4700:30::6812:280a
priviasecurity.com has IPv6 address 2606:4700:30::6812:290a
root@priviasecurity:~# host -t mx priviasecurity.com
priviasecurity.com mail is handled by 10 mx.yandex.net.
root@priviasecurity:~# host -t soa priviasecurity.com
priviasecurity.com has SOA record phil.ns.cloudflare.com. dns.cloudflare.com. 202
9610753 10000 2400 604800 3600
root@priviasecurity:~#
```

Şekil 3.2.1'de gösterildiği gibi linux ortamında DNS kayıt türlerinin öğrenilmesi için host yardımcı uygulaması kullanılarak nameserver'lar hakkında bilgi elde edilmektedir. Ayrıca zone transferi ile ilgili işlemler Şekil 3.2.2'de gösterilmektedir.

Şekil 3.2.2 – Zone Transfer İşleminin Kontrolü

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# host -t ns priviasecurity.com
priviasecurity.com name server phil.ns.cloudflare.com.
priviasecurity.com name server uma.ns.cloudflare.com.
root@priviasecurity:~# dig @phil.ns.cloudflare.com -t AXFR priviasecurity.com
;; Connection to 2400:cb00:2049:1::adf5:3b89#53(2400:cb00:2049:1::adf5:3b89) for
priviasecurity.com failed: network unreachable.
root@priviasecurity:~# dig @uma.ns.cloudflare.com -t AXFR priviasecurity.com
;; Connection to 2400:cb00:2049:1::adf5:3a92#53(2400:cb00:2049:1::adf5:3a92) for
priviasecurity.com failed: network unreachable.
root@priviasecurity:~#
```

Şekil 3.2.2 'de gösterildiği gibi zone transfer işleminin başarılı veya hatalı olduğu gösterilmektedir. Bir domainin IP adresi var olan kapsam içerisinde var mı yok mu gibi işlemleri öğrenmek için DNS çözümlemesi, traceroute ve ilgili IP adres kayıtları için whois kullanılmaktadır.

Şekil 3.2.3 – Nmap ile Traceroute Kullanımı

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn -T4 --traceroute www.priviasecurity.com

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 06:41 EST
Stats: 0:01:33 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 81.00% done; ETC: 06:43 (0:00:22 remaining)
Nmap scan report for www.priviasecurity.com (104.18.40.10)
Host is up (0.033s latency).

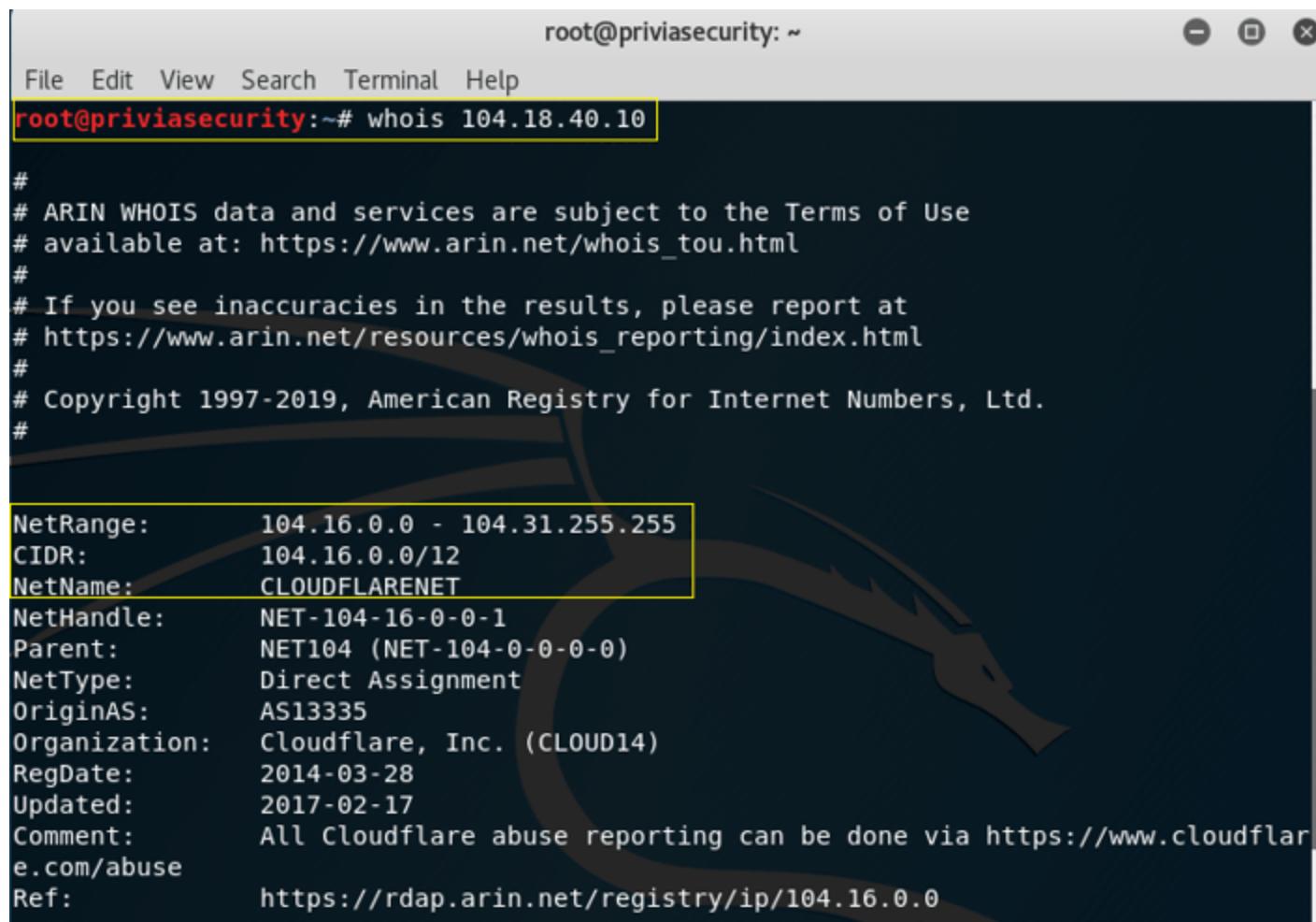
Other addresses for www.priviasecurity.com (not scanned): 104.18.41.10 2606:4700
:30::6812:280a 2606:4700:30::6812:290a
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1  3.40 ms  192.168.16.2
2  35.99 ms 104.18.40.10

Nmap done: 1 IP address (1 host up) scanned in 122.14 seconds
root@priviasecurity:~#
```

Şekil 3.2.3'te gösterildiği gibi hedef domaine yönelik tarama gerçekleştirildiğinde –tracetoute parametresi kullanılarak hedef IP adresine kadarki ara IP adresileri gösterilecektir. Ayrıca bir IP adresini kullanarak bilgi toplama işlemi Şekil 3.2.4'te de gösterilmektedir.

Şekil 3.2.4 – Hedef Hakkında Bilgi Toplama



```

root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# whois 104.18.40.10

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/whois_reporting/index.html
#
# Copyright 1997-2019, American Registry for Internet Numbers, Ltd.
#


NetRange:      104.16.0.0 - 104.31.255.255
CIDR:         104.16.0.0/12
NetName:       CLOUDFLARENET
NetHandle:     NET-104-16-0-0-1
Parent:        NET104 (NET-104-0-0-0-0)
NetType:       Direct Assignment
OriginAS:     AS13335
Organization: Cloudflare, Inc. (CLOUD14)
RegDate:      2014-03-28
Updated:       2017-02-17
Comment:       All Cloudflare abuse reporting can be done via https://www.cloudflare.com/abuse
Ref:          https://rdap.arin.net/registry/ip/104.16.0.0

```

Şekil 3.2.4'te gösterildiği gibi whois ile hedef IP adresi hakkında bilgiler getirmektedir.

## DNS Çözümlemesi

Host keşiflerinde DNS çözümlemesi işleminin kullanılması büyük önem taşımaktadır. Nmap, host keşif problemlerine yanıt veren her IP adresi için DNS çözümlemesi gerçekleştirmektedir. DNS çözümlemesini kontrol etme işleminde 4 parametre kullanılmaktadır. Bu parametreler aşağıdaki gibidir:

**(-n) Parametresi:** Nmap uygulamasının bulduğu IP adreslerine yönelik Reverse DNS çözümlemesi yapmamasını sağlamaktadır. Bu parameter genellikle tarama süresini azaltmaktadır.

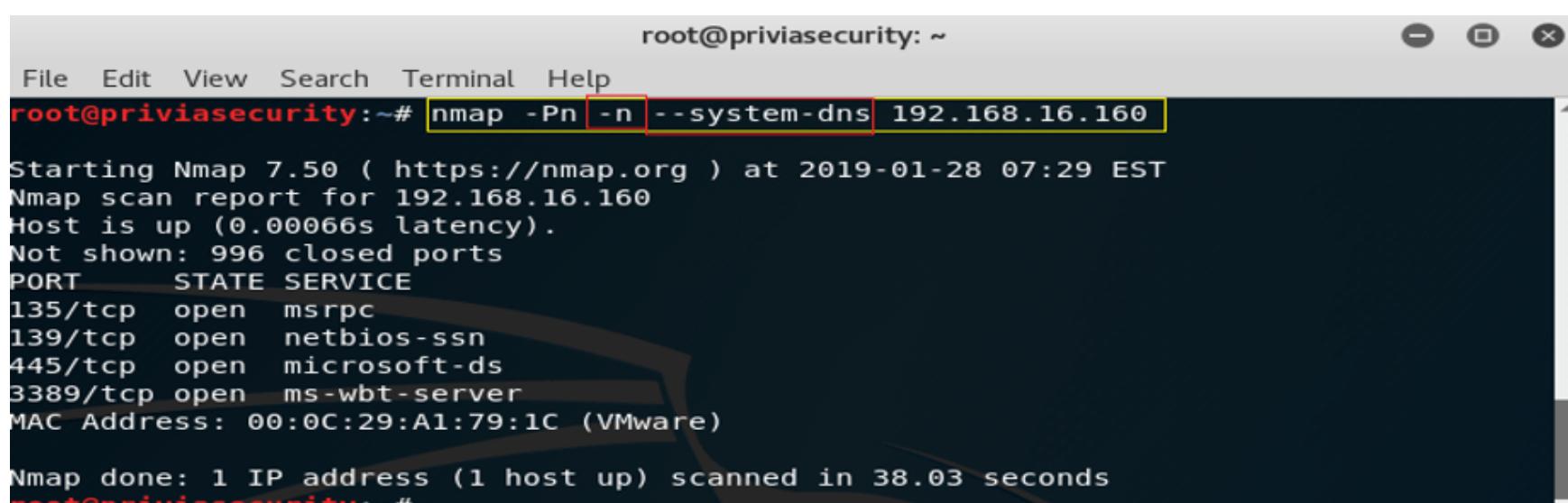
**(-R) Parametresi:** Nmap uygulamasının elde ettiği bütün IP adreslerine yönelik Reverse DNS çözümlemesi yapmasını sağlamaktadır. Varsayılan olarak Reverse DNS çözümlemesi yalnızca açık hostlara karşı gerçekleştirilmektedir.

**(-system-dns) Parametresi:** Nmap uygulaması, varsayılan olarak makinemizde yapılandırılmış name server'lara soru gönderip yanıtları dinleyerek IP adreslerini çözümlemektedir. Performansı artırmak için birçok istek parallel olarak yapılmaktadır. Bunun yerine ise bu parameter kullanılmaktadır. –system-dns parametresi IPv6 için kullanılmaktadır.

**(-dns-server) Parametresi:** Nmap uygulaması, varsayılan olarak DNS sunucuları resolv.conf(Unix) dosyasından veya registry(Win32)'den belirtmektedir. Birden çok DNS sunucusu kullanıldığından daha hızlıdır. İstekler internetteki özyinelemeli DNS sunucusundan hemen hemen ayrılabilceğinin gizliliği de artırmaktadır.

Şekil 3.3'te DNS çözümlemesine yönelik uygulanmıştır.

Şekil 3.3 – Nmap ile –system-dns Parametresinin Kullanılması



```

root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn -n --system-dns 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 07:29 EST
Nmap scan report for 192.168.16.160
Host is up (0.00066s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 38.03 seconds
root@priviasecurity:~#

```

Şekil 3.3'te gösterildiği gibi DNS çözümleme işlemi gerçekleştirılmıştır. Yukarıda belirtilen parametreler kullanılarak sonuçlar elde edilmiştir.

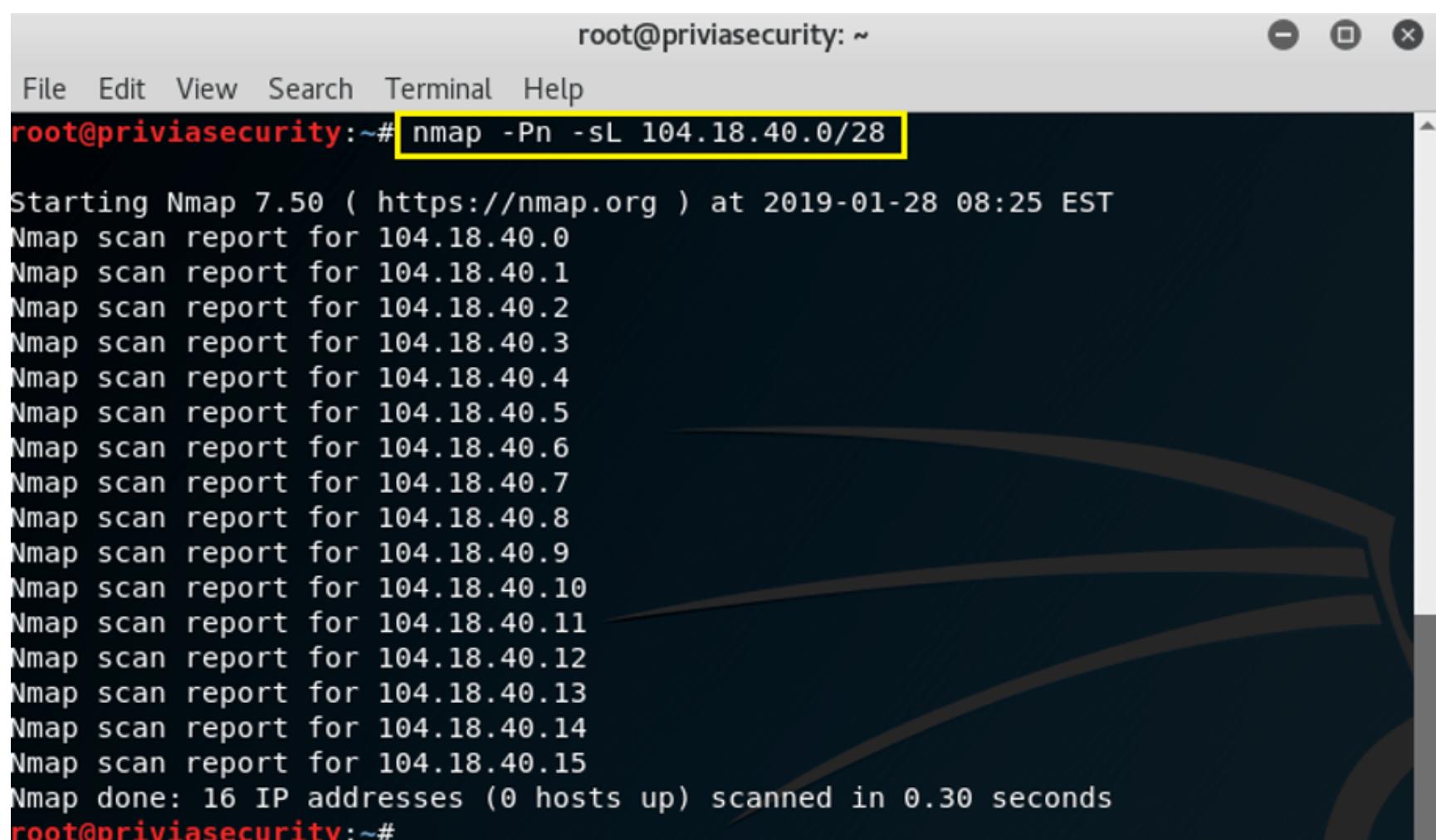
## Host Keşif Kontrolleri

Host keşif kontrollerinde kullanılan parametreler sonucunda, hedeflerin açık/kapalı olma durumu tespit edilebilir. Makinelere gönderilen proların yanıtlarının kontrol edilmesi gerekmektedir.

### Liste Taraması (-sL)

Hedef IP adreslerinin kontrolünü sağlamak amacıyla kullanılır. Hedef makinelere herhangi bir paket gönderilmeden belirtilen ağ üzerindeki hostların listelenmesini sağlayan bir host keşif şeklidir.

Şekil 3.4.1 – Nmap ile Liste Taramasının Gerçekleştirilmesi



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn -sL 104.18.40.0/28

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 08:25 EST
Nmap scan report for 104.18.40.0
Nmap scan report for 104.18.40.1
Nmap scan report for 104.18.40.2
Nmap scan report for 104.18.40.3
Nmap scan report for 104.18.40.4
Nmap scan report for 104.18.40.5
Nmap scan report for 104.18.40.6
Nmap scan report for 104.18.40.7
Nmap scan report for 104.18.40.8
Nmap scan report for 104.18.40.9
Nmap scan report for 104.18.40.10
Nmap scan report for 104.18.40.11
Nmap scan report for 104.18.40.12
Nmap scan report for 104.18.40.13
Nmap scan report for 104.18.40.14
Nmap scan report for 104.18.40.15
Nmap done: 16 IP addresses (0 hosts up) scanned in 0.30 seconds
root@priviasecurity:~#
```

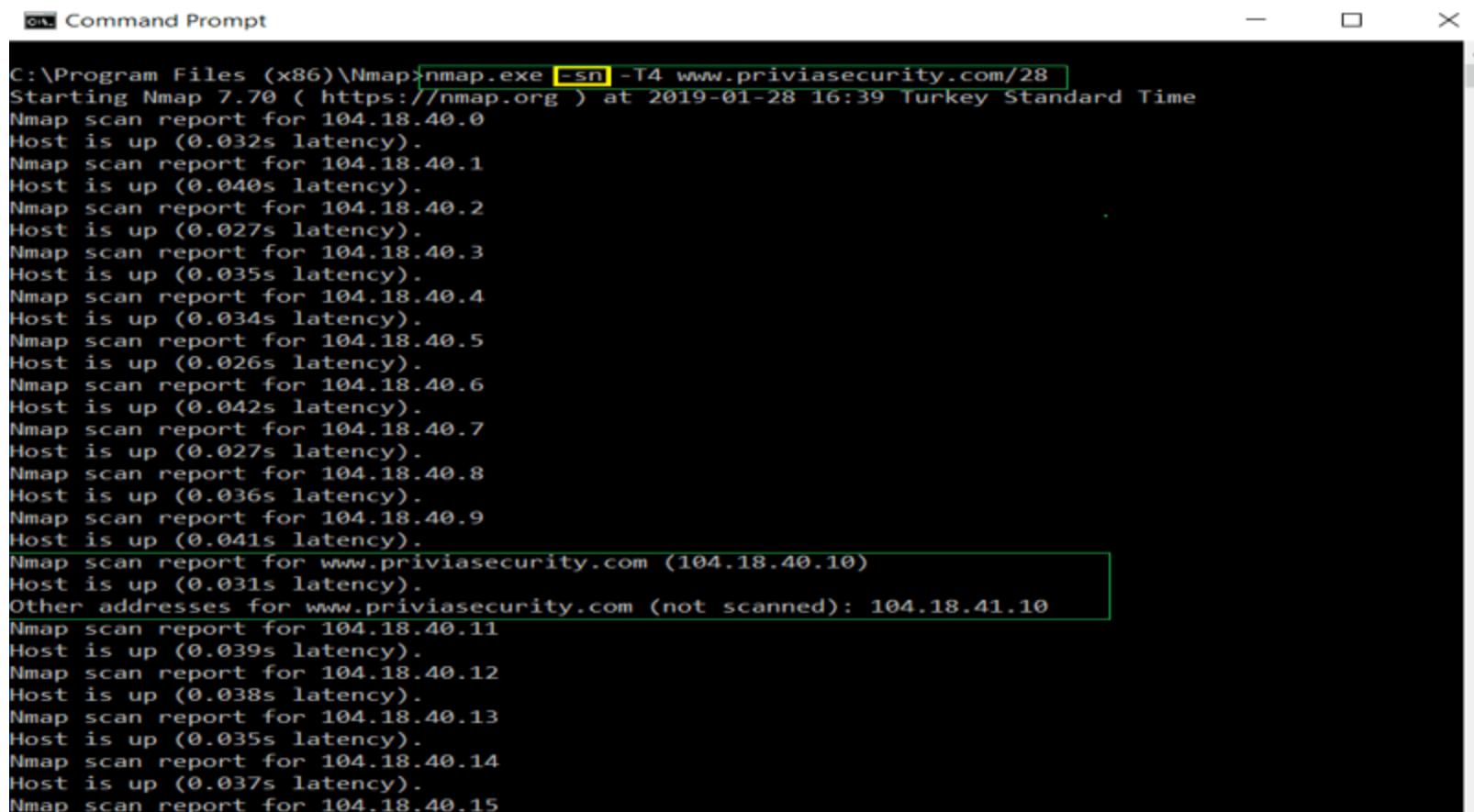
Şekil 3.4.1'de gösterildiği gibi –sL parametresi ile liste taraması gerçekleştirilmektedir. Ayrıca –Pn parametresi kullanılarak ping tarama yapıp taramadaki işlevselligin devam etmesi sağlanılacaktır.

Bir ön liste taraması, hangi hedeflerin tarandığını doğrulamaya yardımcı olmaktadır. Gelişmiş bir liste taramasının nedenlerinden biri gizliliktir. Bazı durumlar IDS sistemlerin tetiklenmesine neden olmaktadır. Liste taraması bu tür tetiklenmelere sebep vermeden hangi makinelerin hedef makine olacağı konusunda bilgi sağlamaktadır. Hedeflerin Reverse DNS çözümleme isteklerini fark etmeleri durumunda –dns-server parametresini kullanarak isimsiz özyinelemeli DNS sunucuları arasında geçiş yapılmaktadır.

### Port Taramasını Devre Dışı Bırakmak (-sn)

Nmap, bir ağ üzerinde aktif hostların hızlı bir şekilde tespit edilmesi için –sn parametresini kullanır. Tespit edilen hostların IP adresleri belirtilmektedir. Bu işleme “ping scan” denir. Port taraması gerçekleştirmeden Nmap uygulamasının içerisindeki scriptlerden ve traceroute probrarından faydalılmaktadır. Ping Scan, liste taramasına göre daha aktif bir tarama türüdür. Bu tarama türü ile hedeflerin IP adresleri ve hostname bilgileri elde edilir. Şekil 3.4.2'de Nmap ile ping taraması gösterilmektedir.

Şekil 3.4.2 – Nmap Uygulaması ile Ping Scan İşlemi



```
C:\Program Files (x86)\Nmap>nmap.exe -sn -T4 www.priviasecurity.com/28
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-28 16:39 Turkey Standard Time
Nmap scan report for 104.18.40.0
Host is up (0.032s latency).
Nmap scan report for 104.18.40.1
Host is up (0.040s latency).
Nmap scan report for 104.18.40.2
Host is up (0.027s latency).
Nmap scan report for 104.18.40.3
Host is up (0.035s latency).
Nmap scan report for 104.18.40.4
Host is up (0.034s latency).
Nmap scan report for 104.18.40.5
Host is up (0.026s latency).
Nmap scan report for 104.18.40.6
Host is up (0.042s latency).
Nmap scan report for 104.18.40.7
Host is up (0.027s latency).
Nmap scan report for 104.18.40.8
Host is up (0.036s latency).
Nmap scan report for 104.18.40.9
Host is up (0.041s latency).
Nmap scan report for www.priviasecurity.com (104.18.40.10)
Host is up (0.031s latency).
Other addresses for www.priviasecurity.com (not scanned): 104.18.41.10
Nmap scan report for 104.18.40.11
Host is up (0.039s latency).
Nmap scan report for 104.18.40.12
Host is up (0.038s latency).
Nmap scan report for 104.18.40.13
Host is up (0.035s latency).
Nmap scan report for 104.18.40.14
Host is up (0.037s latency).
Nmap scan report for 104.18.40.15
```

Şekil 3.4.2'de –sn parametresi kullanılarak ping taraması gerçekleştirilmiştir. Ekran görüntüsünde görüldüğü gibi port taraması yapılmamıştır.

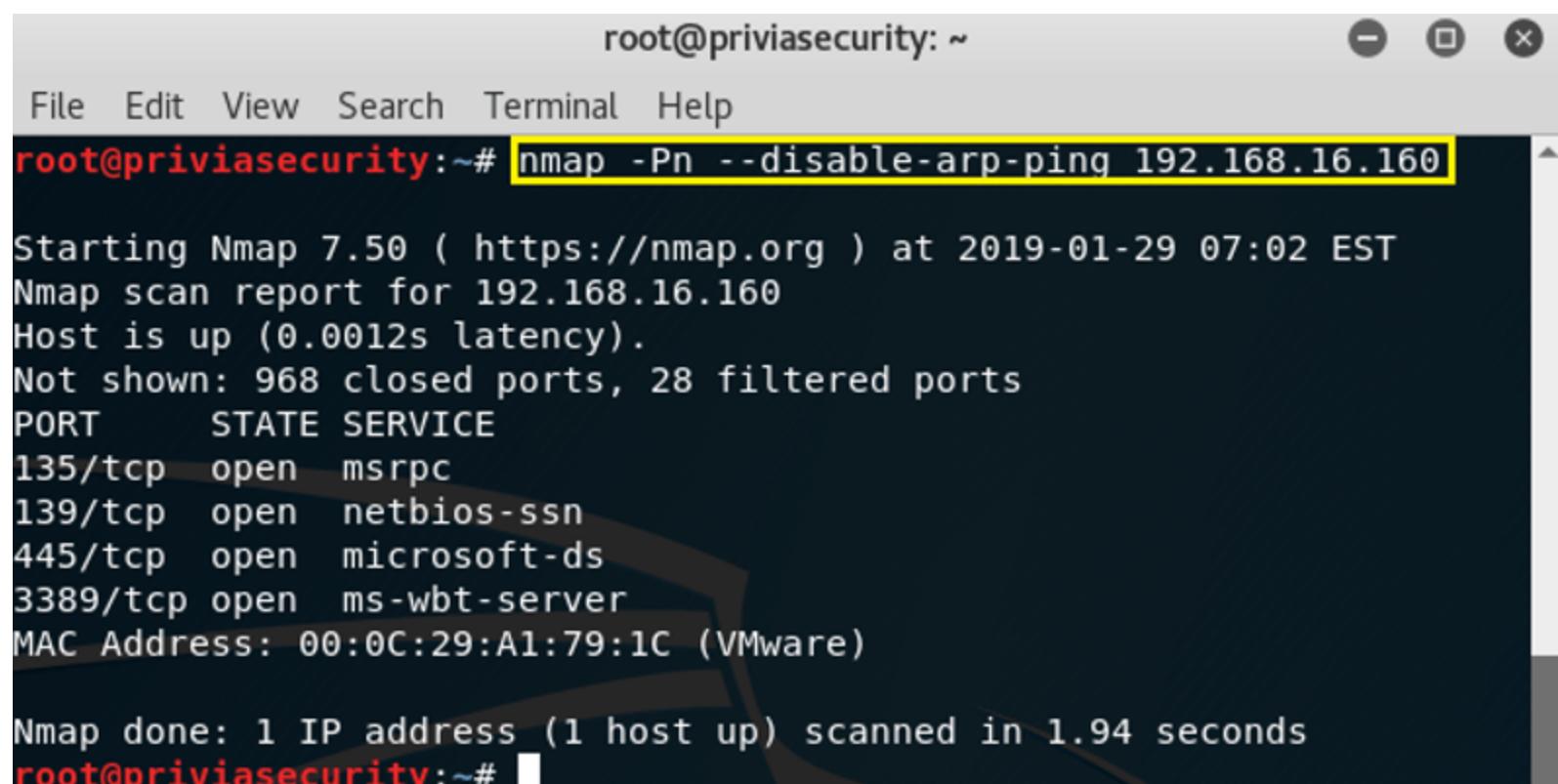
## Ping Devre Dışı Bırakmak (-Pn)

Nmap uygulaması ile pingsiz tarama gerçekleştirilmesi, host keşfinin yapılması istenmemesi anlamına gelmektedir. Bir ağdaki bütün makineleri sırasıyla diğer işlemelere tabi tutulmaktadır. Host keşfi atlanılmaktadır. Bir ağda verilen IP adresleri üzerinde host keşfi yapıldığında pingsiz taramaya göre zaman kaybı meydana gelecektir. Ayrıca nmap ile –Pn parametresi kullanıldığından pingsiz tarama işlemleri gerçekleştirilmektedir. Şekil 3.4.4'te gösterilmiştir.

### Bazı Parametreler

**(–disable-arp-ping) Parametresi:** Genellikle host keşfinde ARP paketleri gönderip alınan yanıtlar doğrultusunda hostun aktif olup olmadığı tespit edilmektedir. Bu seçenek, bir yönlendiricinin bütün ARP isteklerine özel olarak yanıt verdiği ve hedefin ARP taraması yapılmış gibi görünmesini sağlayan ağlarda kullanılmaktadır. Varsayılan ARP taramasını devre dışı bırakmaktadır. Şekil 3.4.4'te gösterilmektedir.

Şekil 3.4.4 – Nmap ile ARP ve ND Ping Taramasını Pasif Tutarak Tarama



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn --disable-arp-ping 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-29 07:02 EST
Nmap scan report for 192.168.16.160
Host is up (0.0012s latency).

Not shown: 968 closed ports, 28 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.94 seconds
root@priviasecurity:~#
```

**(–resolve-all) Parametresi:** Bir hostname hedefi birden fazla adrese çözümlenirse, hepsi taramaktadır. Varsayılan olan, yalnızca ilk çözülen adresi taramaktır.

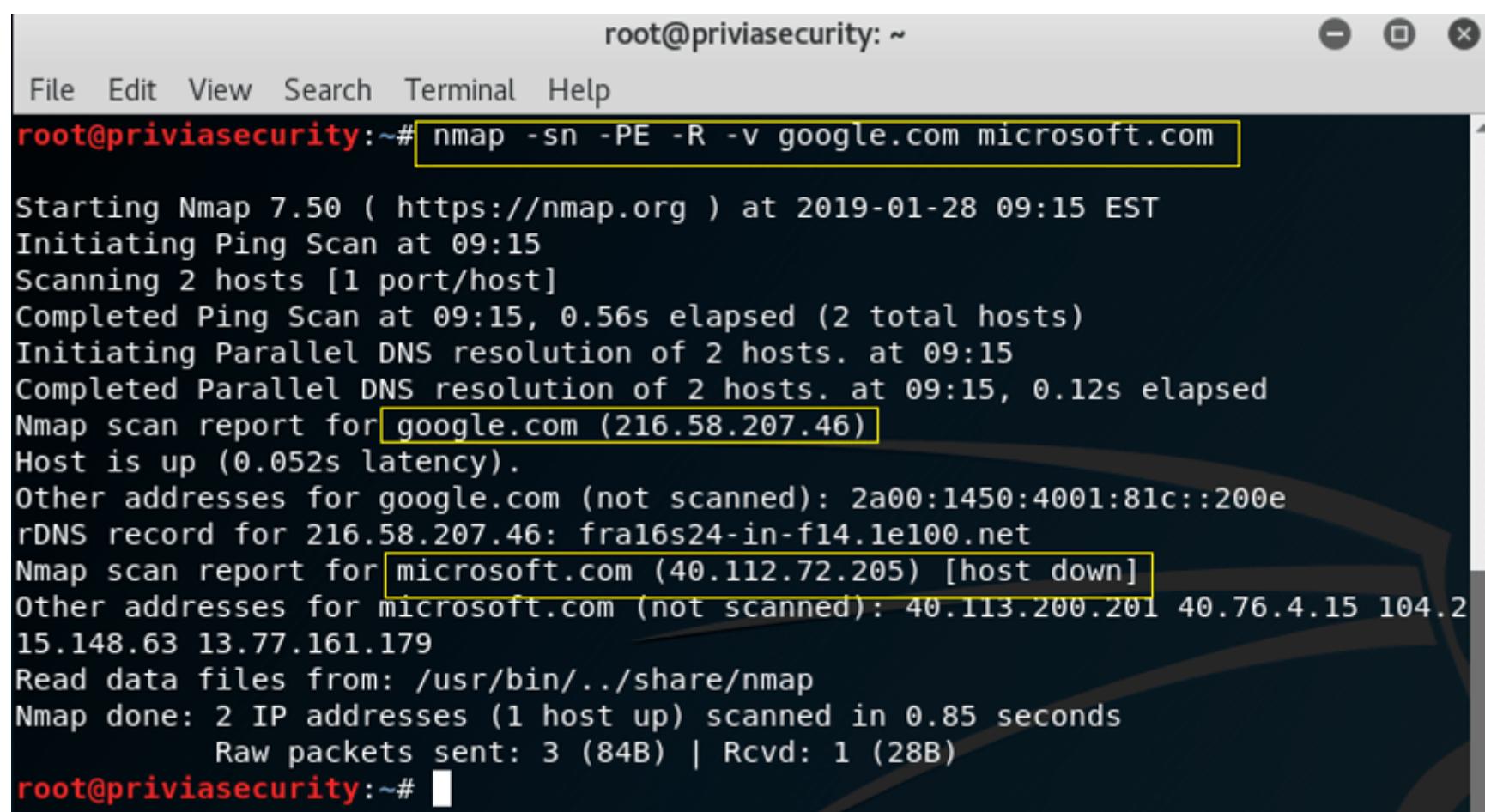
**(–traceroute) Parametresi:** Hedefe ulaşması en uygun portu ve protokolü belirlemek için tarama sonuçlarından gelen bilgileri kullanarak tarama sonrasında gerçekleştirilmektedir. Bağlantı taramaları (-sT) ve boşta taramalar (-sI) dışındaki

bütün tarama türleriyle çalışmaktadır. Traceroute, ICMP zamanını aşmak için tarayıcı ve hedef host arasındaki ara atlama noktalarından aşılmış mesajları almak için düşük TTL (yaşam süresi) sürüme sahip paketler göndererek çalışmaktadır. Standart traceroute uygulamaları 1 TTL ile başlayıp hedef hosta ulaşana kadar artırmaktadır. Bu TTL işlemleri, Nmap uygulaması üzerinde geriye doğru yapıldığında sürecin hızlandırılması için akıllı önbellek algoritması kullanılmıştır.

## Host Keşif Teknikleri

Genellikle bir ū üzerinde bulunan makinelerin aktif olup olmadığını tespit edilmek açısıyla makinelere ICMP echo isteği gönderilmektedir. Daha sonra yapılan istek sonucunda bir yanıt alınmaktadır. Alınan yanıt sonucunda makinenin aktif veya pasif olduğu tespit edilmektedir. Güvenlik duvarları bu istekleri nadiren engellemektedir. Bundan dolayı host keşif çalışmaları için kullanılan bir tekniktir. Şekil 3.5'de –sn –PE parametreleri ICMP ping taramasını belirtmektedir. –R parametresi ise tüm makinelere yönelik reverse DNS çözümlemesi yapmasını istemektedir.

Şekil 3.5 – Nmap Host Keşif Teknikleri



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -sn -PE -R -v google.com microsoft.com

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 09:15 EST
Initiating Ping Scan at 09:15
Scanning 2 hosts [1 port/host]
Completed Ping Scan at 09:15, 0.56s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 09:15
Completed Parallel DNS resolution of 2 hosts. at 09:15, 0.12s elapsed
Nmap scan report for google.com (216.58.207.46)
Host is up (0.052s latency).
Other addresses for google.com (not scanned): 2a00:1450:4001:81c::200e
rDNS record for 216.58.207.46: fra16s24-in-f14.1e100.net
Nmap scan report for microsoft.com (40.112.72.205) [host down]
Other addresses for microsoft.com (not scanned): 40.113.200.201 40.76.4.15 104.2
15.148.63 13.77.161.179
Read data files from: /usr/bin/../share/nmap
Nmap done: 2 IP addresses (1 host up) scanned in 0.85 seconds
    Raw packets sent: 3 (84B) | Rcvd: 1 (28B)
root@priviasecurity:~#
```

### TCP SYN Ping

- PS parametresi kullanılarak, SYN bayraklı boş bir TCP paketi gönderilmektedir. Varsayılan olarak 80. port hedef alınmaktadır. Bu bayrak uzak bir sistem ile bağlantı kurulmak istendiğini göstermektedir. Port açık olursa SYN/ACK paketiyle yanıt verilecektir. Üç el sıkışma tamamlayıp bir ACK paketi yerine RST paketini göndererek bağlantıyi düşürecektir. Alınan RST ve SYN/ACK yanıtları makinenin açık olduğunu belirtmektedir.

Şekil 3.5.1 – TCP SYN probu ile host keşfi

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -sn -PS80 -R -v microsoft.com google.com

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 09:55 EST
Initiating Ping Scan at 09:55
Scanning 2 hosts [1 port/host]
Completed Ping Scan at 09:55, 0.42s elapsed (2 total hosts)
Initiating Parallel DNS resolution of 2 hosts. at 09:55
Completed Parallel DNS resolution of 2 hosts. at 09:55, 0.24s elapsed
Nmap scan report for microsoft.com (104.215.148.63)
Host is up (0.29s latency).
Other addresses for microsoft.com (not scanned): 40.112.72.205 40.76.4.15 13.77.
161.179 40.113.200.201
Nmap scan report for google.com (172.217.23.142)
Host is up (0.094s latency).
Other addresses for google.com (not scanned): 2a00:1450:4001:819::200e
rDNS record for 172.217.23.142: fra16s18-in-f14.1e100.net
Read data files from: /usr/bin/../share/nmap
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.83 seconds
  Raw packets sent: 2 (88B) | Rcvd: 2 (88B)
root@priviasecurity:~#
```

## TCP ACK Ping

- PA parametresi kullanılarak gerçekleştirilen bir host keşif tekniğidir. SYN ping'e benzemektedir. Tek fark bayrakların değişik olmasıdır. Hedef sisteme ACK bayraklı TCP paketi gönderilir. Eğer hedef sistem açıksa RST paketi ile yanıt verir. 80. port hedef alınarak yapılmaktadır. –PS parametresi ile yapılan taramalar engellendiğinde kullanılmaktadır.

Şekil 3.5.2 – Nmap ile TCP ACK Ping tekniğinin kullanımı

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -sn -PA microsoft.com

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 10:56 EST
Nmap scan report for microsoft.com (104.215.148.63)
Host is up (0.00065s latency).
Other addresses for microsoft.com (not scanned): 13.77.161.179 40.112.72.205 40.
113.200.201 40.76.4.15
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@priviasecurity:~#
```

## UDP Ping

UDP paketleri kullanılarak sistemlerin aktif olup olmadığı tespit edilir. –PU parametresi kullanılarak gerçekleştirilmektedir. –PS ve –PA parametreleri ile aynı formattadır. Varsayılan olak 40. Ve 125. Portlar kullanılmaktadır. Genellikle gönderilen paketler boştur. Fakat 53. Ve 161. Portlar genel bağlantı noktaları olduğu için özel payload gönderilmektedir. –data-length parametresi, tüm portlar için ratsgele payload göndermektedir. Bu tarama türünün en önemli avantajı güvenlik duvarını atlatması ve TCP portlarını tarayan filtreleri olmasıdır.

## ICMP Ping Türleri

Nmap, host keşiflerinde ICMP paketlerini kullanır. Hedef hostlara ICMP type 8 (Echo isteği) gönderip ICMP type 0(Echo yanıtı) beklemektedir. Fakat birçok güvenlik duvarı bu isteği engellemektedir. -PE parametresi kullanılarak ICMP echo isteği gerçekleştiriliyor. Bu işlem ICMP ping sorusu olarak bilinmektedir. Ayrıca açık hostların keşfi zaman damgası ve adres damgası üzerinden de tespit edilebilmektedir. Bu işlemler –PP ve –PM parametreleri kullanılarak gerçekleştiriliyor.

Şekil 3.5.4 – ICMP Ping Türleri ile Tarama Gerçekleştirilmesi

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -PP -PE -PM 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 16:25 EST
Nmap scan report for 192.168.16.160
Host is up (0.0016s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.88 seconds
root@priviasecurity:~#
```

## IP Protocol Ping

IP paketlerinin içerisindeki IP başlığında belirtilen protokol numarası ile yapılan bir tarama türüdür. Herhangi bir protokol belirtilmediği zaman ICMP, IGMP, IP-inIP protokoller için birden fazla IP paketi gönderilmektedir. Bu yöntemde kullanılan prob ile aynı protokolü kullanan yanıtlar üzerinde veya hedef hosta yönelik erişilemediğini belirten ICMP paketlerine bakılarak bir makinenin çalışıp çalışılmadığı tespit edilmektedir.

## ARP Ping

En yaygın kullanılan taramalardan biridir. Bu tarama işlemi `-PR` parametresi kullanılarak gerçekleştirilir. Bu tarama ham bir IP paketi gönderilerek gerçekleştirilmektedir. Böylece hedef IP adresine karşılık gelen makinenin fiziksel adresi tespit edilir.

Şekil 3.5.6 – Çevrimdışı hedefe yönelik IP Ping Taraması ve ARP Ping Taraması

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -n -sn --send-ip 192.168.16.161
Ham IP Ping Scan

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 16:41 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
root@priviasecurity:~# nmap -n -sn -PR --packet-trace --send-eth 192.168.16.161
ARP Ping Scan

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-28 16:41 EST
SENT (0.0331s) ARP who-has 192.168.16.161 tell 192.168.16.163
SENT (0.2345s) ARP who-has 192.168.16.161 tell 192.168.16.163
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 0.47 seconds
root@priviasecurity:~#
```

Şekil 3.5.6'da gösterildiği gibi tarama örnekleri gerçekleştirılmıştır. Bu tarama örneğinin ilkinde `-send-ip` parametresi kullanılmasıyla, yerel ağ olmasına rağmen IP seviyesinde paketler gönderilmektedir. İlk örnek 3.09 saniye sürmüştür. Yalnızca bir hedefe yönelik yapılan bir tarama olduğu için taramanın sonuçlanması kısa sürmüştür. Fakat kurumsal bir yerel ağdaki makine sayısının fazlalığı bu süreyi artırmaktadır. İşletim sistemi hosttan vazgeçmediği için bir saniye arayla üç ARP isteği göndermektedir. İkinci örnekte ise ARP taraması 0.47 saniyede gerçekleştirılmıştır. Ağ yöneticileri normal şartlarda ping paketlerini engellemektedir. Fakat ARP istekleri veya yanıtları genellikle engellenmemektedir. Ayrıca bu taramalar gerçekleştirildiğinde `-spoof-mac` parametresini kullanılarak tarama yapan makinenin MAC adresi gizlenebilmektedir.

## SCTP INIT Ping

Bu tarama türü `-PY` kullanılarak gerçekleştirilmektedir. Bu parametre kullanılarak içerisinde INIT öbeği bulunan bit SCTP paketi gönderilmektedir. Varsayılan olarak 80. portu hedef almaktadır. Örnek olarak `-PY22,80` gibi bir parametre ile 22. ve 80. portlar ile bağlantı kurulacaktır. Portlar açık ise INIT-ACK yanıtı dönmektedir. Nmap, bu yanıta işlevsel bir SCTP

paketi göndermek yerine ABORT yanıtını vererek bağlantıyi bitirmektedir. Böylece bu iki yanıt ile hedef makine üzerindeki portların açık olduğu tespit edilmektedir.

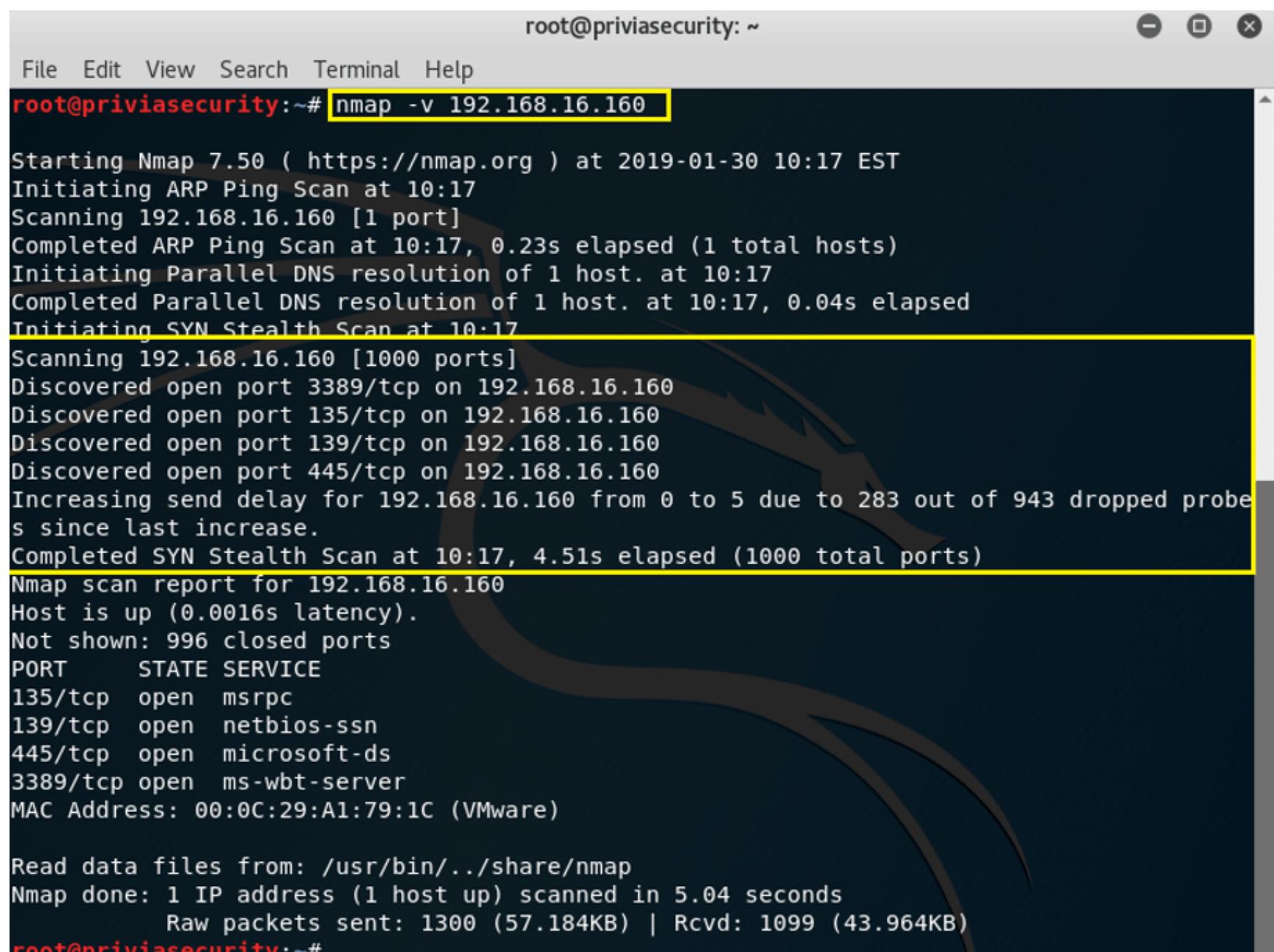
## Host Keşif Stratejileri

Nmap aracı, host keşiflerini daha iyi şekilde tespitinin sağlanması için belirli parametreleri kullanmaktadır. Bu parametreler host keşiflerinde kullanıcının yapmak istediği tarama türlerine göre kullanılmaktadır. Bu parametreler aşağıda belirtilmiştir.

### (-v|-verbose) Parametresi

Nmap aracında bulunan bu parametre, tarama sonucunda gelen çıktıının ayrıntılı bir şekilde gelmesini sağlamaktadır. Bu doğrultuda host hakkında ek bilgiler verilmektedir.

Şekil 3.6.1 – Verbose Parametresinin Kullanımı



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -v 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-30 10:17 EST
Initiating ARP Ping Scan at 10:17
Scanning 192.168.16.160 [1 port]
Completed ARP Ping Scan at 10:17, 0.23s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:17
Completed Parallel DNS resolution of 1 host. at 10:17, 0.04s elapsed
Initiating SYN Stealth Scan at 10:17
Scanning 192.168.16.160 [1000 ports]
Discovered open port 3389/tcp on 192.168.16.160
Discovered open port 135/tcp on 192.168.16.160
Discovered open port 139/tcp on 192.168.16.160
Discovered open port 445/tcp on 192.168.16.160
Increasing send delay for 192.168.16.160 from 0 to 5 due to 283 out of 943 dropped probes since last increase.
Completed SYN Stealth Scan at 10:17, 4.51s elapsed (1000 total ports)
Nmap scan report for 192.168.16.160
Host is up (0.0016s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
    Raw packets sent: 1300 (57.184KB) | Rcvd: 1099 (43.964KB)
root@priviasecurity:~#
```

### (-source-port <port no>) Parametresi

Firewall yöneticileri, DNS ve FTP portlarını açık tutmak için firewall üzerinden özel kurallar oluşturmaktadır. Fakat firewall bypass işlemlerinden biri de source port manipülasyon işlemidir.

### (-data-length <length>) Parametresi

Bu parametre ile her pakete rastgele olarak veri eklenmektedir. Ayrıca TCP, UDP ve ICMP gibi tarama türleriyle birlikte kullanılabilmektedir. Birçok IDS sistemini atlatmak için kullanılan yöntemlerden biridir. Örneğin, data değeri 56 olan bir echo istek paketine rastgele olarak 32 değeri atanırsa, IDS sistemi paketin bir Windows işletim sistemine sahip bir makineden geldiğini işaretler. Fakat gelen istek paketindeki gerçek data değerinin 56 olması isteğin bir Linux işletim sistemine sahip makineden geldiğini gösterebilir.

Şekil 3.6.3 – (-data-length) Parametresinin Kullanımı

```
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -PS135 --data-length 32 192.168.16.0/24

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-30 10:27 EST
Stats: 0:02:04 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 75.71% done; ETC: 10:29 (0:00:39 remaining)
Stats: 0:04:26 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 95.64% done; ETC: 10:31 (0:00:12 remaining)
Stats: 0:06:40 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.61% done; ETC: 10:33 (0:00:06 remaining)
Stats: 0:06:42 elapsed; 251 hosts completed (4 up), 4 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 98.66% done; ETC: 10:33 (0:00:05 remaining)
Nmap scan report for 192.168.16.1
Host is up (0.00030s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
902/tcp   open  iss-realsecure
912/tcp   open  apex-mesh
MAC Address: 00:50:56:C0:00:08 (VMware)

Nmap scan report for 192.168.16.2
Host is up (0.00030s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    filtered domain
MAC Address: 00:50:56:FD:9E:49 (VMware)

Nmap scan report for 192.168.16.160
Host is up (0.00039s latency).
Not shown: 980 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
787/tcp   filtered qsc
1089/tcp  filtered ff-annunc
```

#### (-ttl <value>) Parametresi

Giden TTL değerinin ayarlanması, IPv4 düzeyindeki ping taramalarında kullanılmaktadır. Yapılan taramanın yerel ağ sınırları içerisinde yapılmasını sağlamayı hedeflemektedir. Giden -ttl değeri azaltılarak, herhangi bir döngü ile karşılaşıldığında yönlendirici CPU'sunun işlem yükünün azaltılması hedeflenmektedir.

Şekil 3.6.4 – TTL Parametresinin Kullanımı

```
root@priviasecurity:~#
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn --reason --ttl 128 192.168.16.160

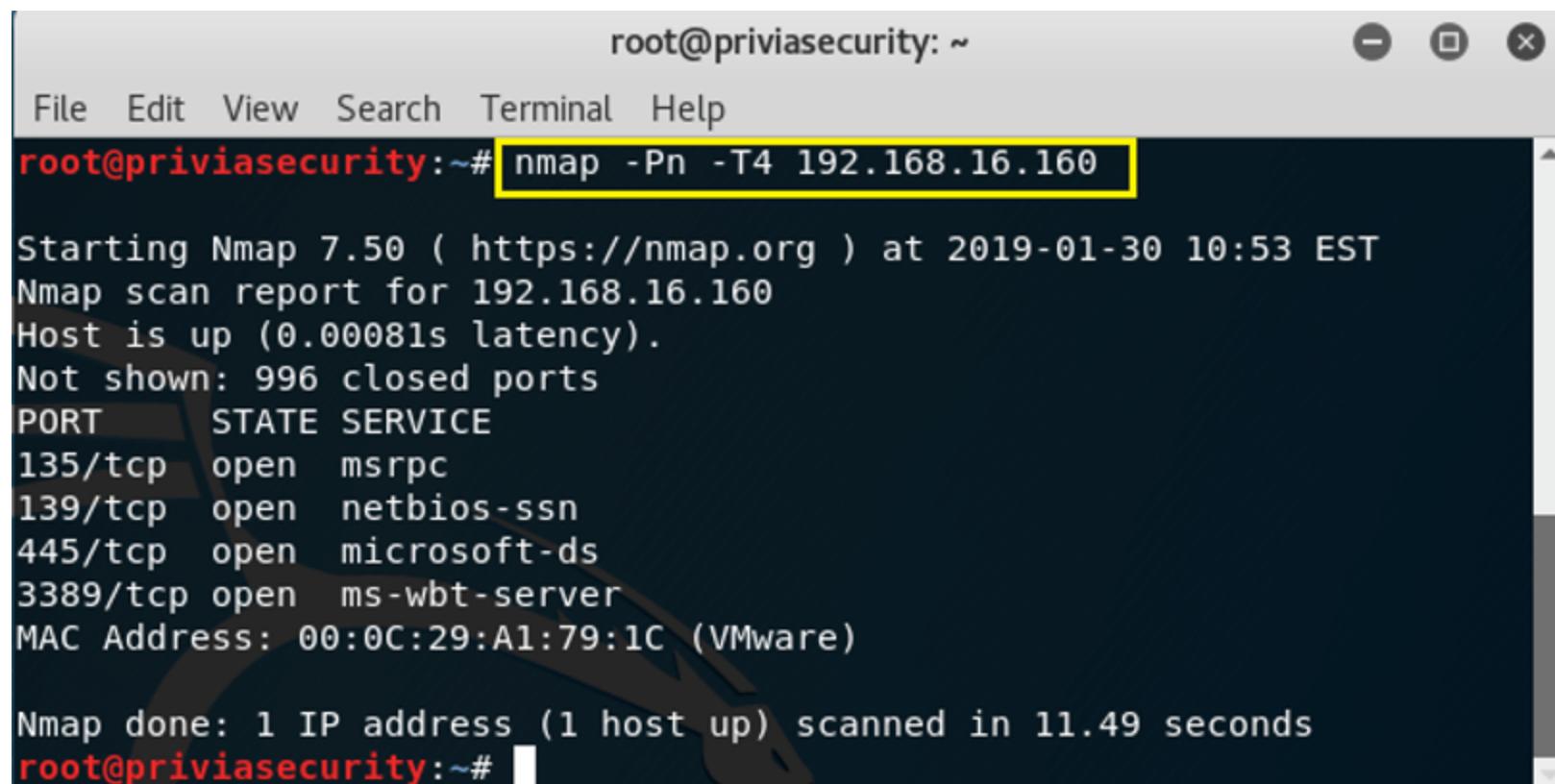
Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-30 10:40 EST
Nmap scan report for 192.168.16.160
Host is up, received arp-response (0.00065s latency).
Not shown: 996 closed ports
Reason: 996 resets
PORT      STATE SERVICE      REASON
135/tcp   open  msrpc        syn-ack ttl 128
139/tcp   open  netbios-ssn   syn-ack ttl 128
445/tcp   open  microsoft-ds  syn-ack ttl 128
3389/tcp  open  ms-wbt-server syn-ack ttl 128
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 67.35 seconds
root@priviasecurity:~#
```

#### Hazır Zamanlama Parametreleri

Ping taramasını hızlandırip sonuçların alınmasına yönelik yapılmış bir parametre düzenlemesidir. **-T** parametresi ile kullanılır. Hazır zamanlama şablonları, **paranoid(0)**, **sneaky(1)**, **polite(2)**, **normal(3)**, **aggressive(4)** ve **insane(5)** olarak 6 tanedir.

Şekil 3.6.5 – Zamanlama Parametresinin Kullanılması



```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn -T4 192.168.16.160

Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-30 10:53 EST
Nmap scan report for 192.168.16.160
Host is up (0.00081s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
MAC Address: 00:0C:29:A1:79:1C (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.49 seconds
root@priviasecurity:~#
```

#### (-max/min-parallelism <value>) Parametreleri

Yapılan taramalarda taranacak makinelerin paralel bir şekilde taramasını sağlamak için düzenlenmiş bir parametredir. Parametreyi kullanarak <value> değeri olarak makine sayısı belirtilmektedir.

#### (-min/max/initial-rtt-timeout <time>) Parametreleri

Bu parametreler, Nmap aracının yaptığı istek sonucunda gelecek yanıt paketinin ne kadar bekleyeceğini kontrol etmektedir.

### Çıktı Parametreleri

- **-oA**, **-oN**, **-oG**, **-oX** vb. parametrelerden oluşur. Örneğin, **-oX** parametresinin kullanılması ile Nmap çıktıları XML formatında oluşturulur.

#### (-randomize-hosts) Parametresi

Ağda bir tarama yapılırken, **-randomize-hosts** parametresinin kullanılması taramayı belirsizleştirir. Bu yöntem IDS ve IPS sistemlerinden kaçınmak için kullanılır. Nmap, varsayılan olarak bir ağdaki makineleri ardışık olarak tarar. Bazı IDS ve IPS sistemleri ise, yapılan taramayı tespit edip engelleyebilir.

#### (-reason) Parametresi

Varsayılan taramalar sonucunda gelen çıktıda hedef portun çalışır durumda olup olmadığını göstermektedir. Bu parametre ile nmap taramasında hedef makinesinin hangi keşif testlerine yanıt verdiği açıklanmaktadır. Nmap çalışma sırasında yanıt paketi olarak bir ICMP echo paketi yanıtı rapor edilebilir. Fakat ikinci bir tarama sonucunda önce bir RST paketi alınabilir ve Nmap aracının bunu bildirmesine neden olabilir. Bundan dolayı detaylı olarak hedef makinenin ne tür yanıtlar verip vermediğini görebilmek için bu parametrenin kullanılması fayda sağlamaktadır.

Şekil 3.6.10 – Reason Parametresinin Kullanılması

```
root@priviasecurity: ~
File Edit View Search Terminal Help
root@priviasecurity:~# nmap -Pn --reason 192.168.16.160
Starting Nmap 7.50 ( https://nmap.org ) at 2019-01-30 10:32 EST
Nmap scan report for 192.168.16.160
Host is up, received arp-response (0.00060s latency).
Not shown: 972 closed ports
Reason: 972 resets
PORT      STATE     SERVICE          REASON
82/tcp    filtered xfer
135/tcp   open      msrpc
139/tcp   open      netbios-ssn
389/tcp   filtered ldap
445/tcp   open      microsoft-ds
497/tcp   filtered retrospect
514/tcp   filtered shell
912/tcp   filtered apex-mesh
1094/tcp  filtered rootd
1287/tcp  filtered routematch
1455/tcp  filtered esl-lm
1658/tcp  filtered sixnetudr
1914/tcp  filtered elm-momentum
2701/tcp  filtered sms-rcinfo
3389/tcp  open      ms-wbt-server
                                syn-ack ttl 128
```

## (-packet-trace) Parametresi

Nmap, `--packet-trace` parametresini kullanarak tarama süresince neler yapıldığını detaylı olarak gösterir. `--packet-trace` parametresi, Sıra numaraları, TTL değerleri ve TCP bayrakları gibi ayrıntılar dâhil olmak üzere, alınan ve gönderilen her paketin gösterilmesini sağlar.

### **(-D <decoy1, decoy2,..>) Parametresi**

Decoy olarak tanımlanan IP adresleri, saldırgan IP adresini gizlemek için kullanılan sahte IP adresleri olarak tanımlanabilir. Resim 3.6.12'deki saldırgan IP adresi, 192.168.16.163'tür. Fakat, -D parametresi ile verilen 192.168.16.138, 192.168.16.2 gibi sahte IP adresleri kullanılarak saldırgan IP ile tarama yapılmıştır. Böylelikle ağı izleyen yetkililerin saldırganı tespit etmesi zorlaşır.

Şekil 3.6.12 – Decoy Parametresinin Kullanımı

The figure shows a Wireshark interface capturing traffic on interface eth0. The packet list shows numerous SYN and SYN-ACK exchanges between various IP addresses, primarily 192.168.16.163 and 192.168.16.160. The terminal window below shows the output of an Nmap scan, indicating that 192.168.16.138, 192.168.16.2, and 192.168.16.160 are up and undergoing an ARP ping scan. The Nmap command used was nmap -Pn -D192.168.16.138,192.168.16.2 192.168.16.160.

No.	Time	Source	Destination	Protocol	Length	Info
135	27.639565114	192.168.16.163	192.168.16.160	TCP	58	55702 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
136	27.639572431	192.168.16.2	192.168.16.160	TCP	58	55702 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
137	27.639580139	192.168.16.138	192.168.16.160	TCP	58	55702 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
138	27.639587857	192.168.16.163	192.168.16.160	TCP	58	55702 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
139	27.639595394	192.168.16.2	192.168.16.160	TCP	58	55702 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
140	27.639602992	192.168.16.138	192.168.16.160	TCP	58	55702 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
141	27.639610474	192.168.16.163	192.168.16.160	TCP	58	55702 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
142	27.639617866	192.168.16.2	192.168.16.160	TCP	58	55702 → 1025 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
143	27.639625439	192.168.16.138	192.168.16.160	TCP	58	55702 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
144	27.639632931	192.168.16.163	192.168.16.160	TCP	58	55702 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
145	27.639641005	192.168.16.2	192.168.16.160	TCP	58	55702 → 139 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

## (-6) Parametresi

Taramalarda ipv4 adresi yerine ipv6 kullanmayı sağlar.

(-S <source IP address>, -e <sending device name>) Parametreleri

Kaynak IP adresini ve gönderen cihazın adını belirterek yapılan tarama türleridir.