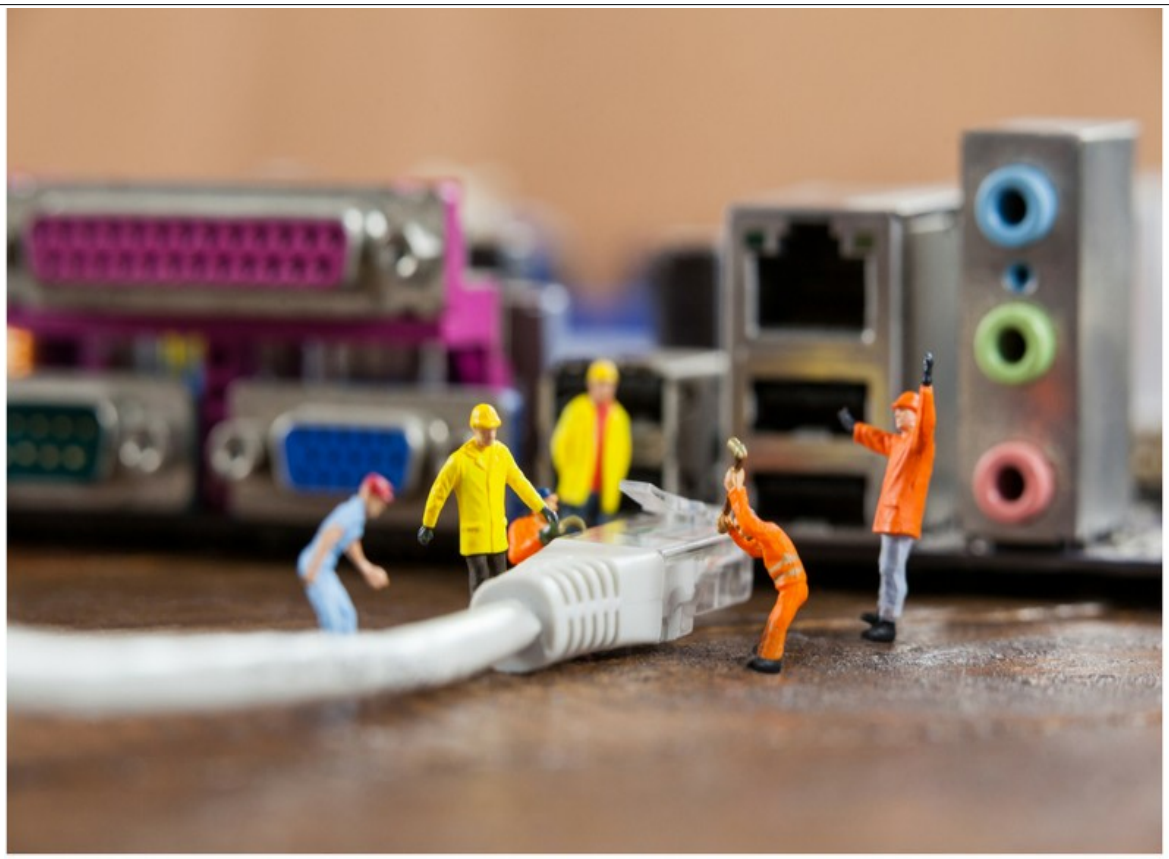


NMAP

KULLANIM REHBERi

CEMAL TANER

İÇİNDEKİLER :

BÖLÜM 1: NMAP KURULUMU

Nmap, GNU Genel Kamu Lisansı altında yayınlanan bir açık kaynak kodlu programdır. TCP / IP sistemlerini keşfetmek, izlemek ve sorun gidermek için kullanılabilen bir araçtır. Nmap, Gordon “Fyodor” Lyon tarafından oluşturulan ve bir gönüllü topluluğu tarafından aktif olarak geliştirilen ücretsiz, çapraz platform bir ağ tarama yardımcı programıdır.
Nmap ile taradığımız ağdaki açık makineleri, makinelerdeki açık portları, çalışan servisleri, işletim sistemi versiyonlarını ve belli başlı zayıflıkları tespit edebiliriz. Bunun dışında ağ haritasının çıkarılması veya ağ envanterinin hazırlanması içinde nmap çok kullanışlı bir araçtır.
Özellikle penetrasyon testi yapanlar Nmap programını çok kullanır. Siz de **network penetrasyon** testleri alanında uzmanlaşmak istiyorsanız **Nmap programının kullanımını** çok iyi bilmelisiniz.

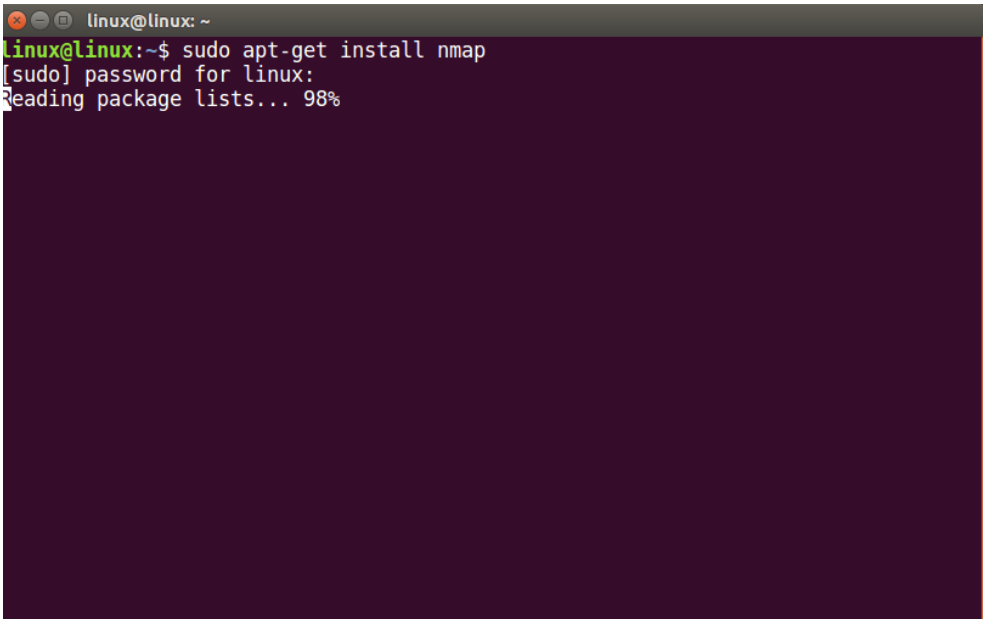
Nmap Kurulumu

Nmap genellikle Linux sistemlerde kullanılsa da Windows ve Mac için de geliştirilen versiyonları vardır. Nmap’ten en iyi verimi almak için şu OS’u kullanmalısınız gibi bir iddiam yok kendiniz farklı platformlarda deneyip görebilirsiniz. Ben bu rehber boyunca **Windows sürümünü** kullanacağım.

Linux’ta Kurulum

Kali, Blackarch, Pento vb. penetrasyon testi için özel hazırlanmış Linux dağıtımlarında Nmap kurulu olarak gelir. Biz burada Ubuntu’da Nmap nasıl kurabiliriz onu göreceğiz. Ubuntu’da paket deposundan Nmap kurulumu için aşağıdaki komutu yazmanız yeterli

$ sudo apt-get install nmap



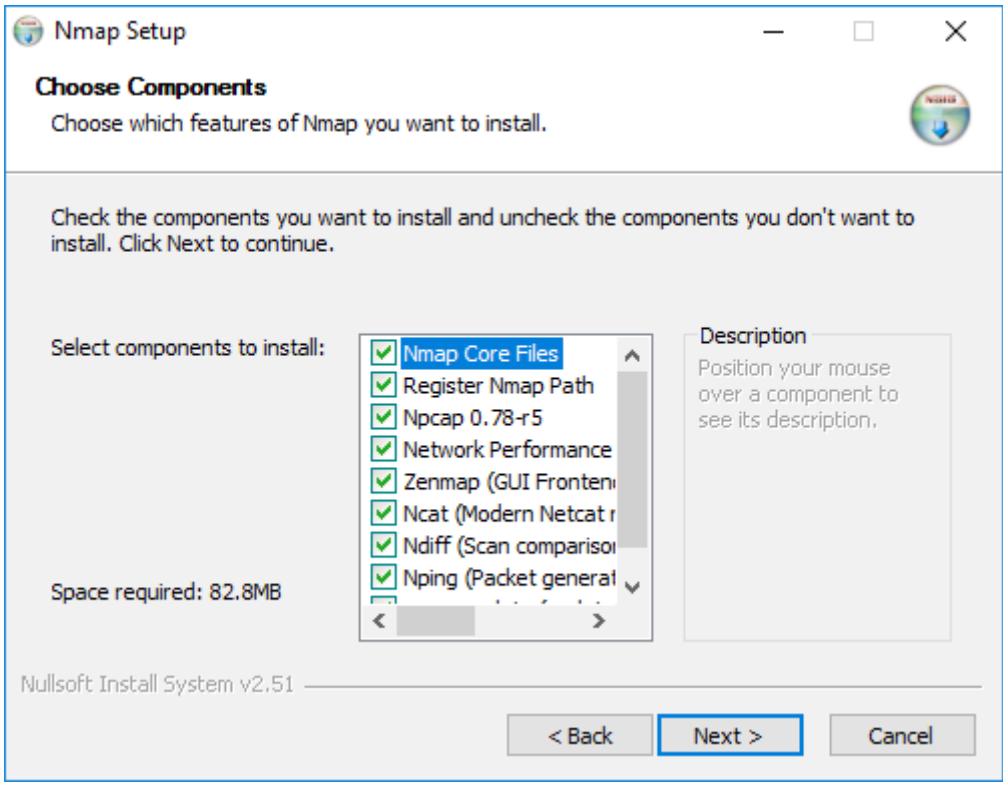
Kurulum bittikten sonra aşağıdaki komutla nmap versiyonunu kontrol edebilirsiniz.

$ nmap -V

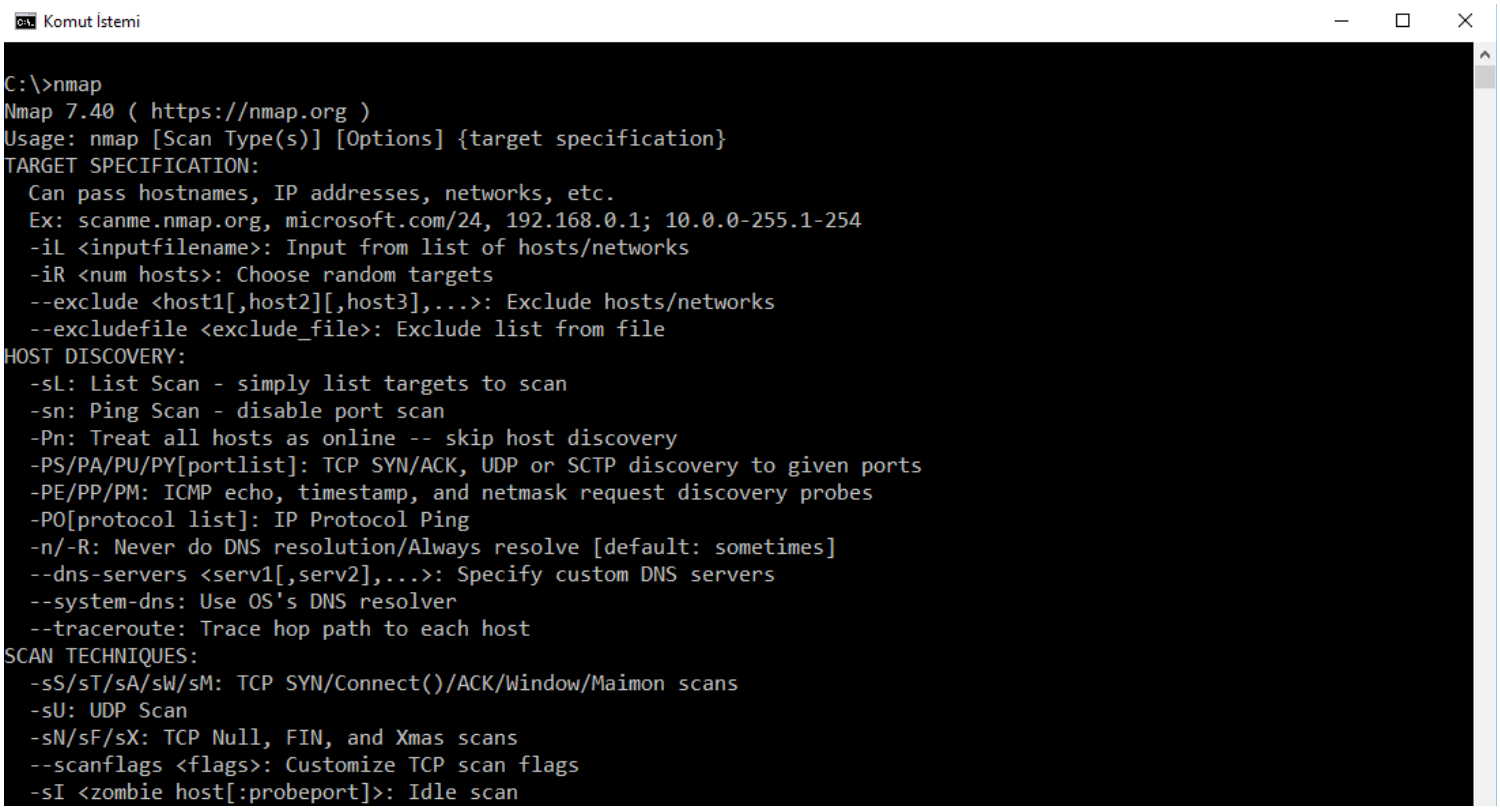
Yukarıda gördüğünüz üzere 7.01 versiyonunu kurmuş olduk.

Windows'ta Kurulum

Windowsta kurulum için öncelikle Nmap sitesinden Windows sürümünü indirmeniz gerekli. Bu adresten gerekli dosyayı indirebilirsiniz.
Klasik bir Windows programı gibi yani Next, Next,Next,Install, End şeklinde kurulumu gerçekleştiriyoruz. Dikkat etmemiz gereke tek şey aşağıdaki resimde gördüğünüz üzere tüm bileşenlerin seçili olmasıdır.



Kurulum bittikten sonra komut satırını açıp **nmap** yazarak kullanmaya başlayabiliriz.



Tabi nmap komutu ile beraber bazı parametreler kullanmamız gerektiği için bize kullanabileceğimiz parametreler listelenmiş oldu.

BÖLÜM 2: TEMEL TARAMA TEKNİKLERİ

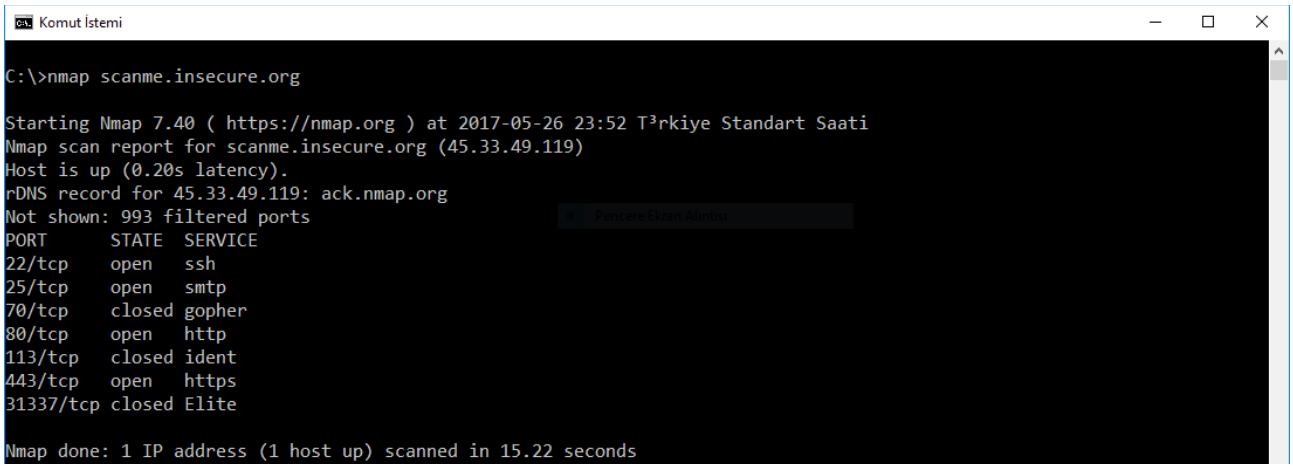
Temel Tarama Teknikleri

Tek Bir Hedefi Taramak

Nmap'i hiçbir komut satırı seçeneğiyle çalıştırmadığınızda sadece belirlenmiş hedef taranır. Bir hedef bir IP adresi veya ana makine adı olabilir (Makine adını Nmap çözmeye çalışacaktır).

Kullanım şekli : *nmap hedef*

Aşağıdaki örnekte nmap programını üretenlerin bizim için hazırldığı **scanme.insecure.org** sitesini tarayacağız. Eğer İnternet bağlantınız varsa bu taramayı yapabilirsiniz. Eğer bağlantınız yoksa kendi yerel ağınızdaki IP adresini bildiğiniz bir makineyi de tarayabilirsiniz.



Oluşan tarama, belirtilen hedefte tespit edilen bağlantı noktalarının durumunu gösterir.
Aşağıdaki tabloda, tarama tarafından görüntülenen çıktı alanları açıklanmaktadır.

PORT	DURUM	HİZMET
Bağlantı noktası numarası / protokol	Port durumu	Port için hizmet tipi

Yukarıdaki tarama sonuçlarının ilk satırına bakalım 22 numaralı TCP protoklü portu, portun durumu açık ve bu porttan ssh hizmeti sunuluyor. İkinci satırda 25 numaralı TCP protokolü, portun durumu açık ve bu porttan smtp hizmeti sunuluyor. Üçüncü satırda 70 numaralı TCP protokolü portu, portun durumu kapalı ve bu porttan port açık olsaydı gopher hizmeti sunulucaktı. Dördüncü satırda 80 numaralı TCP protokolü potru ve bu porttan http hizmeti sunuluyor, vb...

Varsayılan bir Nmap taraması en sık kullanılan 1000 TCP / IP portunu denetler.Bir sorguya yanıt veren bağlantı noktaları altı bağlantı noktasından birine sınıflandırılır: açık(open), kapalı(closed), filtrelenmiş(filtered), filtrelenmemiş(unfiltered), açık | filtrelenmiş, kapalı | filtrelenmiş. Aşağıda bu durumlar ayrıntılı açıklanmıştır.

Açık
Açık bağlantı noktası, gelen bir bağlantı isteklerine aktif şekilde yanıt veren bir bağlantı noktasıdır.

Kapalı
Kapalı bir bağlantı noktası, hedefte aktif olarak bir sorguya yanıt veren, ancak bağlantı noktasında çalışan herhangi bir hizmeti olmayan bir bağlantı noktasıdır. Kapatılan bağlantı noktaları, gelen trafiği filtrelemek için herhangi bir güvenlik duvarının bulunmadığı sistemlerde yaygın olarak bulunur.

Filtrelenmiş
Filtrelenmiş portlar, tipik olarak, Nmap'ın portun açık veya kapalı olup olmadığını belirlemesini önleyen bir güvenlik duvarı tarafından korunan portlardır.

Filtrelenmemiş
Filtrelenmemiş bir port, Nmap'ın erişebildiği bir porttur ancak açık veya kapalı olup olmadığını belirleyemez.

Açık | Filtrelenmiş
Açık filtrelenmiş bir port, Nmap tarafından açık veya filtrelendiği düşünülen bir porttur. Portun hangi durumunda olduğunu kesin belirleyememiştir.

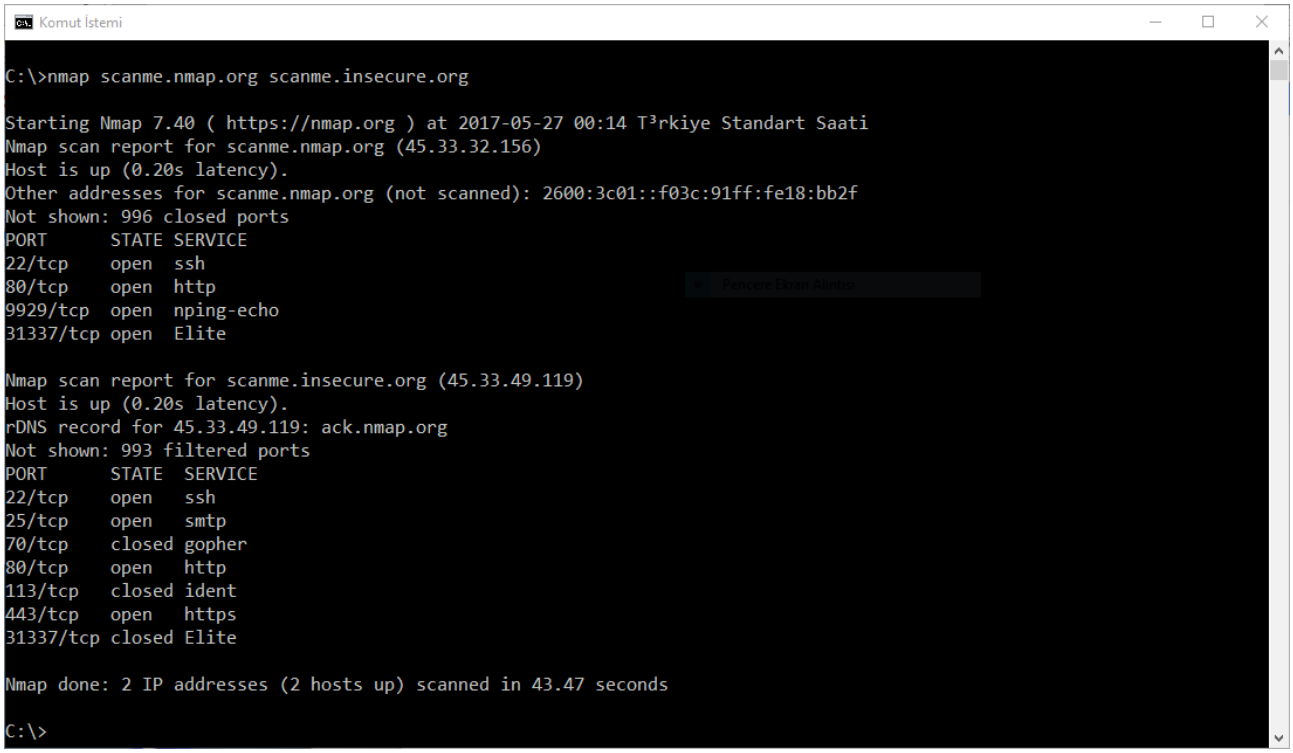
Kapalı | Filtrelenmiş
Kapalı filtrelenmiş bir , Nmap tarafından kapalı veya filtrelendiği düşünülen bir porttur. Portun hangi durumunda olduğunu kesin belirleyememiştir.

Birden Çok Hedefi Tarama

Nmap, aynı anda birden fazla bilgisayarı taramak için kullanılabilir. Bunun için komut satırında hedef IP adreslerini veya ana bilgisayar adlarını boşluklarla ayrılmış şekilde birlikte yazmak yeterlidir.

Kullanım şekli : *nmap hedef1 hedef2*

Aşağıdaki örnekte yine Nmapın sunduğu **scanme.nmap.org** ve **scanme.insecure.org** adresleri aynı anda taranmıştır.



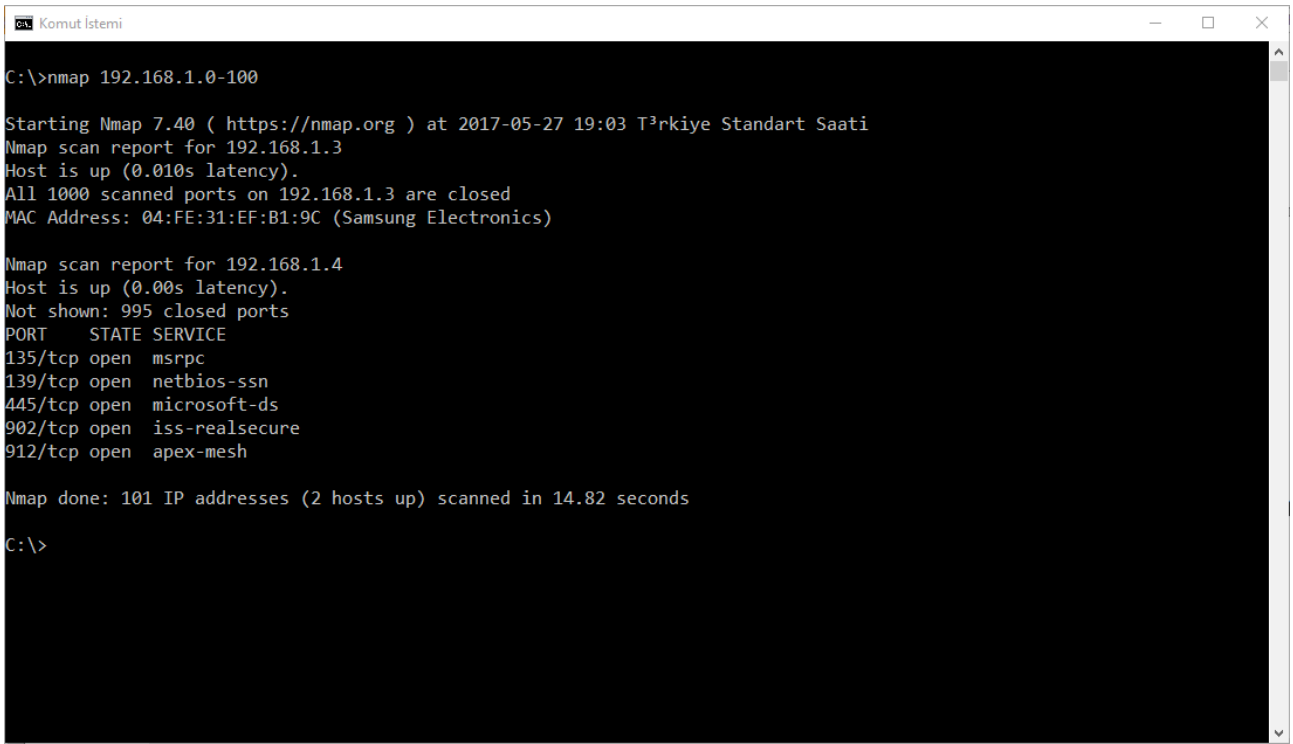
IP Adresi Aralığı Tarama

İstenirse belirli bir IP adresi aralığı taranabilir.

Kullanım şekli : *nmap hedef Ip adres aralığı*

Aşağıdaki örnekte yerel ağımdaki 1.0 adresinden 1.100 adresine kadar bu adres aralığındaki makineler taranmıştır. Bu taramaya 1.0 ve 1.100 adresleri de dahildir.

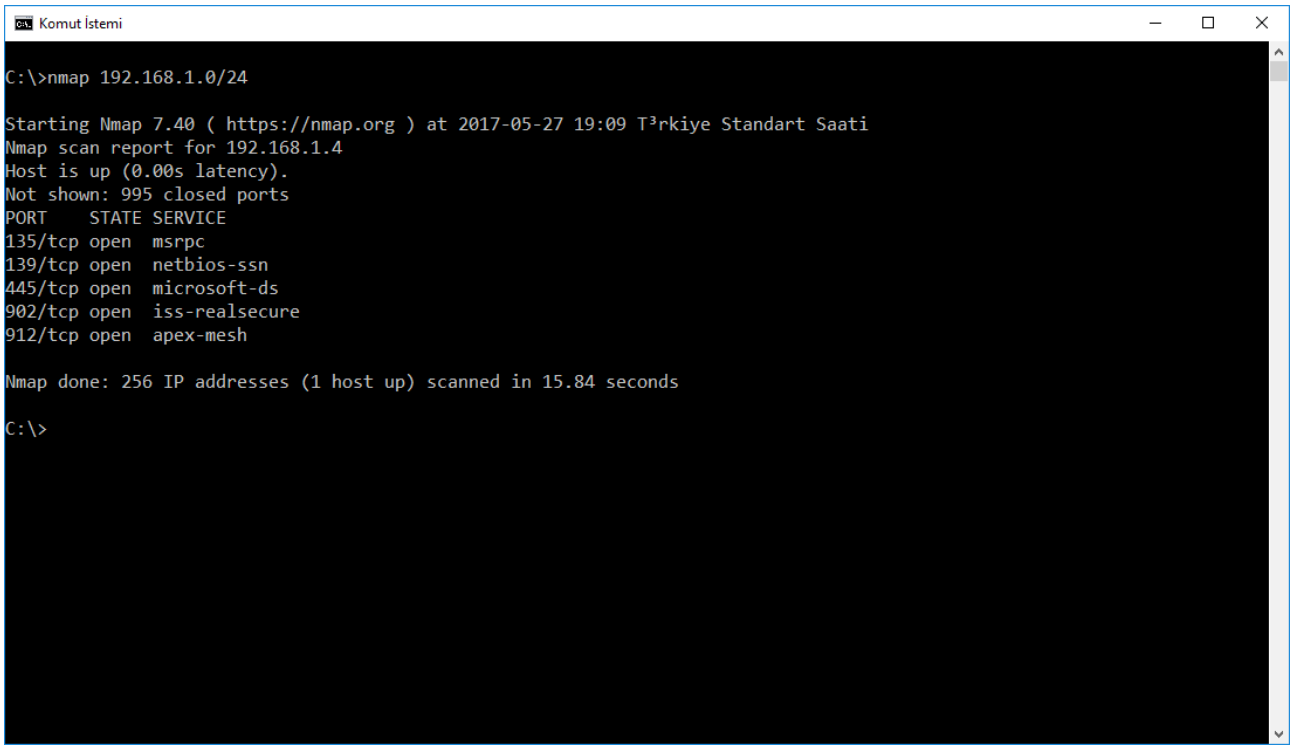
Tüm Alt Ağda Tarama



Nmap, CIDR (Classless Inter-Domain Routing-Sınıfsız Etki Alanı Arası Yönlendirme) gösterimini kullanarak tüm bir alt ağı taramak için kullanılabilir.

Kullanım şekli : *nmap network/CIDR (Prefix)*

Aşağıdaki örnekte, Nmap'a tüm 192.168.1.0 ağını taraması söylenmiştir. CIDR gösterimi, ağ adresi ve alt ağ maskesinden oluşur.



Hedef Listesini Tarama

Taranacak çok sayıda sisteminiz varsa, IP adresini (veya ana bilgisayar adlarını) bir metin dosyasına girebilir ve bu dosyayı komut satırında Nmap girişi olarak kullanabilirsiniz.

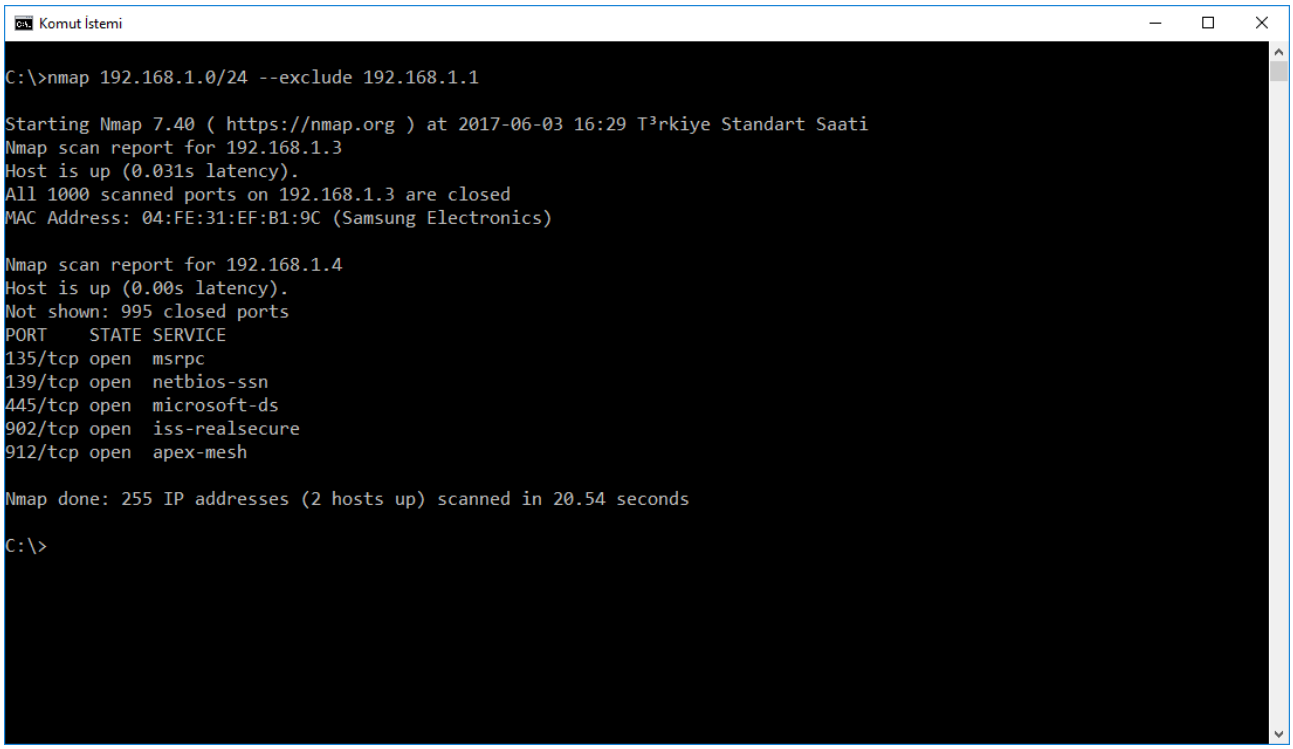
Kullanım şekli : *nmap -iL list.txt*

Hedefleri Bir Taramadan Çıkarma

İstenilen makineyi taramadan hariç tutmak için --exclude seçeneği Nmap ile birlikte kullanılır.

Kullanım şekli : *nmap [targets] --exclude [target(s)]*

Aşağıdaki örnekte tüm 192.168.1.0 ağı taranmış fakat 192.168.1.1 IP adresli makine bu taramaya dahil edilmemiştir.



İstenirse aşağıdaki komut örneğinde olduğu gibi birden fazla makine taramadan çıkarılabilir.

nmap 192.168.1.0/24 --exclude 192.168.1.100-105

Yukarıdaki komut ile 192.168.1.100 ile 105 aralığı dışındaki tüm ağ taranmıştır.

Liste Kullanarak Hedefleri Hariç Tutma

Yukarıdaki exclude seçeneğine benzer şekilde hedef makine IP adresi veya alan adından oluşan bir liste ile taramasından hariç tutulabilir.

Kullanım Şekli: *nmap [targets] --excludefile [list.txt]*

Örnek olarak aşağıdaki komut kullanıldığında belirlediğimiz listedeki makineler hariç tüm 192.168.1.0 ağı taranacaktır.

nmap 192.168.1.0/24 --excludefile list.txt

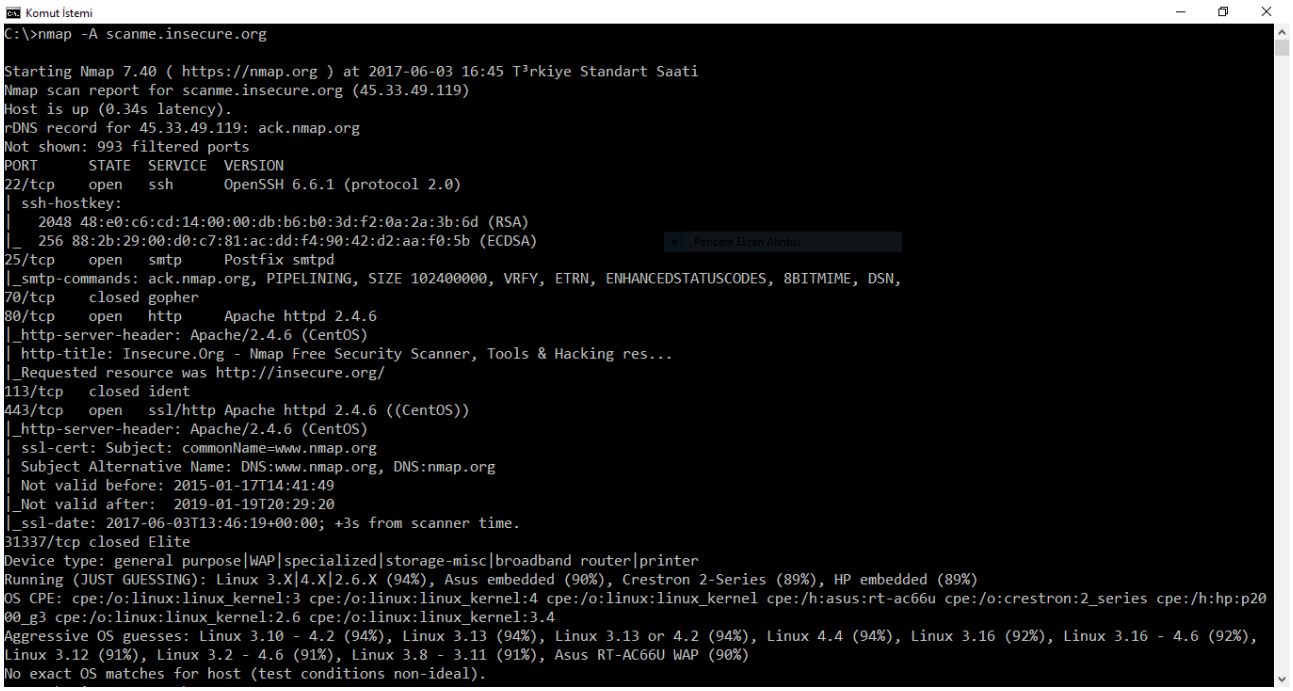
Agresif Tarama Yapma

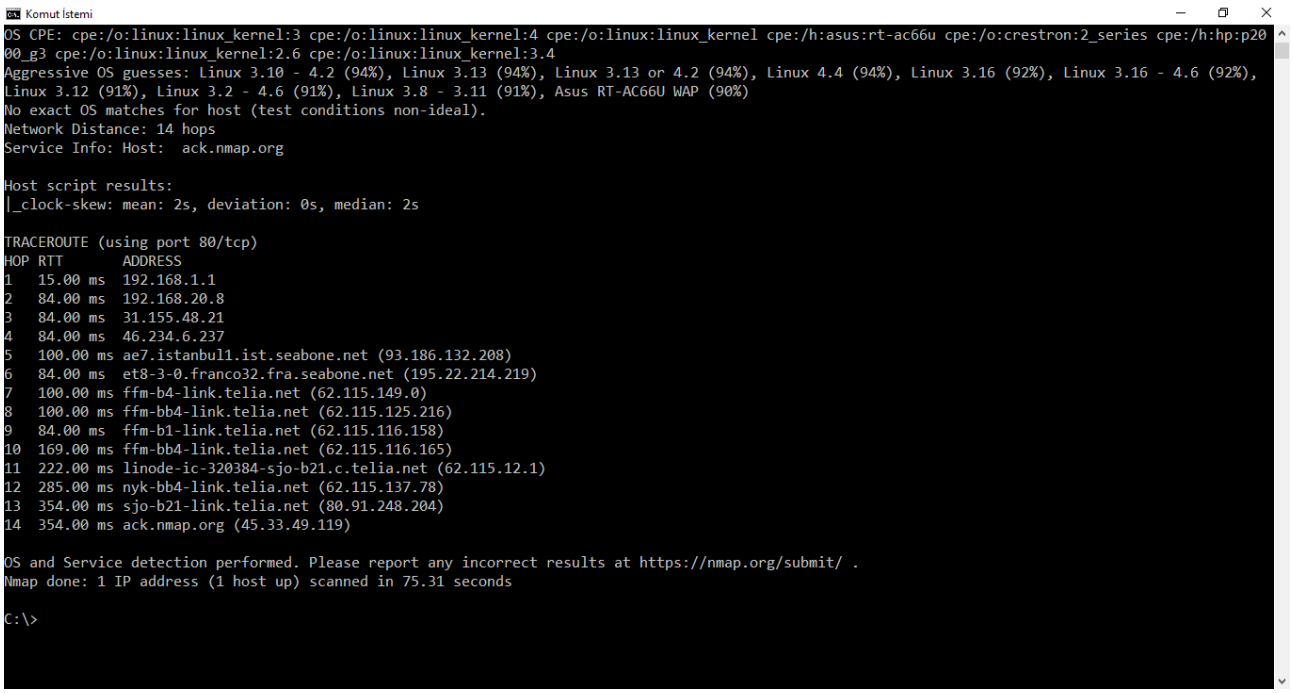
-A parametresi, Nmap'a agresif bir tarama yapmasını söyler. Agresif tarama, Nmap'te en çok kullanılan seçeneklerin bazılarını seçer ve komut satırı argümanlarının uzun bir dizesini yazmanın basit bir alternatifi olarak

sunulmaktadır. -A parametresi birkaç gelişmiş seçenek için eşanlamlıdır (örneğin -O-sC --traceroute) gibi komutları ayrı ayrı yazmaktan kurtuluruz bu komutlar ne anlama geliyor derseniz rehberin ileriki bölümlerinde göreceğiz.

Kullanım Şekli : *nmap -A [target]*

Aşağıdaki örnekte insecure sitesine agresif tarama yapılmıştır.





Bir IPv6 Hedefi Tarama

-6 parametresi, bir IPv6 hedefin taranmasını yapmak için kullanılır. Bu taramanın çalışması için hem ana bilgisayar hem de hedef sistemler IPv6 protokolünü desteklemelidir.
Kullanım Şekli : *nmap -6 [target]*

BÖLÜM 3: KEŞİF SEÇENEKLERİ

Keşif Seçeneklerine Genel Bakış

Nmap bir hedefin portlarını taramadan önce, ana bilgisayarın "canlı" olup olmadığını görmek için ICMP yankı istekleri göndermeye çalışacaktır. Nmap, çevrimiçi olmayan ana makineleri araştırmaya çalışırken zaman kaybetmeyeceğinden, birden çok ana bilgisayarı tararken zamandan kazanabilirsiniz. ICMP istekleri genellikle güvenlik duvarları tarafından engellendiği için, Nmap bu ortak web sunucusu bağlantı noktaları genellikle (ICMP olmasa bile) açık olduğundan port 80 ve 443'e bağlanmaya çalışacaktır.

Varsayılan bulma seçenekleri, güvenli sistemleri tararken yararlı değildir ve taramayı engellemektedir. Aşağıdaki bölümde, mevcut hedefleri ararken daha kapsamlı keşif yapmanıza olanak tanıyan ana bilgisayar bulma için alternatif yöntemler tanımlamaktadır.

Bu bölümde ele alınan özelliklerin özeti:

Özellik	**Opsiyon**
Ping atma	-PN
Sadece Ping taraması yap	-sP
TCP SYN Ping	-PS
TCP ACK Ping	-PA
UDP Ping	-PU
SCTP INIT Ping	-PY
ICMP Echo Ping	-PE
ICMP Zaman Damgası Ping	-PP
ICMP Adres Maskesi Ping	-PM
IP Protokol Ping	-PO
ARP Ping	-PR
Traceroute	--traceroute
Ters DNS Çözünürlüğünü Zorla	-R

Ters DNS Çözünürlüğünü Devre Dışı Bırak	-n
Alternatif DNS Arama	--system-dns
DNS Sunucularını Manuel Olarak Belirleyin	--dns-servers
Bir ana bilgisayar Liste Oluştur	-sL

Ping Atma

Varsayılan olarak, Nmap, açık portlar için bir sistemi taramaya çalışmadan önce hedefe çevrimiçi olup olmadığını görmek için ping atar. Bu özellik, yanıt vermeyen hedeflerin atlanmalarına neden olması nedeniyle tarama yaparken zamandan kazanmanıza yardımcı olur.

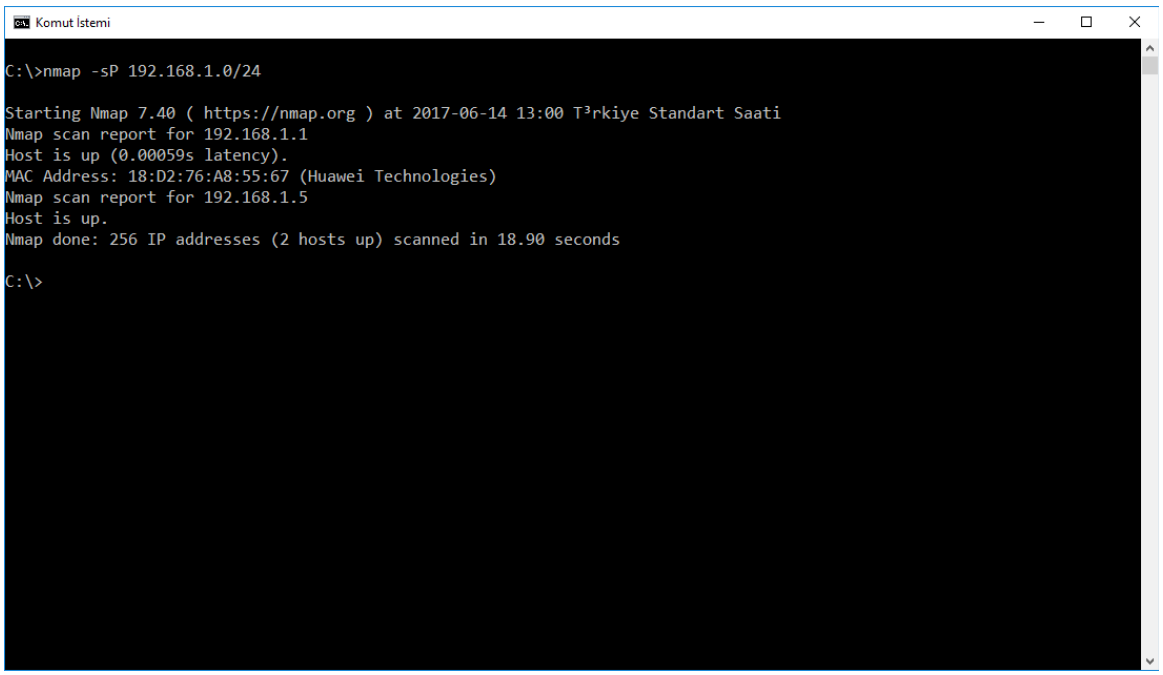
Kullanım Şekli : *nmap Hedef*

Örnek : nmap -PN 192.168.1.48

Sadece Ping taraması yap

-sP seçeneği, belirtilen ana bilgisayarda basit bir ping gerçekleştirmek için kullanılır.

Kullanım Şekli : nmap -sP Hedef

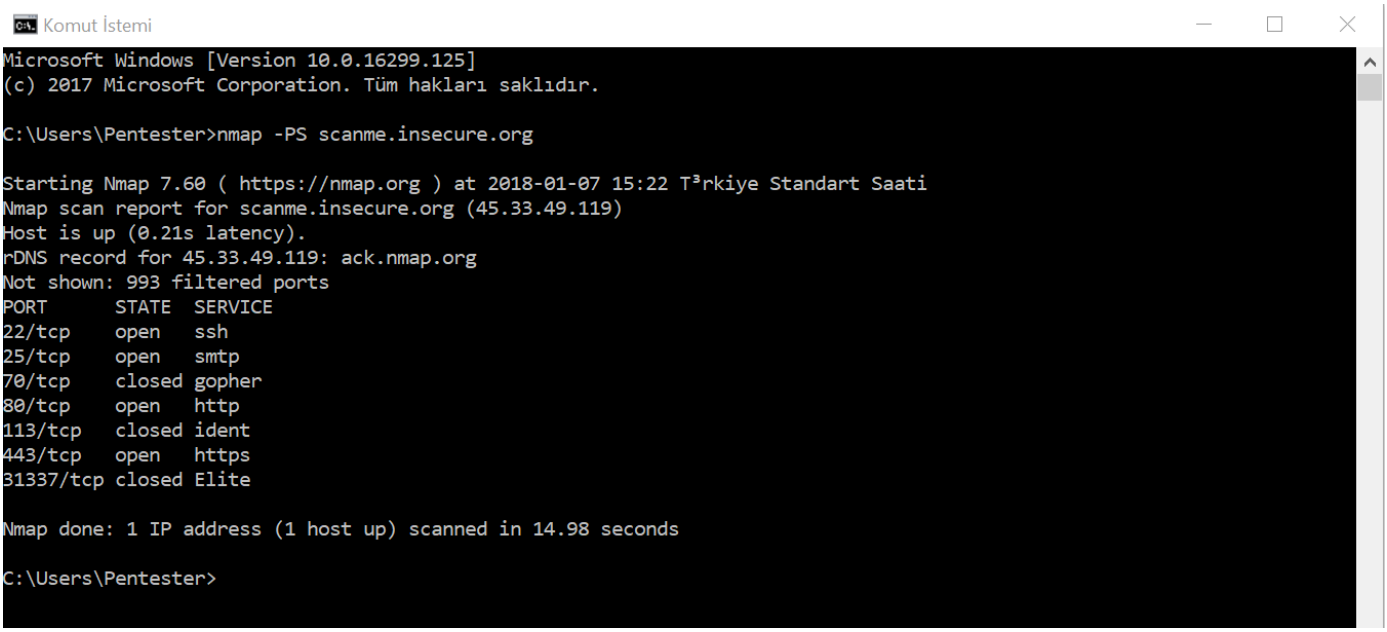


Bu seçenek, taranacak ağdaki hedefleri gerçekten taramadan hangi ana bilgisayarların çevrim içi olduğunu görmek için hedef ağın hızlı bir şekilde aranmasını istiyorsanız yararlıdır. Yukarıdaki örnekte, 192.168.1.0 alt ağ bölgesindeki 254 adres pinglenir ve sadece canlı hostlardan gelen sonuçlar görüntülenir.

TCP SYN Ping

-PS seçeneği bir TCP SYN ping işlemi gerçekleştirir.

Kullanım Şekli : nmap -PS [port1,port1,etc] [hedef]



TCP SYN ping, hedef sisteme bir SYN paketi gönderir ve bir yanıt dinler. Bu alternatif bulma yöntemi, standart ICMP pinglerini engelleyecek şekilde yapılandırılmış sistemler için kullanışlıdır.

NOT: -PS için varsayılan bağlantı noktası 80'dir, ancak diğer portlar şu sözdizimini kullanarak belirtilebilir: nmap -PS 22,25,80,443, vb.

TCP ACK Ping

-PA, belirtilen hedefte TCP ACK ping gerçekleştirir.

Kullanım Şekli : nmap -PA [port1,port1,etc] [hedef]

```
C:\Users\Pentester>nmap -PA scanme.insecure.org

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-07 15:26 T³rkiye Standart Saati
Nmap scan report for scanme.insecure.org (45.33.49.119)
Host is up (0.21s latency).
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
22/tcp    open   ssh
25/tcp    open   smtp
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 14.24 seconds
```

-PA seçeneği, Nmap'in belirtilen ana makinelere TCP ACK paketleri göndermesine neden olur. Bu yöntem, hedeften gelen bir yanıt istemek için varolmayan TCP bağlantılarına yanıt vererek ana bilgisayarları keşfetmeye çalışır. Diğer ping seçenekleri gibi, standart ICMP pinglerinin engellendiği durumlarda yararlıdır.

UDP Ping

-PU seçeneği, hedef sistemde bir UDP ping işlemi gerçekleştirir.

Kullanım Şekli : nmap -PU [port1,port1,etc] [hedef]

```
C:\Users\Pentester>nmap -PU scanme.insecure.org

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-07 15:29 T³rkiye Standart Saati
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 4.22 seconds
```

Bu keşif yöntemi, bir hedefin yanıtını almak için UPD paketleri gönderir. Çoğu firewalllu sistem bu tür bir bağlantıyı engellese de, yalnızca yapılandırılmış bazı sistemler, TCP bağlantılarını filtrelemek üzere yapılandırıldıysa, izin verebilir.

SCTP INIT Ping

-PY parametresi, Nmap'a bir SCTP INIT ping işlemi gerçekleştirmesini bildirir.

Kullanım Şekli : nmap -PY [port1,port1,etc] [hedef]

Bu keşif yöntemi, Ana Bilgisayarların Akış Kontrol İletim Protokolünü (SCTP-Stream Control Transmission Protocol) kullanarak bulunmasını dener. SCTP genellikle IP tabanlı telefon sistemleri için kullanılır.

Kali Linux İle Network Sızma (Penetrasyon) Testleri Eğitimi **SADECE ₺25**

https://www.udemy.com/kali-ile-temel-network-penetrasyon-testleri/?couponCode=SADECE25