

Nmap Live Host Discovery

Task 1 Introduction (Görev 1 Giriş)

Bir ağı hedeflemek istediğimizde, tekrar eden görevleri yerine getirmemize ve aşağıdaki soruları yanıtlamamıza yardımcı olacak verimli bir araç bulmak isteriz:

1. Hangi sistemler açık?
2. Bu sistemlerde hangi hizmetler çalışıyor?

Güveneceğimiz araç Nmap'tir. Canlı bilgisayarları bulmakla ilgili ilk soru bu odada yanıtlanıyor. Bu oda, Nmap'e adanmış dört odadan oluşan bir serinin ilk odasıdır. Çalışan hizmetleri keşfetme hakkındaki ikinci soru, port taramaya odaklanan sonraki Nmap odalarında yanıtlanmaktadır.

Bu oda, bu Nmap serisindeki dört odadan ikidir. Bu dört oda da Ağ Güvenliği modülünün bir parçasıdır.

1. Nmap Live Host Discovery (Nmap Canlı Ana Bilgisayar Keşfi)
2. Nmap Basic Port Scans (Nmap Temel Port Taramaları)
3. Nmap Advanced Port Scans (Nmap Gelişmiş Port Taramaları)
4. Nmap Post Port Scans (Nmap Post Port Taramaları)

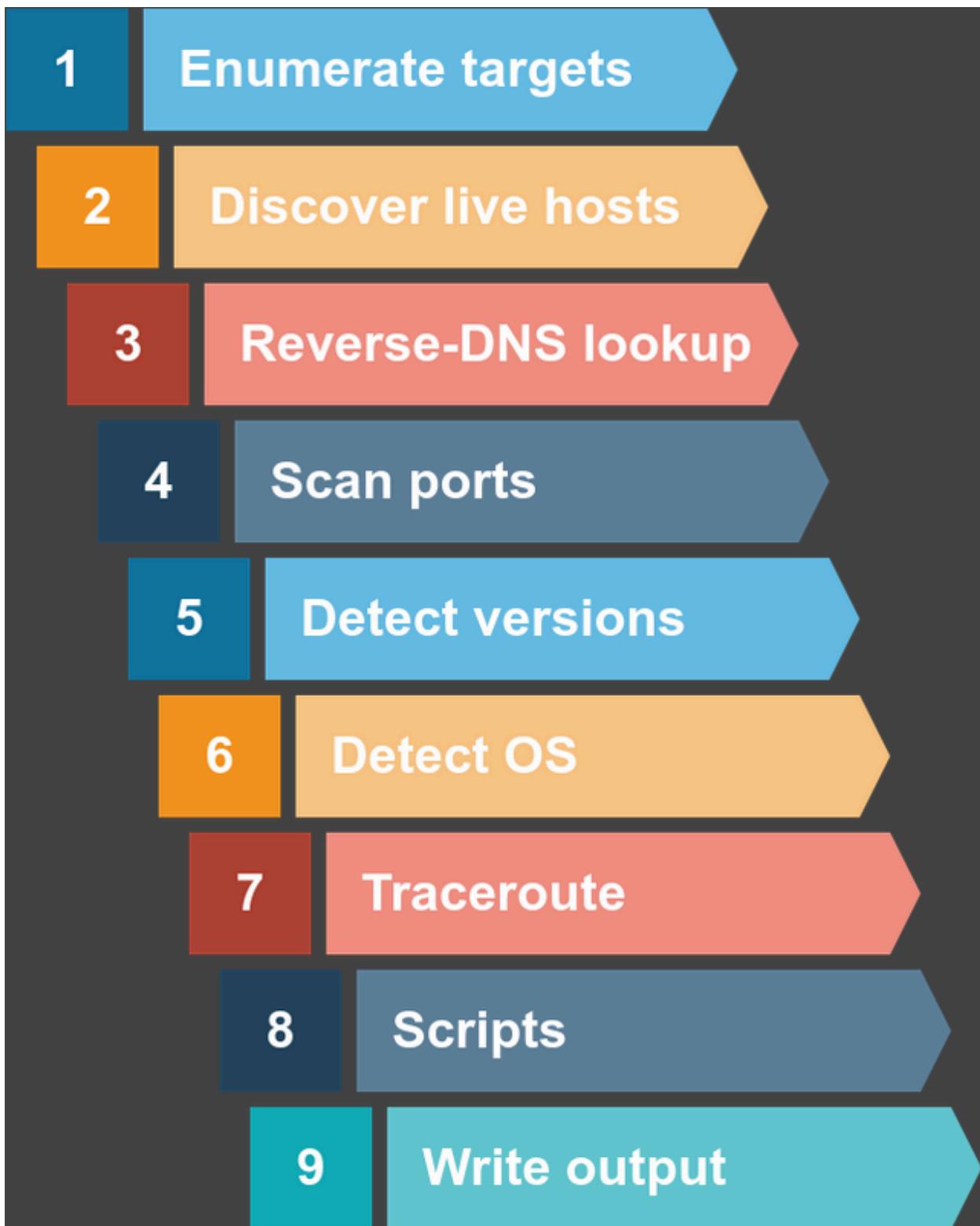
Bu oda, Nmap'in port taramasından önce çevrimiçi olan sistemleri keşfetmek için gerçekleştirdiği adımları açıklamaktadır. Bu aşama çok önemlidir çünkü çevrimdışı sistemleri port taramaya çalışmak sadece zaman kaybettirir ve ağıda gereksiz gürültü yaratır.

Nmap'in canlı ana bilgisayarları keşfetmek için kullandığı farklı yaklaşımları sunuyoruz. Özellikle, biz kapsar:

1. ARP taraması: Bu tarama, canlı ana bilgisayarları keşfetmek için ARP isteklerini kullanır

2. ICMP taraması: Bu tarama, canlı ana bilgisayarları tanımlamak için ICMP isteklerini kullanır
3. TCP/UDP ping taraması: Bu tarama, canlı ana bilgisayarları belirlemek için TCP bağlantı noktalarına ve UDP bağlantı noktalarına paketler gönderir.

Daha önce de belirtildiği gibi, bu odadan başlayarak, sistemleri ve hizmetleri aktif olarak keşfetmek için Nmap kullanacağınız. Nmap, bir ağ güvenliği uzmanı ve açık kaynak programcısı olan Gordon Lyon (Fyodor) tarafından yaratılmıştır. 1997 yılında piyasaya sürüldü. Network Mapper'ın kısaltması olan Nmap, GPL lisansı altında yayınlanan ücretsiz, açık kaynaklı bir yazılımdır. Nmap, ağları haritalamak, canlı ana bilgisayarları tanımlamak ve çalışan hizmetleri keşfetmek için endüstri standarı bir araçtır. Nmap'in komut dosyası motoru, parmak izi hizmetlerinden güvenlik açıklarından yararlanmaya kadar işlevsellliğini daha da genişletebilir. Bir Nmap taraması genellikle aşağıdaki şekilde gösterilen adımlardan geçer, ancak çoğu isteğe bağlıdır ve sağladığınız komut satırı argümanlarına bağlıdır.



Soru ⇒ Bu sorulardan bazıları, görev sorularını yanıtlamak için statik bir sitenin kullanılmasını gerektirirken, diğerleri AttackBox ve hedef VM'nin kullanılmasını

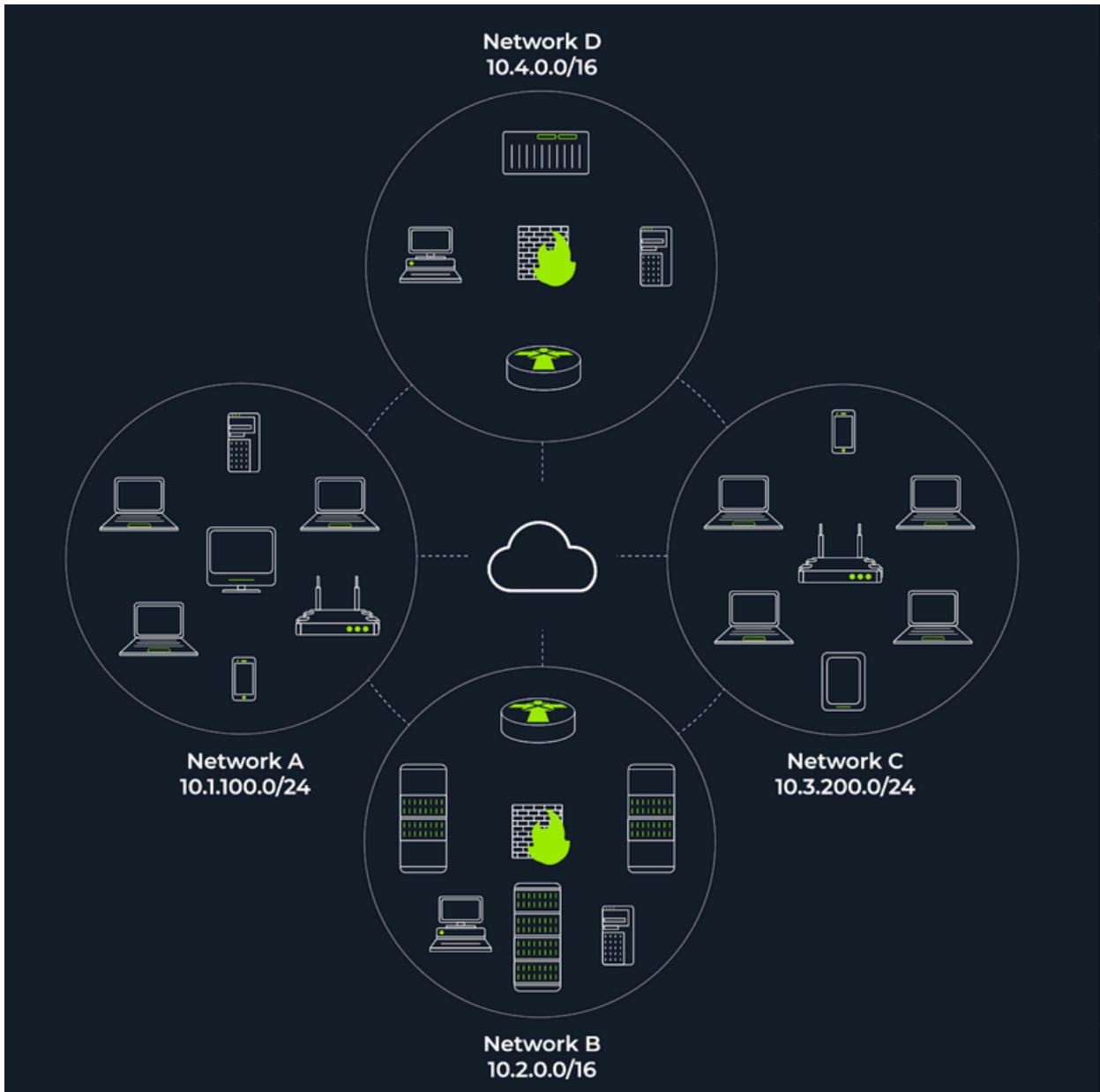
gerektirecektir.

Cevap ⇒ Cevap Gerekmemektedir.

Task 2 Subnetworks (Görev 2 Alt Ağlar)

Ana görevlere geçmeden önce birkaç terimi gözden geçirelim. Bir ağ segmenti, paylaşılan bir ortam kullanılarak bağlanan bir grup bilgisayardır. Örneğin, bu ortam Ethernet anahtarı veya WiFi erişim noktası olabilir. Bir IP alanında, bir alt ağ genellikle birbirine bağlı ve aynı yönlendiriciyi kullanmak üzere yapılandırılmış bir veya daha fazla ağ segmentine eşdeğerdir. Ağ segmenti fiziksel bir bağlantıyı ifade ederken, alt ağ mantıksal bir bağlantıyı ifade eder.

Aşağıdaki ağ şemasında, dört ağ segmentimiz veya alt ağımız vardır. Genel olarak, sisteminiz bu ağ bölümlerinden/alt ağlardan birine bağlı olacaktır. Bir alt ağ ya da basitçe bir alt ağ, kendi IP adres aralığına sahiptir ve bir yönlendirici aracılığıyla daha kapsamlı bir ağa bağlanır. Her ağa bağlı olarak güvenlik politikalarını uygulayan bir güvenlik duvarı olabilir.



Yukarıdaki şekilde iki tür alt ağ gösterilmektedir:

- 16'lı alt ağlar, yani alt ağ maskesi 255.255.0.0 olarak yazılabilir. Bu alt ağ yaklaşık 65 bin ana bilgisayara sahip olabilir.
- Alt ağ maskesinin 255.255.255.0 olarak ifade edilebileceğini gösteren /24'lü alt ağlar. Bu alt ağ yaklaşık 250 ana bilgisayara sahip olabilir.

Alt ağ oluşturma hakkında daha fazla bilgi edinmek isterseniz LAN'a Giriş bölümündeki Görev 2'ye başvurabilirsiniz.

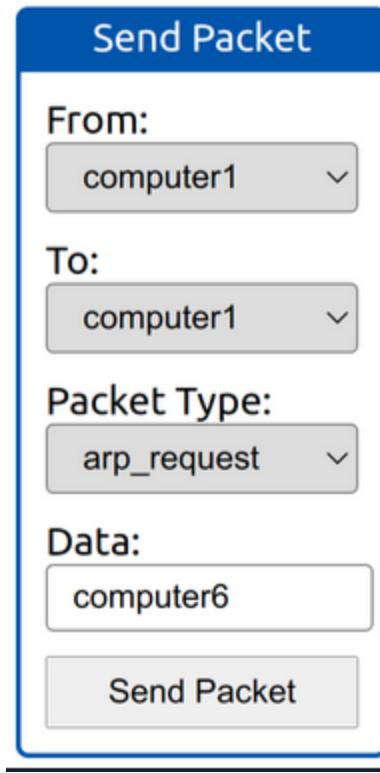
Aktif keşfin bir parçası olarak, bir grup ana bilgisayar veya bir alt ağ hakkında daha fazla bilgi keşfetmek isteriz. Aynı alt ağa bağlıysanız, tarayıcınızın canlı ana bilgisayarları keşfetmek için ARP (Adres Çözümleme Protokolü) sorgularına güvenmesini beklersiniz. Bir ARP sorgusu donanım adresini (MAC adresi) almayı amaçlar, böylece bağlantı katmanı üzerinden iletişim mümkün olur; ancak bunu ana bilgisayarın çevrimiçi olduğu sonucunu çıkarmak için kullanabiliriz. (Bağlantı katmanını Görev 4'te tekrar ele alacağız).

A Aşındaysanız, ARP'yi yalnızca bu alt ağdaki (10.1.100.0/24) cihazları keşfetmek için kullanabilirsiniz. Hedef sistem(ler)in alt ağından farklı bir alt ağa bağlı olduğunuzu varsayıyalım. Bu durumda, tarayıcınız tarafından oluşturulan tüm paketler başka bir alt ağdaki sistemlere ulaşmak için varsayılan ağ geçidi (yönlendirici) üzerinden yönlendirilecektir; ancak ARP sorguları yönlendirilmeyecek ve dolayısıyla alt ağ yönlendiricisini geçemeyecektir. ARP bir bağlantı katmanı protokolüdür ve ARP paketleri kendi alt ağlarına bağlıdır.

Ağ simülatörünü başlatmak için "Siteyi Görüntüle" düğmesine tıklayın. Görev 2, 4 ve 5'teki soruları yanıtlamak için bu simülatörü kullanacağız.

Sorular

Aşağıdakileri içeren bir paket gönderin:



- Bilgisayar1'den
- Bilgisayar1'e (yayın olduğunu belirtmek için)
- Paket Türü: "ARP İsteği"
- Veri: computer6 (çünkü ARP İsteği kullanarak computer6 MAC adresini soruyoruz)

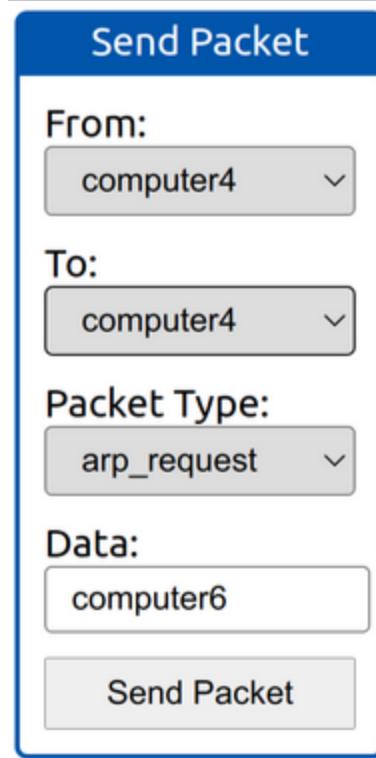
Soru ⇒ ARP İsteğini kaç cihaz görebilir(Cihazları sayarken anahtarı saymayın.)?

Cevap ⇒ 4

Soru ⇒ Bilgisayar6 ARP İsteğini aldı mı? (Y/N)

Cevap ⇒ N

Aşağıdakileri içeren bir paket gönderin:



- Bilgisayar4'ten
- Bilgisayara4 (yayın olduğunu belirtmek için)
- Paket Türü: "ARP İsteği"
- Veri: computer6 (çünkü ARP İsteği kullanarak computer6 MAC adresini soruyoruz)

Soru ⇒ ARP İsteğini kaç cihaz görebilir(Cihazları sayarken anahtarları saymayın.)?

Cevap ⇒ 4

Soru ⇒ Bilgisayar6 ARP İsteğine yanıt verdi mi? (Y/N)

Cevap ⇒ Y

Task 3 Enumerating Targets (Görev 3 Hedeflerin Numaralandırılması)

Görev 1'de tarama için kullanabileceğimiz farklı tekniklerden bahsetmiştik. Her birini ayrıntılı olarak açıklamadan ve canlı bir hedefe karşı kullanmadan önce, taramak istediğimiz hedefleri belirtmemiz gereklidir. Genel olarak, bir liste, bir aralık veya bir alt ağ sağlayabilirsiniz. Hedef belirtimi örnekleri şunlardır:

- liste: MACHINE_IP scanme.nmap.org example.com 3 IP adresini tarayacaktır.
- aralık: 10.11.12.15-20 6 IP adresini tarayacaktır: 10.11.12.15, 10.11.12.16, ... ve 10.11.12.20.
- alt ağ: MACHINE_IP/30 4 IP adresini tarayacaktır.

Hedef listeniz için girdi olarak bir dosya da sağlayabilirsiniz, nmap -iL list_of_hosts.txt.

Nmap'in tarayacağı ana bilgisayarların listesini kontrol etmek istiyorsanız, nmap -sL TARGETS seçeneğini kullanabilirsiniz. Bu seçenek size Nmap'in tarayacağı ana bilgisayarların ayrıntılı bir listesini taramadan verecektir; ancak Nmap, adlarını almak için tüm hedefler üzerinde bir ters DNS çözümlemesi deneyecektir. İsimler, pentester için çeşitli bilgileri açığa çıkarabilir. (Eğer Nmap'in DNS sunucusuna girmesini istemiyorsanız -n ekleyebilirsiniz).

AttackBox'ı Başlat düğmesini kullanarak AttackBox'ı başlatın, AttackBox hazır olduğunda terminali açın ve aşağıdakileri yanıtlamak için Nmap'i kullanın.

Soru ⇒ Hedef olarak 10.10.12.13/29 adresini verdığınızde Nmap'in tarayacağı ilk IP adresi nedir(İpucu⇒ Run nmap -sL -n 10.10.12.13/29.)?

Cevap ⇒ **10.10.12.8**

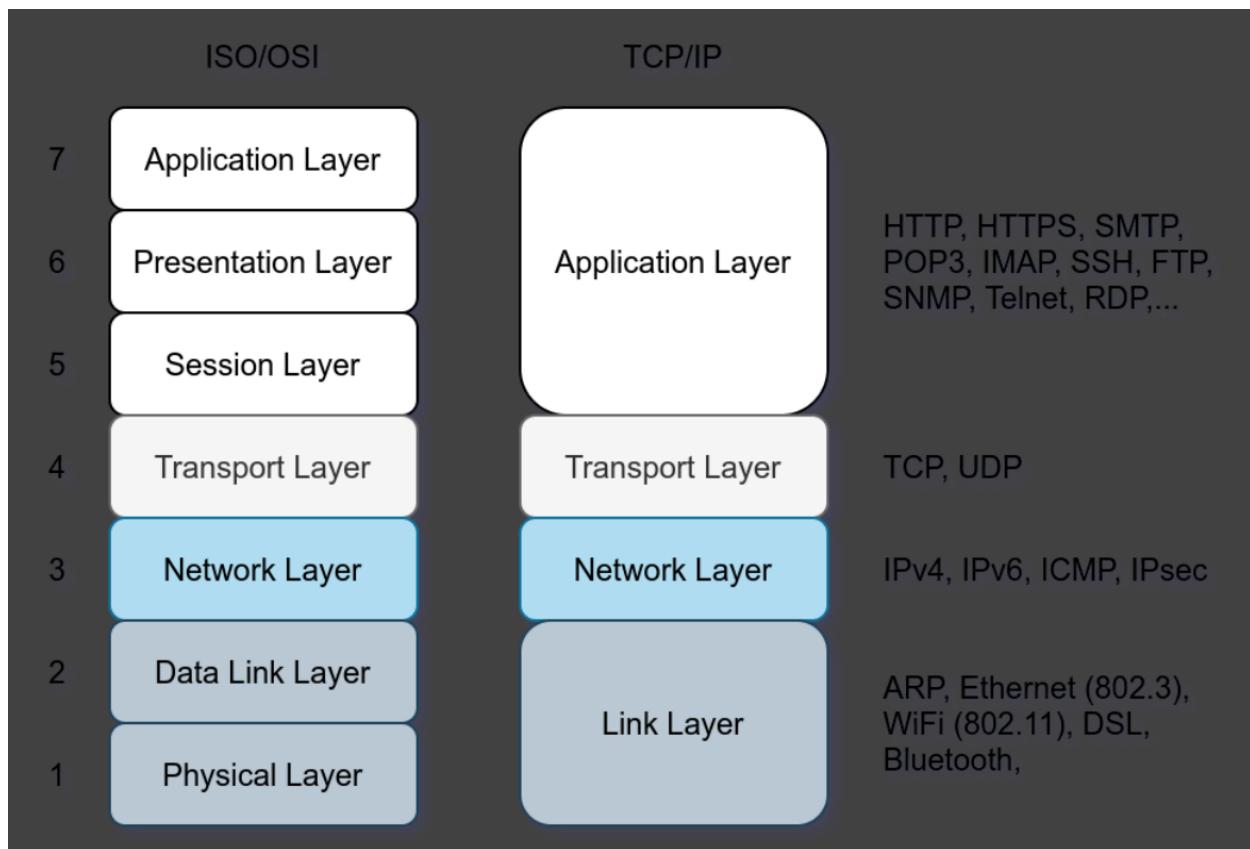
Soru ⇒ Aşağıdaki 10.10.0-255.101-125 aralığını sağlarsanız Nmap kaç IP adresi tarayacaktır (İpucu⇒Run nmap -sL -n 10.10.0-255.101-125.)?

Cevap ⇒ **6400**

Task 4 Discovering Live Hosts (Görev 4 Canlı Ana Bilgisayarları Keşfetme)

Şimdi şekilde gösterilen TCP/IP katmanlarını tekrar gözden geçirelim. Canlı ana bilgisayarları keşfetmek için protokollerden yararlanacağız. Aşağıdan yukarıya doğru, şunları kullanabiliriz:

- Bağlantı Katmanından ARP
- Ağ Katmanından ICMP
- Aktarım Katmanından TCP
- Aktarım Katmanından UDP



Tarayıcıların her birini nasıl kullanabileceğini ayrıntılı olarak tartışmadan önce, bu dört protokolü kısaca gözden geçireceğiz. ARP'nin tek bir amacı vardır: ağ segmentindeki yayın adresine bir çerçeve göndermek ve belirli bir IP adresine sahip bilgisayardan MAC (donanım) adresini sağlayarak yanıt vermesini istemek.

ICMP'nin birçok türü vardır. ICMP ping Tip 8 (Echo) ve Tip 0 (Echo Reply) kullanır.

Aynı alt ağdaki bir sisteme ping atmak istiyorsanız, ICMP Echo'dan önce bir ARP sorusu yapılmalıdır.

TCP ve UDP taşıma katmanları olmasına rağmen, ağ tarama amacıyla, bir tarayıcı hedefin yanıt verip vermeyeceğini kontrol etmek için ortak TCP veya UDP bağlantı

noktalarına özel olarak hazırlanmış bir paket gönderebilir. Bu yöntem, özellikle ICMP Echo engellendiğinde etkilidir.

Ağ simülatörünü kapattıysanız, tekrar görüntülemek için Görev 2'deki "Siteyi Görüntüle" düğmesine tıklayın.

Aşağıdakileri içeren bir paket gönderin:

- Bilgisayar1'den
- Bilgisayar3'e
- Paket Türü: "Ping İsteği"

Sorular

Soru ⇒ Bilgisayar1'in ping işleminden önce gönderdiği paket türü nedir?

Cevap ⇒ ARP Request

Soru ⇒ Bilgisayar1'in ping göndermeden önce aldığı paketin türü nedir?

Cevap ⇒ ARP Response

Soru ⇒ Ping isteğine kaç bilgisayar yanıt verdi?

Cevap ⇒ 1

Aşağıdakileri içeren bir paket gönderin:

- Bilgisayar2'den
- Bilgisayar5'e
- Paket Türü: "Ping İsteği"

Soru ⇒ İlk ARP İsteğine yanıt veren ilk cihazın adı nedir?

Cevap ⇒ router

Soru ⇒ İkinci ARP İsteğine yanıt veren ilk cihazın adı nedir?

Cevap ⇒ computer5

Soru ⇒ Başka bir Ping İsteği gönderin. Yeni ARP Talepleri gerektirdi mi? (Y/N)

Cevap ⇒ N

Task 5 Nmap Host Discovery Using ARP (Görev 5 ARP Kullanarak Nmap Ana Bilgisayar Bulma)

Hangi ana bilgisayarların çalışır durumda olduğunu nasıl anlarsınız? Çevrimdışı bir ana bilgisayarı veya kullanılmayan bir IP adresini port taraması yaparak zamanımızı boş harcamaktan kaçınmak çok önemlidir. Çevrimiçi ana bilgisayarları keşfetmenin çeşitli yolları vardır. Herhangi bir ana bilgisayar bulma seçeneği sağlanmadığında, Nmap canlı ana bilgisayarları keşfetmek için aşağıdaki yaklaşımları izler:

1. Ayrıcalıklı bir kullanıcı yerel bir ağdaki (Ethernet) hedefleri taramaya çalıştığında, Nmap ARP isteklerini kullanır. Ayrıcalıklı kullanıcı root veya sudoers'a ait olan ve sudo'yu çalıştırabilen bir kullanıcıdır.
2. Ayrıcalıklı bir kullanıcı yerel ağ dışındaki hedefleri taramaya çalıştığında, Nmap ICMP yankı isteklerini, 80 numaralı bağlantı noktasına TCP ACK (Onay), 443 numaralı bağlantı noktasına TCP SYN (Senkronize Et) ve ICMP zaman damgası isteğini kullanır.
3. Ayrıcalıksız bir kullanıcı yerel ağ dışındaki hedefleri taramaya çalıştığında, Nmap 80 ve 443 numaralı bağlantı noktalarına SYN paketleri göndererek TCP 3 yönlü el sıkışmasına başvurur.

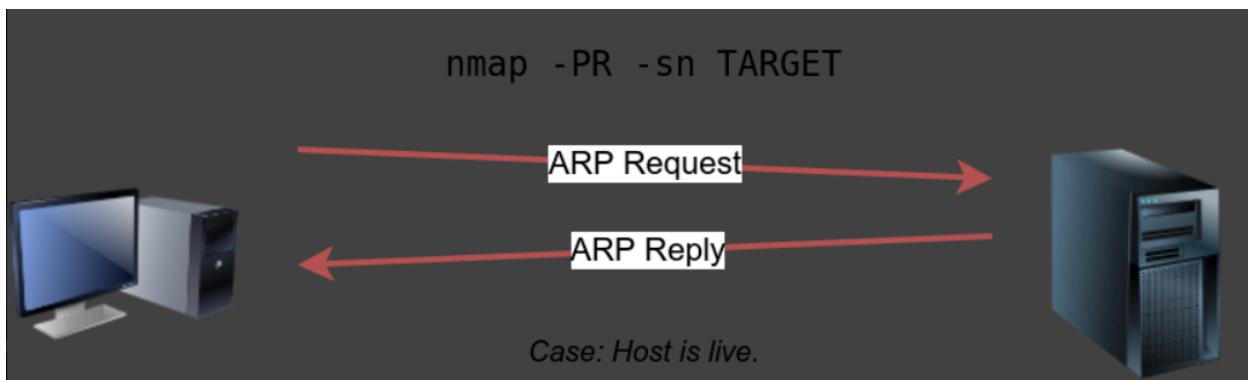
Nmap, varsayılan olarak, canlı ana bilgisayarları bulmak için bir ping taraması kullanır, ardından yalnızca canlı ana bilgisayarları taramaya devam eder. Nmap'i canlı sistemleri port taraması yapmadan çevrimiçi ana bilgisayarları keşfetmek için kullanmak istiyorsanız, nmap -sn TARGETS komutunu verebilirsiniz. Kullanılan farklı teknikler hakkında sağlam bir anlayış kazanmak için daha derine inelim.

ARP taraması yalnızca hedef sistemlerle aynı alt ağ üzerindeyseñiz mümkündür. Ethernet (802.3) ve WiFi (802.11) üzerinde, herhangi bir sistemle iletişim kurabilmeniz için o sistemin MAC adresini bilmeniz gereklidir. MAC adresi bağlantı katmanı başlığı için gereklidir; başlık diğer alanların yanı sıra kaynak MAC adresini ve hedef MAC adresini içerir. MAC adresini almak için işletim sistemi bir ARP sorgusu gönderir. ARP sorgularına yanıt veren bir ana bilgisayar açıktır. ARP sorgusu yalnızca hedef sizinle aynı alt ağ üzerindeyse, yani aynı Ethernet/WiFi üzerindeyse çalışır. Yerel bir ağın Nmap taraması sırasında birçok ARP sorgusunun oluşturulduğunu görmeyi beklemelisiniz. Nmap'in port taraması yapmadan

yalnızca ARP taraması yapmasını istiyorsanız, nmap -PR -sn TARGETS komutunu kullanabilirsiniz; burada -PR yalnızca ARP taraması istediğiniz belirtir. Aşağıdaki örnekte Nmap'in herhangi bir port taraması yapmadan konak keşfi için ARP kullandığı gösterilmektedir. Hedef makinemizle aynı alt ağdaki tüm canlı sistemleri keşfetmek için nmap -PR -sn MACHINE_IP/24 çalıştırıyoruz.

```
pentester@TryHackMe$ sudo nmap -PR -sn 10.10.210.6/24Starting Nmap 7.60
( https://nmap.org ) at 2021-09-02 07:12 BST
Nmap scan report for ip-10-10-210-75.eu-west-1.compute.internal (10.10.210.7
5)
Host is up (0.00013s latency).
MAC Address: 02:83:75:3A:F2:89 (Unknown)
Nmap scan report for ip-10-10-210-100.eu-west-1.compute.internal (10.10.210.
100)
Host is up (-0.100s latency).
MAC Address: 02:63:D0:1B:2D:CD (Unknown)
Nmap scan report for ip-10-10-210-165.eu-west-1.compute.internal (10.10.210.1
65)
Host is up (0.00025s latency).
MAC Address: 02:59:79:4F:17:B7 (Unknown)
Nmap scan report for ip-10-10-210-6.eu-west-1.compute.internal (10.10.210.6)
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.12 seconds
```

Bu durumda, AttackBox 10.10.210.6 IP adresine sahipti ve aynı alt ağdaki canlı ana bilgisayarları keşfetmek için ARP isteklerini kullandı. ARP taraması aşağıdaki şekilde gösterildiği gibi çalışır. Nmap tüm hedef bilgisayarlara ARP istekleri gönderir ve çevrimiçi olanlar bir ARP yanıtı göndermelidir.



Eğer tcpdump veya Wireshark gibi bir araç kullanarak oluşturulan paketlere bakarsak, aşağıdaki şekilde benzer bir ağ trafiği görürüz. Aşağıdaki şekilde, Wireshark her ARP isteğiyle ilgili kaynak MAC adresini, hedef MAC adresini, protokolü ve soruyu görüntüler. Kaynak adres AttackBox'ımızın MAC adresidir, hedef ise hedefin MAC adresini bilmediğimiz için yayın adresidir. Ancak, Bilgi sütununda görünen hedefin IP adresini görüyoruz. Şekilde, 10.10.210.1 ile başlayarak altındaki tüm IP adreslerinin MAC adreslerini istediğimizi görebiliriz. Sorduğumuz IP adresine sahip ana bilgisayar, MAC adresiyle birlikte bir ARP yanıtı gönderecek ve bu şekilde çevrimiçi olduğunu bileceğiz.

nmap-PR-sn-AttackBox.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp

Source	Destination	Protocol	Info
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	Who has 10.10.210.11? Tell 10.10.210.6

ARP taramalarından bahsetmişken, ARP sorguları etrafında oluşturulmuş bir tarayıcıdan bahsetmeliyiz: arp-scan; taramanızı özelleştirmek için birçok seçenek sunar. Ayrıntılı bilgi için arp-scan wiki'sini ziyaret edin. Popüler seçeneklerden biri arp-scan --localnet veya basitçe arp-scan -l'dir. Bu komut yerel ağınızdaki tüm geçerli IP adreslerine ARP sorguları gönderecektir. Ayrıca, sisteminizde birden fazla arayüz varsa ve bunlardan birindeki canlı ana bilgisayarları keşfetmekle ilgileniyorsanız, -l kullanarak arayüzü belirtebilirsiniz. Örneğin, sudo arp-scan -l eth0 -l eth0 arayüzündeki tüm geçerli IP adresleri için ARP sorguları gönderecektir.

AttackBox'ta arp-scan'in kurulu olmadığını unutmayın; ancak apt install arp-scan kullanılarak kurulabilir.

Aşağıdaki örnekte, AttackBox'ın alt ağını arp-scan ATTACKBOX_IP/24 kullanarak taradık. Bu taramayı bir öncekine yakın bir zaman diliminde çalıştırduğumuz için nmap -PR -sn ATTACKBOX_IP/24, aynı üç canlı hedefi elde ettik.

```
pentester@TryHackMe$ sudo arp-scan 10.10.210.6/24
Interface: eth0, datalink type: EN10MB (Ethernet)
WARNING: host part of 10.10.210.6/24 is non-zero
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
10.10.210.75 02:83:75:3a:f2:89 (Unknown)
10.10.210.100 02:63:d0:1b:2d:cd (Unknown)
10.10.210.165 02:59:79:4f:17:b7 (Unknown)

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 2.726 seconds (93.91 hosts/sec). 3 responded
```

Benzer şekilde, arp-scan komutu tcpdump, Wireshark veya benzer bir araç kullanarak görebileceğimiz birçok ARP sorgusu oluşturacaktır. arp-scan ve nmap -PR -sn için paket yakalamanın benzer trafik modelleri verdiğini fark edebiliriz. Wireshark çıktısı aşağıdadır.

arp-scan-AttackBox.pcapng			
Source	Destination	Protocol	Info
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.0? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.1? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.2? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.3? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.4? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.5? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	ARP Announcement for 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.7? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.8? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.9? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.10? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.11? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.12? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.13? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.14? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.15? Tell 10.10.210.6
02:ba:eb:d6:18:2b	Broadcast	ARP	who has 10.10.210.16? Tell 10.10.210.6

Ağ simülörünü kapattıysanız, tekrar görüntülemek için Görev 2'deki "Siteyi Ziyaret Et" düğmesine tıklayın.

Aşağıdaki seçeneklerle broadcast ARP Requests paketleri göndereceğiz:

- Bilgisayar1'den
- Bilgisayar1'e (yayın olduğunu belirtmek için)
- Paket Türü: "ARP İsteği"
- Veri: agdaki tüm olası sekiz cihazı (bilgisayar1 dışında) deneyin: bilgisayar2, bilgisayar3, bilgisayar4, bilgisayar5, bilgisayar6, anahtar1, anahtar2 ve yönlendirici.

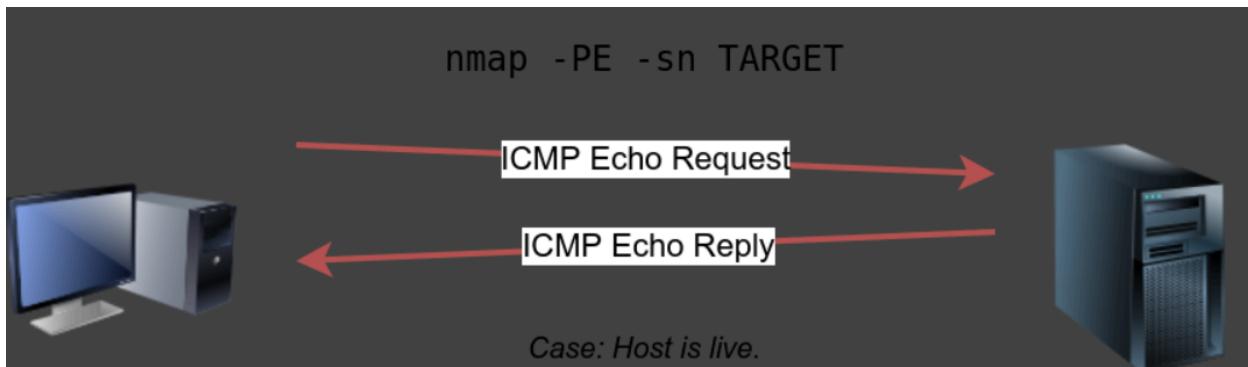
Soru⇒ ARP isteklerini kullanarak kaç cihaz keşfediniz?

Cevap ⇒ 3

Task 6 Nmap Host Discovery Using ICMP (Görev 6 ICMP Kullanarak Nmap Ana Bilgisayar Bulma)

Hedef ağdaki her IP adresine ping atabilir ve ping (ICMP Tip 8/Echo) isteklerimize kimlerin ping yanıtını (ICMP Tip 0) verdiğiğini görebiliriz. Basit, değil mi? Bu en basit yaklaşım olsa da, her zaman güvenilir değildir. Birçok güvenlik duvarı ICMP echo'yu engeller; MS Windows'un yeni sürümleri varsayılan olarak ICMP echo isteklerini engelleyen bir ana bilgisayar güvenlik duvarı ile yapılandırılmıştır. Hedefiniz aynı alt ağ üzerindeyse ARP sorgusunun ICMP isteğinden önce geleceğini unutmayın.

Canlı ana bilgisayarları keşfetmek üzere ICMP yanıtını kullanmak için -PE seçeneğini ekleyin. (Bunu bir port taraması ile takip etmek istemiyorsanız -sn eklemeyi unutmayın.) Aşağıdaki şekilde gösterildiği gibi, ICMP yanıt taraması bir ICMP yanıt isteği göndererek çalışır ve hedefin çevrimiçi olması durumunda bir ICMP yanıt yanıt ile yanıt vermesini bekler.



Aşağıdaki örnekte, nmap -PE -sn MACHINE_IP/24 kullanarak hedefin alt ağını taradık. Bu tarama alt ağdaki her IP adresine ICMP eko paketleri gönderecektir. Yine, canlı ana bilgisayarların yanıt vermesini bekliyoruz; ancak, birçok güvenlik duvarının ICMP'yi engellediğini hatırlamak akıllıca olacaktır. Aşağıdaki çıktı, sanal makinenin C sınıfı alt ağının AttackBox'tan sudo nmap -PE -sn MACHINE_IP/24 kullanılarak taramasının sonucunu göstermektedir.

```
pentester@TryHackMe$ sudo nmap -PE -sn 10.10.68.220/24Starting Nmap 7.60 ( https://nmap.org ) at 2021-09-02 10:16 BST
Nmap scan report for ip-10-10-68-50.eu-west-1.compute.internal (10.10.68.5)
```

```
0)
Host is up (0.00017s latency).
MAC Address: 02:95:36:71:5B:87 (Unknown)
Nmap scan report for ip-10-10-68-52.eu-west-1.compute.internal (10.10.68.5
2)
Host is up (0.00017s latency).
MAC Address: 02:48:E8:BF:78:E7 (Unknown)
Nmap scan report for ip-10-10-68-77.eu-west-1.compute.internal (10.10.68.77)
Host is up (-0.100s latency).
MAC Address: 02:0F:0A:1D:76:35 (Unknown)
Nmap scan report for ip-10-10-68-110.eu-west-1.compute.internal (10.10.68.11
0)
Host is up (-0.10s latency).
MAC Address: 02:6B:50:E9:C2:91 (Unknown)
Nmap scan report for ip-10-10-68-140.eu-west-1.compute.internal (10.10.68.14
0)
Host is up (0.00021s latency).
MAC Address: 02:58:59:63:0B:6B (Unknown)
Nmap scan report for ip-10-10-68-142.eu-west-1.compute.internal (10.10.68.14
2)
Host is up (0.00016s latency).
MAC Address: 02:C6:41:51:0A:0F (Unknown)
Nmap scan report for ip-10-10-68-220.eu-west-1.compute.internal (10.10.68.2
20)
Host is up (0.00026s latency).
MAC Address: 02:25:3F:DB:EE:0B (Unknown)
Nmap scan report for ip-10-10-68-222.eu-west-1.compute.internal (10.10.68.2
22)
Host is up (0.00025s latency).
MAC Address: 02:28:B1:2E:B0:1B (Unknown)
Nmap done: 256 IP addresses (8 hosts up) scanned in 2.11 seconds
```

Tarama çıktısı sekiz ana bilgisayarın açık olduğunu gösteriyor; dasası, MAC adreslerini de gösteriyor. Genel olarak, sistemimizle aynı alt ağda olmadıkları sürece hedeflerin MAC adreslerini öğrenmeyi beklemiyoruz. Yukarıdaki çıktı, Nmap'in ICMP paketleri göndermesine gerek olmadığını, çünkü aldığı ARP

yanıtlarına dayanarak bu ana bilgisayarların açık olduğunu doğruladığını göstermektedir.

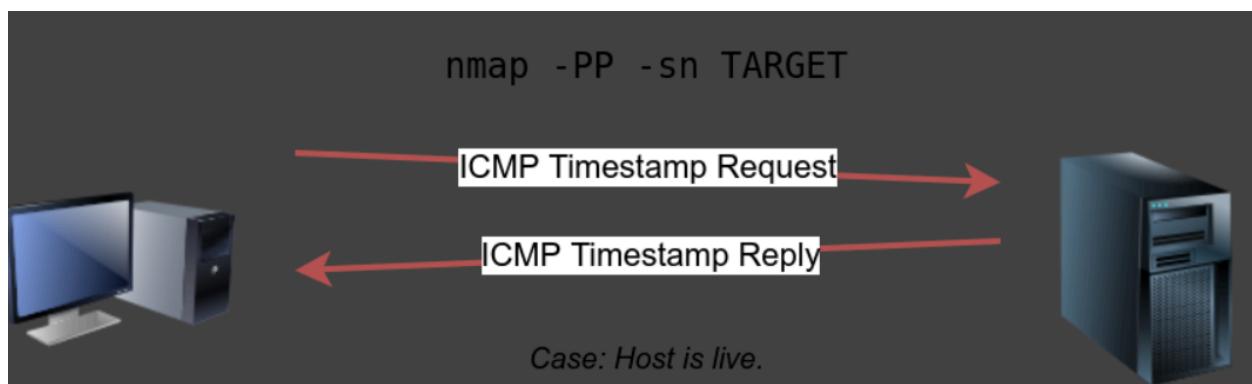
Yukarıdaki taramayı tekrarlayacağız; ancak bu kez farklı bir alt ağa ait bir sistemden tarama yapacağız. Sonuçlar benzerdir ancak MAC adresleri yoktur.

```
pentester@TryHackMe$ sudo nmap -PE -sn 10.10.68.220/24Starting Nmap 7.  
92 ( https://nmap.org ) at 2021-09-02 12:16 EEST  
Nmap scan report for 10.10.68.50  
Host is up (0.12s latency).  
Nmap scan report for 10.10.68.52  
Host is up (0.12s latency).  
Nmap scan report for 10.10.68.77  
Host is up (0.11s latency).  
Nmap scan report for 10.10.68.110  
Host is up (0.11s latency).  
Nmap scan report for 10.10.68.140  
Host is up (0.11s latency).  
Nmap scan report for 10.10.68.142  
Host is up (0.11s latency).  
Nmap scan report for 10.10.68.220  
Host is up (0.11s latency).  
Nmap scan report for 10.10.68.222  
Host is up (0.11s latency).  
Nmap done: 256 IP addresses (8 hosts up) scanned in 8.26 seconds
```

Wireshark gibi bir araç kullanarak ağ paketlerine bakarsanız, aşağıdaki görüntüye benzer bir şey göreceksiniz. Hedef alt ağdan farklı bir alt ağıda bir kaynak IP adresimiz olduğunu ve hangisinin yanıt vereceğini görmek için hedef alt ağdaki tüm IP adreslerine ICMP yanıt istekleri gönderdiğini görebilirsiniz.

nmap-PE-sn-openvpn.pcapng				
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help				
A series of small icons representing network analysis functions like packet capture, filtering, and analysis.				
icmp				
Source	Destination	Protocol	Info	
10.11.35.214	10.10.68.1	ICMP	Echo (ping) request id=0x22e1, seq=0/0, ttl=	
10.11.35.214	10.10.68.2	ICMP	Echo (ping) request id=0xd13b, seq=0/0, ttl=	
10.11.35.214	10.10.68.3	ICMP	Echo (ping) request id=0x65c8, seq=0/0, ttl=	
10.11.35.214	10.10.68.4	ICMP	Echo (ping) request id=0x2b62, seq=0/0, ttl=	
10.11.35.214	10.10.68.5	ICMP	Echo (ping) request id=0x8681, seq=0/0, ttl=	
10.11.35.214	10.10.68.6	ICMP	Echo (ping) request id=0x6a13, seq=0/0, ttl=	
10.11.35.214	10.10.68.7	ICMP	Echo (ping) request id=0x2dbc, seq=0/0, ttl=	
10.11.35.214	10.10.68.8	ICMP	Echo (ping) request id=0x2029, seq=0/0, ttl=	
10.11.35.214	10.10.68.9	ICMP	Echo (ping) request id=0xf800, seq=0/0, ttl=	
10.11.35.214	10.10.68.10	ICMP	Echo (ping) request id=0xca62, seq=0/0, ttl=	
10.11.35.214	10.10.68.1	ICMP	Echo (ping) request id=0xe95f, seq=0/0, ttl=	
10.11.35.214	10.10.68.2	ICMP	Echo (ping) request id=0x896e, seq=0/0, ttl=	
10.11.35.214	10.10.68.3	ICMP	Echo (ping) request id=0xdffe, seq=0/0, ttl=	
10.11.35.214	10.10.68.4	ICMP	Echo (ping) request id=0xdf2c, seq=0/0, ttl=	
10.11.35.214	10.10.68.5	ICMP	Echo (ping) request id=0x4602, seq=0/0, ttl=	
10.11.35.214	10.10.68.6	ICMP	Echo (ping) request id=0xd84a, seq=0/0, ttl=	
10.11.35.214	10.10.68.7	ICMP	Echo (ping) request id=0x90dc, seq=0/0, ttl=	

ICMP yanıt istekleri engellenme eğiliminde olduğundan, bir sistemin çevrimiçi olup olmadığını anlamak için ICMP Zaman Damgası veya ICMP Adres Maskesi isteklerini de düşünebilirsiniz. Nmap zaman damgası isteği (ICMP Tip 13) kullanır ve bir Zaman Damgası yanıtı (ICMP Tip 14) alıp almayacağını kontrol eder. PP seçeneğinin eklenmesi Nmap'e ICMP zaman damgası isteklerini kullanmasını söyler. Aşağıdaki şekilde gösterildiği gibi, canlı ana bilgisayarların yanıt vermesini beklersiniz.



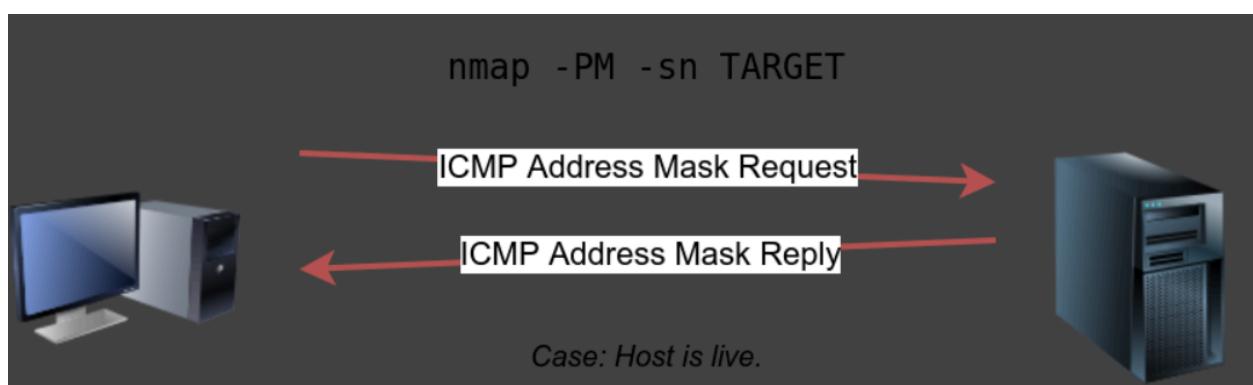
Aşağıdaki örnekte, hedef makine alt ağındaki çevrimiçi bilgisayarları keşfetmek için nmap -PP -sn MACHINE_IP/24 çalıştırıyoruz.

```
pentester@TryHackMe$ sudo nmap -PP -sn 10.10.68.220/24Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 12:06 EEST
Nmap scan report for 10.10.68.50
Host is up (0.13s latency).
Nmap scan report for 10.10.68.52
Host is up (0.25s latency).
Nmap scan report for 10.10.68.77
Host is up (0.14s latency).
Nmap scan report for 10.10.68.110
Host is up (0.14s latency).
Nmap scan report for 10.10.68.140
Host is up (0.15s latency).
Nmap scan report for 10.10.68.209
Host is up (0.14s latency).
Nmap scan report for 10.10.68.220
Host is up (0.14s latency).
Nmap scan report for 10.10.68.222
Host is up (0.14s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 10.93 seconds
```

Önceki ICMP taramasına benzer şekilde, bu tarama hedef alt ağdaki her geçerli IP adresine birçok ICMP zaman damgası isteği gönderecektir. Aşağıdaki Wireshark ekran görüntüsünde, bir kaynak IP adresinin çevrimiçi ana bilgisayarları keşfetmek için mümkün olan her IP adresine ICMP paketleri gönderdiğini görebilirsiniz.

nmap-PP-sn-openvpn.pcapng					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
A series of small icons representing network analysis functions like packet capture, filtering, and analysis.					
icmp					
Source	Destination	Protocol	Info		
10.11.35.214	10.10.68.1	ICMP	Timestamp request	id=0xb6bf, seq=0/0, ttl=	
10.11.35.214	10.10.68.2	ICMP	Timestamp request	id=0xcad3, seq=0/0, ttl=	
10.11.35.214	10.10.68.3	ICMP	Timestamp request	id=0x53ce, seq=0/0, ttl=	
10.11.35.214	10.10.68.4	ICMP	Timestamp request	id=0x0149, seq=0/0, ttl=	
10.11.35.214	10.10.68.5	ICMP	Timestamp request	id=0x2ead, seq=0/0, ttl=	
10.11.35.214	10.10.68.6	ICMP	Timestamp request	id=0x3ce5, seq=0/0, ttl=	
10.11.35.214	10.10.68.7	ICMP	Timestamp request	id=0x5de2, seq=0/0, ttl=	
10.11.35.214	10.10.68.8	ICMP	Timestamp request	id=0x884d, seq=0/0, ttl=	
10.11.35.214	10.10.68.9	ICMP	Timestamp request	id=0xbff35, seq=0/0, ttl=	
10.11.35.214	10.10.68.10	ICMP	Timestamp request	id=0x6b44, seq=0/0, ttl=	
10.11.35.214	10.10.68.1	ICMP	Timestamp request	id=0x1a28, seq=0/0, ttl=	
10.11.35.214	10.10.68.2	ICMP	Timestamp request	id=0x8586, seq=0/0, ttl=	
10.11.35.214	10.10.68.3	ICMP	Timestamp request	id=0xacce, seq=0/0, ttl=	
10.11.35.214	10.10.68.4	ICMP	Timestamp request	id=0x0cf8, seq=0/0, ttl=	
10.11.35.214	10.10.68.5	ICMP	Timestamp request	id=0xa39f, seq=0/0, ttl=	
10.11.35.214	10.10.68.6	ICMP	Timestamp request	id=0x2279, seq=0/0, ttl=	
10.11.35.214	10.10.68.7	ICMP	Timestamp request	id=0x800f, seq=0/0, ttl=	

Benzer şekilde, Nmap adres maskesi sorgularını (ICMP Tip 17) kullanır ve bir adres maskesi yanıtını (ICMP Tip 18) alıpmadığını kontrol eder. Bu tarama -PM seçeneği ile etkinleştirilebilir. Aşağıdaki şekilde gösterildiği gibi, canlı ana bilgisayarların ICMP adres maskesi isteklerine yanıt vermesi beklenir.



ICMP adres maskesi sorgularını kullanarak canlı ana bilgisayarları keşfetmeye çalışmak için nmap -PM -sn MACHINE_IP/24 komutunu çalıştırıyoruz. Daha önceki taramalara dayanarak en az sekiz ana bilgisayarın açık olduğunu bilmemize

rağmen, bu tarama hiçbirini döndürmedi. Bunun nedeni, hedef sistemin ya da rota üzerindeki bir güvenlik duvarının bu tür ICMP paketlerini engellemesidir. Bu nedenle, aynı sonuca ulaşmak için birden fazla yaklaşım öğrenmek önemlidir. Bir paket türü engelleniyorsa, hedef ağı ve hizmetleri keşfetmek için her zaman başka bir paket seçebiliriz.

```
pentester@TryHackMe$ sudo nmap -PM -sn 10.10.68.220/24Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 12:13 EEST
Nmap done: 256 IP addresses (0 hosts up) scanned in 52.17 seconds
```

Herhangi bir yanıt alamamış ve hangi ana bilgisayarların çevrimiçi olduğunu anlayamamış olsak da, bu taramanın her geçerli IP adresine ICMP adres maskesi istekleri gönderdiğini ve bir yanıt beklediğini belirtmek önemlidir. Aşağıdaki ekran görüntüsünde de görebileceğimiz gibi her ICMP isteği iki kez gönderildi.

The screenshot shows a Wireshark capture window titled "nmap-PM-sn-openvpn.pcapng". The "icmp" tab is selected. The table displays 16 rows of ICMP packets, all of which are "Address mask request" type. The "Source" column shows the source IP as 10.11.35.214, and the "Destination" column shows various destination IPs in the 10.10.68.0/24 subnet. The "Protocol" column is labeled "ICMP" and the "Info" column provides detailed information about each request, such as the sequence number (seq=0/0), ttl, and ID.

Source	Destination	Protocol	Info
10.11.35.214	10.10.68.1	ICMP	Address mask request id=0xa3c4, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Address mask request id=0xb793, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request id=0x2d87, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request id=0x091c, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request id=0x692c, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request id=0x4bec, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request id=0x4d61, seq=0/0, ttl=
10.11.35.214	10.10.68.8	ICMP	Address mask request id=0xb84f, seq=0/0, ttl=
10.11.35.214	10.10.68.9	ICMP	Address mask request id=0x7d19, seq=0/0, ttl=
10.11.35.214	10.10.68.10	ICMP	Address mask request id=0x92be, seq=0/0, ttl=
10.11.35.214	10.10.68.1	ICMP	Address mask request id=0xd204, seq=0/0, ttl=
10.11.35.214	10.10.68.2	ICMP	Address mask request id=0x683d, seq=0/0, ttl=
10.11.35.214	10.10.68.3	ICMP	Address mask request id=0x2711, seq=0/0, ttl=
10.11.35.214	10.10.68.4	ICMP	Address mask request id=0xfde3, seq=0/0, ttl=
10.11.35.214	10.10.68.5	ICMP	Address mask request id=0x2eb1, seq=0/0, ttl=
10.11.35.214	10.10.68.6	ICMP	Address mask request id=0x8300, seq=0/0, ttl=
10.11.35.214	10.10.68.7	ICMP	Address mask request id=0x7400, seq=0/0, ttl=

Sorular

Soru ⇒ Nmap'e canlı ana bilgisayarları keşfetmek için ICMP Timestamp kullanmasını söylemek için gereken seçenek nedir?

Cevap ⇒ **-PP**

Soru ⇒ Nmap'e canlı ana bilgisayarları keşfetmek için ICMP Adres Maskesi kullanmasını söylemek için gereken seçenek nedir?

Cevap ⇒ **-PM**

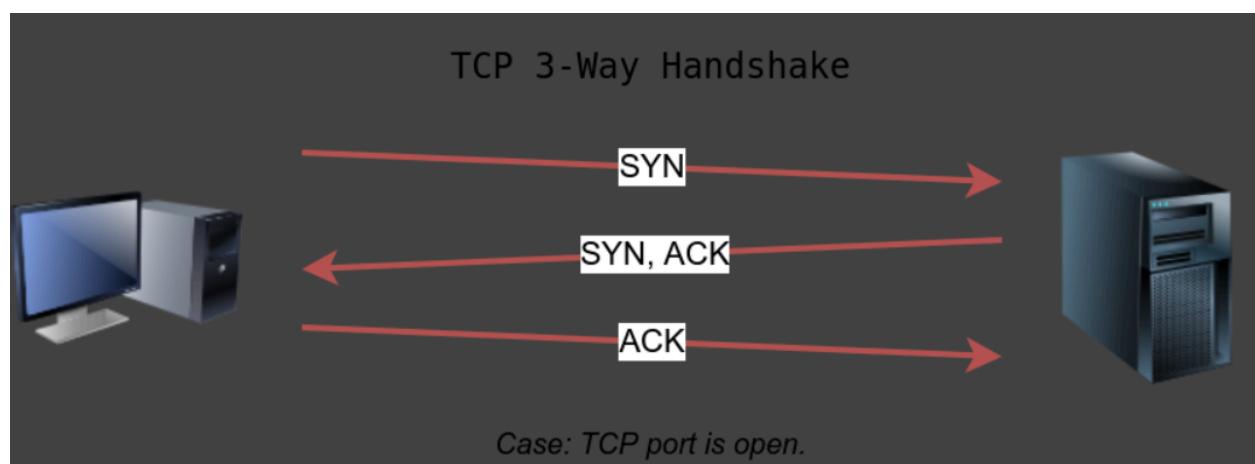
Soru ⇒ Nmap'e canlı ana bilgisayarları keşfetmek için ICMP Echo kullanmasını söylemek için gereken seçenek nedir?

Cevap ⇒ **-PE**

Task 7 Nmap Host Discovery Using TCP and UDP (Görev 7 TCP ve UDP Kullanarak Nmap Ana Bilgisayar Bulma)

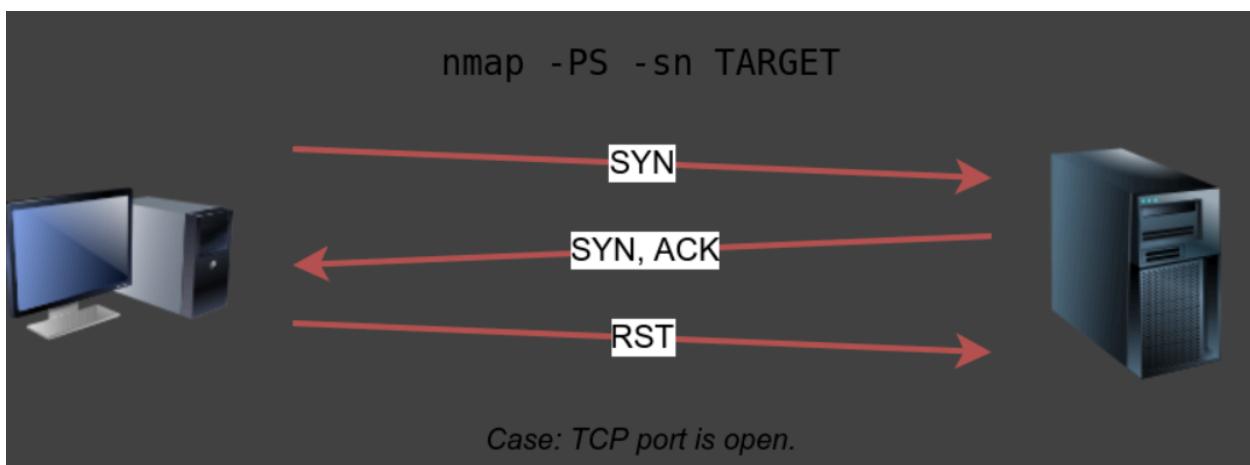
TCP SYN Ping

Varsayılan olarak 80 olan bir TCP portuna SYN (Senkronize Et) bayrağı ayarlanmış bir paket gönderebilir ve yanıt bekleyebiliriz. Açık bir port SYN/ACK (Acknowledge) ile yanıt vermelidir; kapalı bir port ise RST (Reset) ile sonuçlanacaktır. Bu durumda, ana bilgisayarın açık olup olmadığını anlamak için yalnızca herhangi bir yanıt alıp almayacağımızı kontrol ederiz. Portun özel durumu burada önemli değildir. Aşağıdaki şekil, TCP 3 yönlü el sıkışmasının genellikle nasıl çalıştığını hatırlatır.



Nmap'in TCP SYN kullanmasını istiyorsanız, bunu -PS seçeneğini ve ardından port numarası, aralığı, listesi veya bunların bir kombinasyonunu kullanarak yapabilirsiniz. Örneğin, -PS21 21 numaralı portu hedeflerken, -PS21-25 21, 22, 23, 24 ve 25 numaralı portları hedefleyecektir. Son olarak -PS80,443,8080, 80, 443 ve 8080 numaralı üç bağlantı noktasını hedefleyecektir.

Ayrıcalıklı kullanıcılar (root ve sudoers) TCP SYN paketleri gönderebilir ve aşağıdaki şekilde gösterildiği gibi port açık olsa bile TCP 3 yönlü el sıkışmasını tamamlamaları gerekmez. Ayrıcalıklı olmayan kullanıcıların, bağlantı noktası açıksa 3 yönlü el sıkışmayı tamamlamaktan başka seçeneği yoktur.



Hedef VM alt ağını taramak için nmap -PS -sn MACHINE_IP/24 komutunu çalıştıracağınız. Aşağıdaki çıktıda görebileceğimiz gibi, beş ana bilgisayar keşfedebildik.

```
pentester@TryHackMe$ sudo nmap -PS -sn 10.10.68.220/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 13:45 EEST
Nmap scan report for 10.10.68.52
Host is up (0.10s latency).

Nmap scan report for 10.10.68.121
Host is up (0.16s latency).

Nmap scan report for 10.10.68.125
Host is up (0.089s latency).

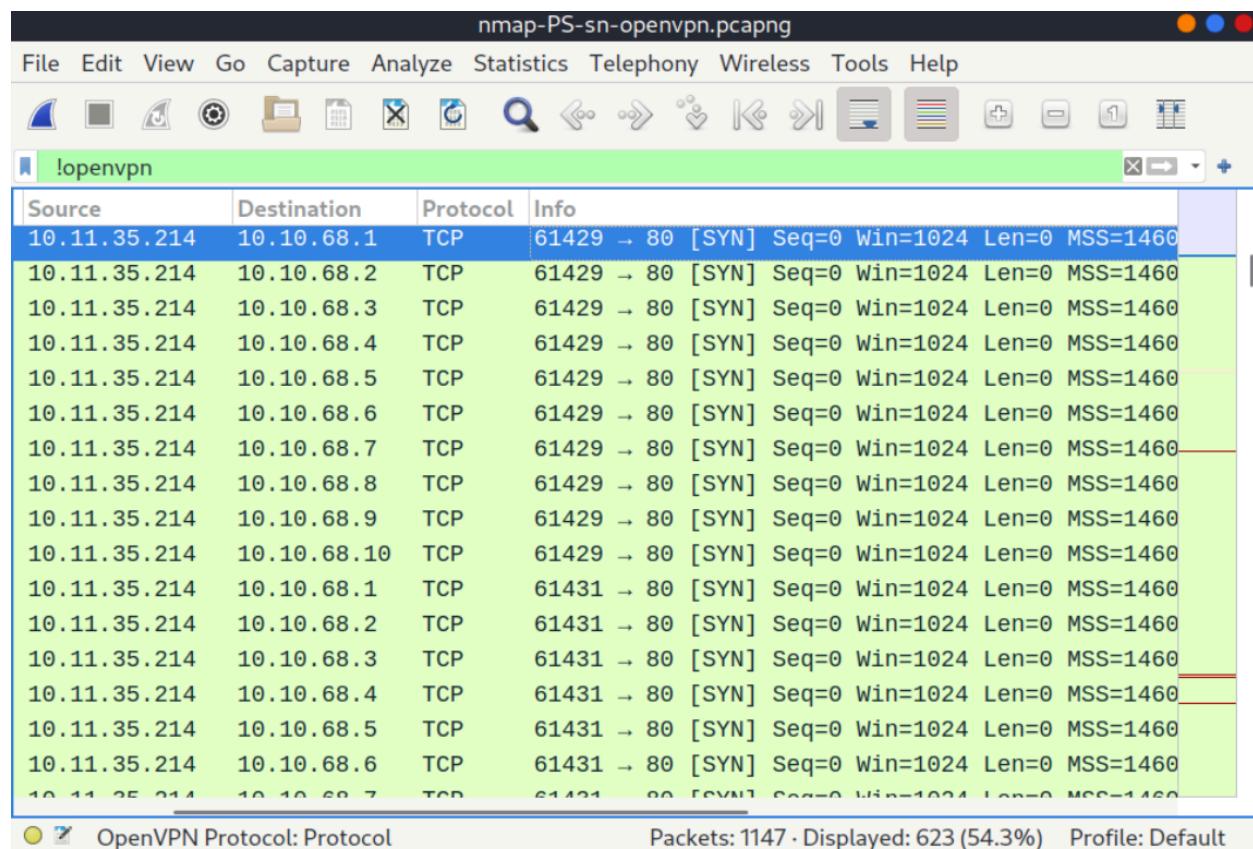
Nmap scan report for 10.10.68.134
Host is up (0.13s latency).

Nmap scan report for 10.10.68.220
```

Host is up (0.11s latency).

Nmap done: 256 IP addresses (5 hosts up) scanned in 17.38 seconds

Aşağıdaki şekilde Wireshark üzerindeki ağ trafigine bakarak perde arkasında neler olduğuna daha yakından bakalım. Teknik olarak konuşmak gereklidir, TCP ping taramasında kullanılacak herhangi bir TCP portu belirtmediğimiz için, Nmap ortak portları kullandı; bu durumda, TCP portu 80'dir. Port 80'i dinleyen herhangi bir hizmetin yanıt vermesi beklenir, bu da dolaylı olarak ana bilgisayarın çevrimiçi olduğunu gösterir.

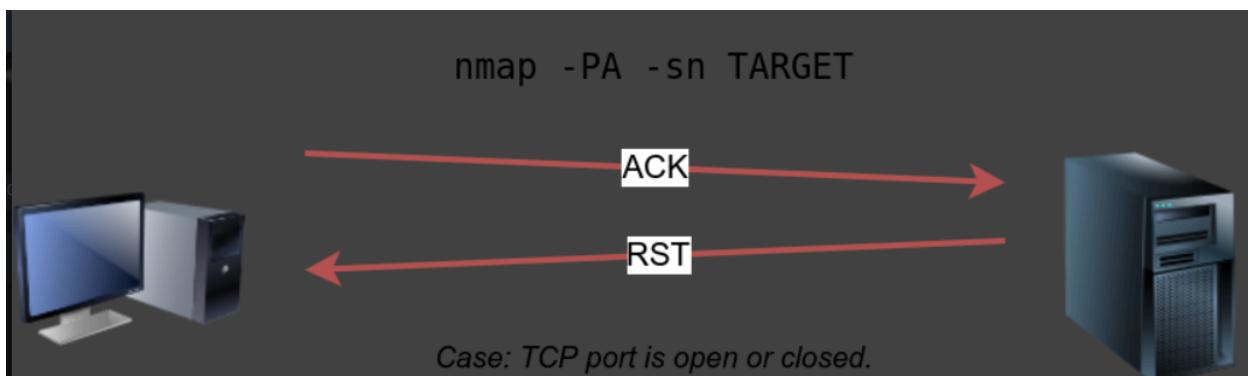


TCP ACK Ping

Tahmin ettiğiniz gibi, bu ACK bayrağı ayarlanmış bir paket gönderir. Bunu yapabilmek için Nmap'i ayrıcalıklı bir kullanıcı olarak çalıştırıyor olmanız gereklidir. Eğer bunu ayrıcalıksız bir kullanıcı olarak denerseniz, Nmap 3 yönlü bir el sıkışma deneyecektir.

Varsayılan olarak 80 numaralı bağlantı noktası kullanılır. Söz dizimi TCP SYN ping'e benzer. -PA'nın ardından bir bağlantı noktası numarası, aralığı, listesi veya bunların bir kombinasyonu gelmelidir. Örneğin, -PA21, -PA21-25 ve -PA80,443,8080'i düşünün. Herhangi bir bağlantı noktası belirtilmezse, 80 numaralı bağlantı noktası kullanılacaktır.

Aşağıdaki şekil, ACK bayrağına sahip herhangi bir TCP paketinin RST bayrağı ayarlanmış bir TCP paketi ile geri dönmesi gerektiğini göstermektedir. ACK bayraklı TCP paketi devam eden herhangi bir bağlantının parçası olmadığı için hedef RST bayrağı ayarlı olarak yanıt verir. Beklenen yanıt, hedef ana bilgisayarın açık olup olmadığını tespit etmek için kullanılır.



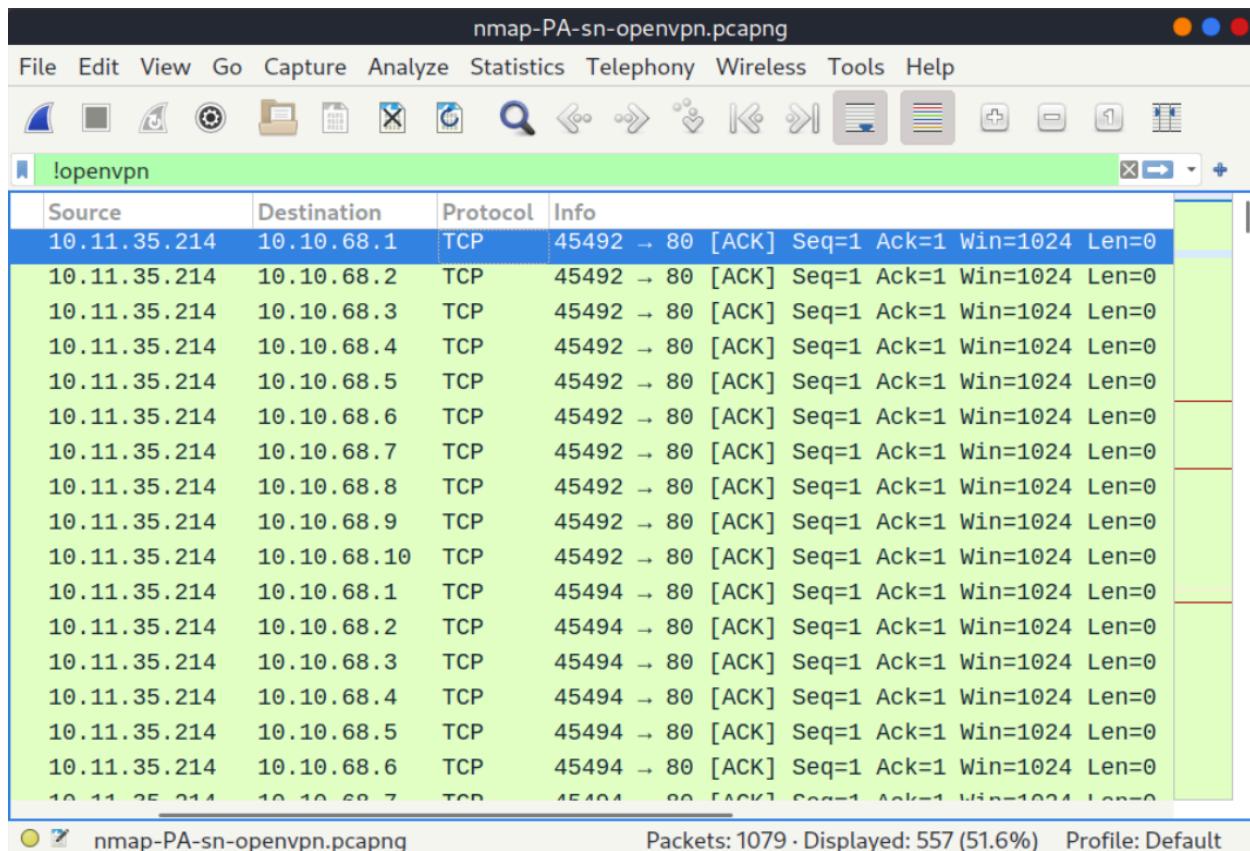
Bu örnekte, hedefin alt ağındaki çevrimiçi ana bilgisayarları keşfetmek için sudo nmap -PA -sn MACHINE_IP/24 komutunu çalıştırıyoruz. TCP ACK ping taramasının beş ana bilgisayarı açık olarak algıladığını görebiliriz.

```
pentester@TryHackMe$ sudo nmap -PA -sn 10.10.68.220/24
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 13:46 EEST
Nmap scan report for 10.10.68.52
Host is up (0.11s latency).
Nmap scan report for 10.10.68.121
Host is up (0.12s latency).
Nmap scan report for 10.10.68.125
Host is up (0.10s latency).
Nmap scan report for 10.10.68.134
Host is up (0.10s latency).
Nmap scan report for 10.10.68.220
```

Host is up (0.10s latency).

Nmap done: 256 IP addresses (5 hosts up) scanned in 29.89 seconds

Aşağıdaki şekilde gösterildiği gibi ağ trafiğine göz atarsak, ACK bayrağı ayarlanmış ve hedef sistemlerin 80 numaralı portuna gönderilen birçok paket keşfedeceğiz. Nmap her paketi iki kez gönderir. Yanıt vermeyen sistemler çevrimdışı veya erişilemez durumdadır.

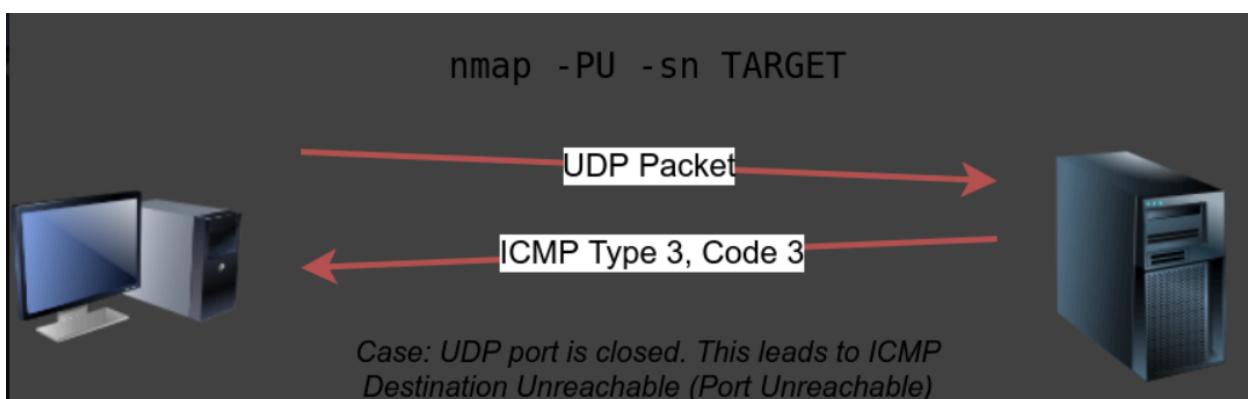
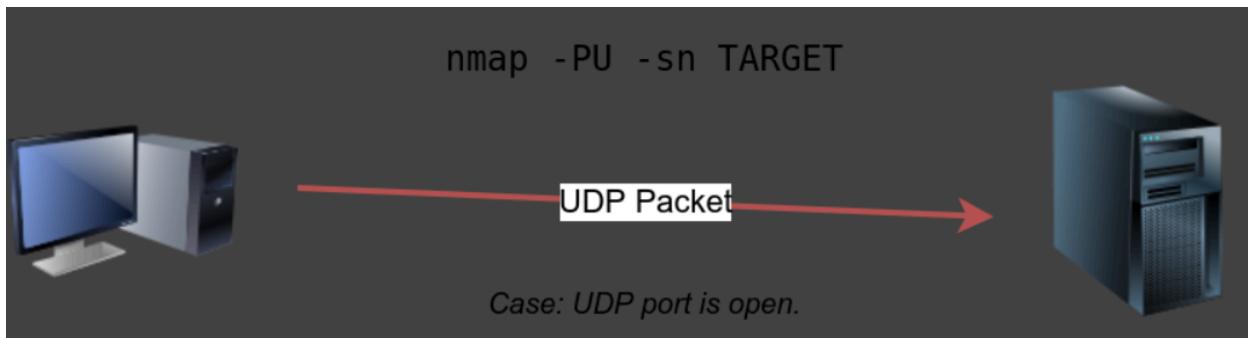


UDP Ping

Son olarak, ana bilgisayarın çevrimiçi olup olmadığını keşfetmek için UDP'yi kullanabiliyoruz. TCP SYN ping'in aksine, açık bir porta UDP paketi göndermenin herhangi bir yanıt vermesi beklenmez. Ancak, kapalı bir UDP portuna bir UDP paketi gönderirsek, bir ICMP portuna ulaşamıyor paketi almayı bekleriz; bu, hedef sistemin açık ve kullanılabilir olduğunu gösterir.

Aşağıdaki şekilde, açık bir UDP portuna gönderilen ve herhangi bir yanıtı tetiklemeyen bir UDP paketi görüyoruz. Ancak, herhangi bir kapalı UDP portuna bir

UDP paketi göndermek, dolaylı olarak hedefin çevrimiçi olduğunu gösteren bir yanıtı tetikleyebilir.



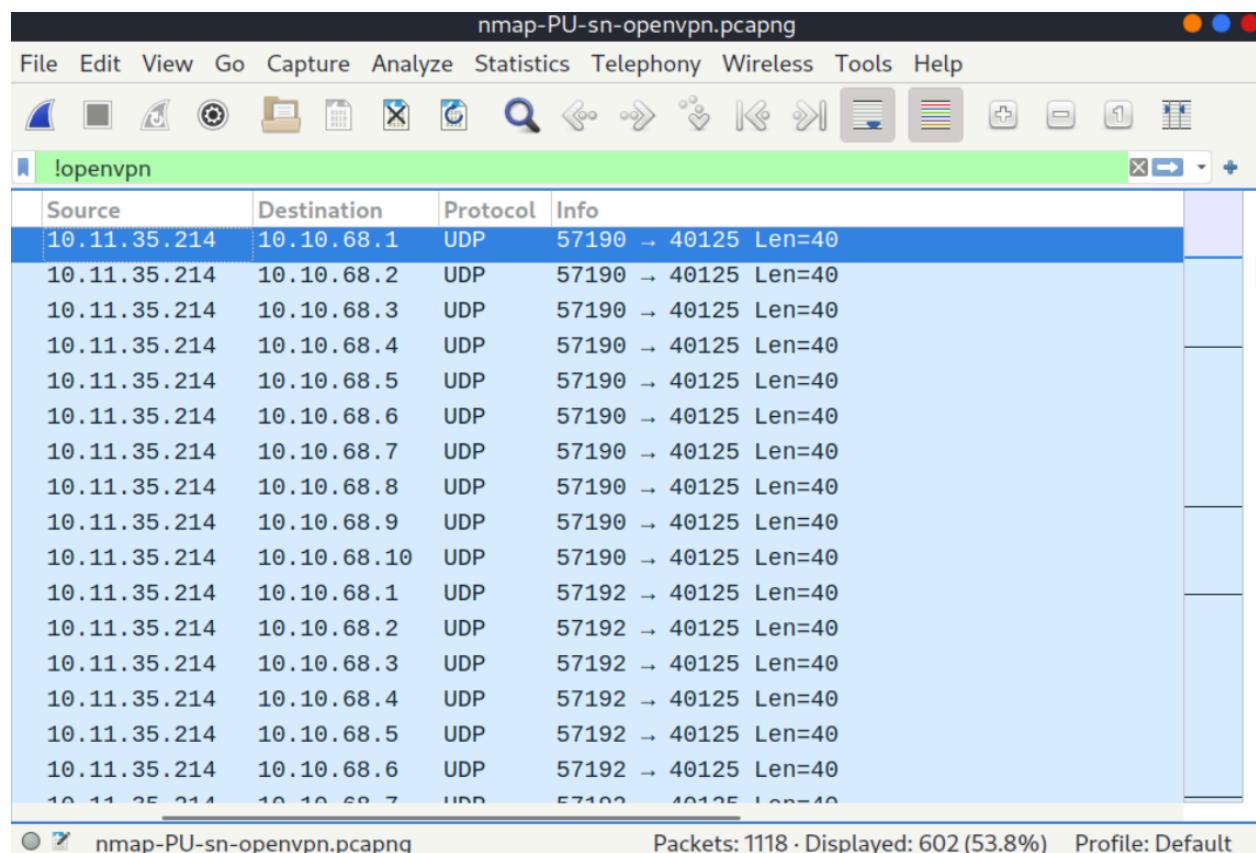
Portları belirtmek için kullanılan sözdizimi TCP SYN ping ve TCP ACK ping'e benzer; Nmap UDP ping için -PU kullanır. Aşağıdaki örnekte, bir UDP taraması kullanıyoruz ve beş canlı ana bilgisayar keşfetiyoruz.

```
pentester@TryHackMe$ sudo nmap -PU -sn 10.10.68.220/24Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-02 13:45 EEST
Nmap scan report for 10.10.68.52
Host is up (0.10s latency).
Nmap scan report for 10.10.68.121
Host is up (0.10s latency).
Nmap scan report for 10.10.68.125
Host is up (0.14s latency).
Nmap scan report for 10.10.68.134
Host is up (0.096s latency).
Nmap scan report for 10.10.68.220
```

```
Host is up (0.11s latency).
```

```
Nmap done: 256 IP addresses (5 hosts up) scanned in 9.20 seconds
```

Üretilen UDP paketlerini inceleyelim. Aşağıdaki Wireshark ekran görüntüsünde, Nmap'in büyük olasılıkla kapalı olan UDP portlarına UDP paketleri gönderdiğini görüyoruz. Aşağıdaki görüntü Nmap'in ICMP hedefe ulaşılamıyor (port unreachable) hmasını tetiklemek için yaygın olmayan bir UDP portu kullandığını göstermektedir.



Masscan

Bu arada, Masscan mevcut sistemleri keşfetmek için benzer bir yaklaşım kullanır. Bununla birlikte, ağ taramasını hızlı bir şekilde bitirmek için, Masscan ürettiği paketlerin oranı konusunda oldukça agresiftir. Söz dizimi oldukça benzerdir: -p'nin ardından bir bağlantı noktası numarası, liste veya aralık gelebilir. Aşağıdaki örnekleri göz önünde bulundurun:

- masscan MACHINE_IP/24 -p443

- `masscan MACHINE_IP/24 -p80,443`
- `masscan MACHINE_IP/24 -p22-25`
- `masscan MACHINE_IP/24 --top-ports 100`

Masscan AttackBox üzerinde kurulu değildir; ancak apt install masscan kullanılarak kurulabilir.

Sorular

Soru ⇒ Hangi TCP ping taraması ayrıcalıklı bir hesap gerektirmez?

Cevap ⇒ [TCP SYN Ping](#)

Soru ⇒ Hangi TCP ping taraması ayrıcalıklı bir hesap gerektirir?

Cevap ⇒ [TCP ACK Ping](#)

Soru ⇒ Telnet portunda TCP SYN ping taraması yapmak için Nmap'e hangi seçeneği eklemeniz gereklidir (İpucu ⇒ Telnet 23 numaralı bağlantı noktasını kullanır)?

Cevap ⇒ [-PS23](#)

Task 8 Using Reverse-DNS Lookup (Görev 8 Ters-DNS Aramasını Kullanma)

Nmap'in varsayılan davranışları ters-DNS çevrimiçi ana bilgisayarları kullanmaktadır. Ana bilgisayar adları çok şey ortaya çıkarabileceğinden, bu yararlı bir adım olabilir. Ancak, bu tür DNS sorguları göndermek istemiyorsanız, bu adımı atlamak için `-n` kullanırsınız.

Varsayılan olarak, Nmap çevrimiçi ana bilgisayarları arayacaktır; ancak, çevrimdışı ana bilgisayarlar için bile DNS sunucusunu sorgulamak için `-R` seçeneğini kullanabilirsiniz. Belirli bir DNS sunucusu kullanmak istiyorsanız, `--dns-servers DNS_SERVER` seçeneğini ekleyebilirsiniz.

Soru ⇒ Nmap'in bir alt ağdaki tüm olası ana bilgisayarlar için bir ters DNS araması yapmasını istiyoruz, isimlerden bazı bilgiler elde etmeyi umuyoruz. Hangi seçeneği eklemeliyiz?

Cevap ⇒ [-R](#)

Task 9 Summary (Görev 9 Özeti)

Bu odayı tamamlayarak ARP, ICMP, TCP ve UDP'nin canlı ana bilgisayarları nasıl tespit edebileceğini öğrendiniz. Bir ana bilgisayardan gelen herhangi bir yanıt, çevrimiçi olduğunun bir göstergesidir. Aşağıda, Nmap için ele aldığımız komut satırı seçeneklerinin hızlı bir özeti bulunmaktadır.

Scan Type	Example Command
ARP Scan	<code>sudo nmap -PR -sn MACHINE_IP/24</code>
ICMP Echo Scan	<code>sudo nmap -PE -sn MACHINE_IP/24</code>
ICMP Timestamp Scan	<code>sudo nmap -PP -sn MACHINE_IP/24</code>
ICMP Address Mask Scan	<code>sudo nmap -PM -sn MACHINE_IP/24</code>
TCP SYN Ping Scan	<code>sudo nmap -PS22,80,443 -sn MACHINE_IP/30</code>
TCP ACK Ping Scan	<code>sudo nmap -PA22,80,443 -sn MACHINE_IP/30</code>
UDP Ping Scan	<code>sudo nmap -PU53,161,162 -sn MACHINE_IP/30</code>

Eğer port taraması yapmadan sadece host keşfi ile ilgileniyorsanız `-sn` eklemeyi unutmayın. `sn`'yi atlamak, Nmap'in varsayılan olarak canlı ana bilgisayarları port taramasına izin verecektir.

Option	Purpose
<code>-n</code>	no DNS lookup
<code>-R</code>	reverse-DNS lookup for all hosts
<code>-sn</code>	host discovery only

Soru ⇒ Bu odada açıklanan tüm Nmap seçeneklerini not aldiğinizden emin olun. Nmap hakkında bilgi edinmeye devam etmek için, lütfen temel port tarama türlerini tanıtan Nmap Temel Port Taramaları odasına katılın.

Cevap ⇒ Cevap Gerekmemektedir.