Nmap Advanced Port Scans

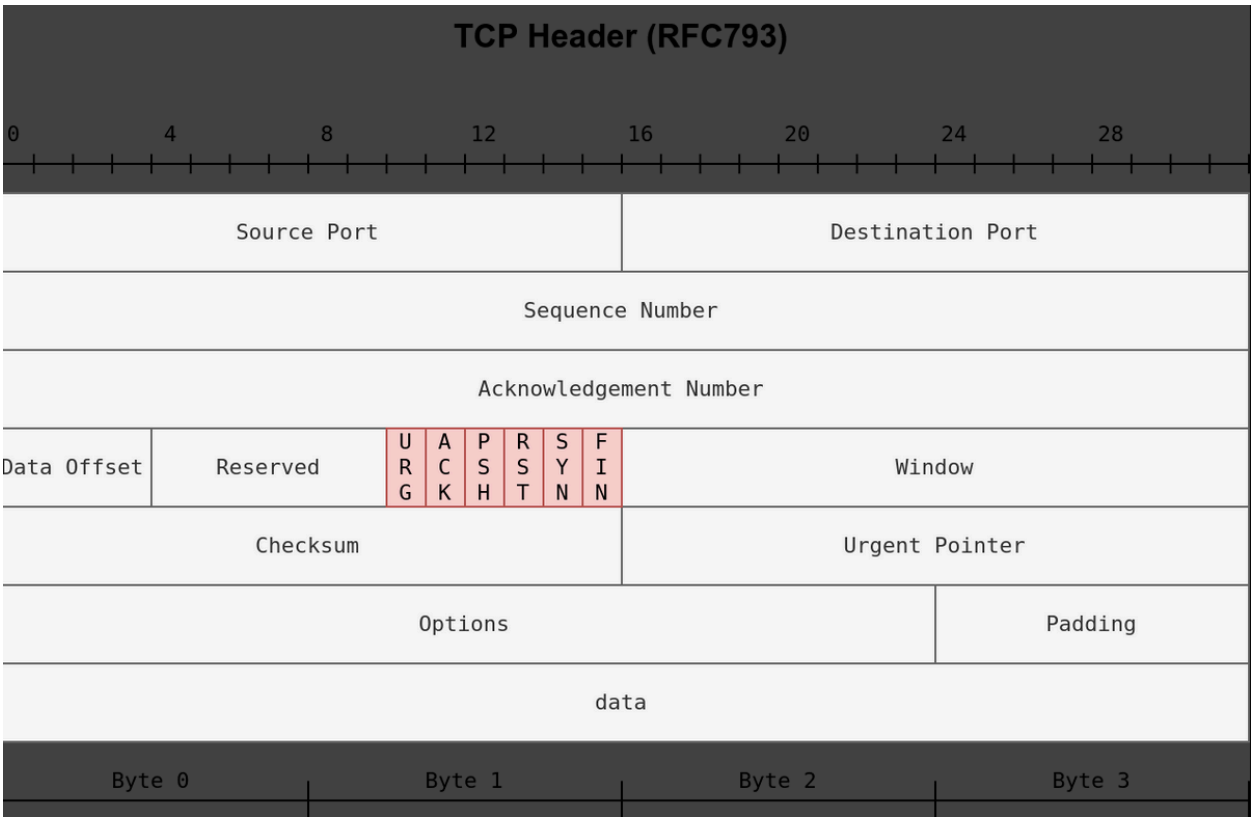
Task 1 Introduction (Görev 1 Giriş)

Bu oda, Nmap serisinin (Ağ Güvenliğine Giriş modülünün bir parçası) üçüncü odasıdır. İlk iki odada, canlı konak keşfi ve temel port taramaları hakkında bilgi edinmiştik.

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)

Nmap Temel Port Taramalarında, TCP bayraklarını ele aldık ve TCP 3 yönlü el sıkışmasını inceledik. Bir bağlantıyı başlatmak için TCP ilk paketin SYN bayrağına sahip olmasını gerektirir. Sonuç olarak, aldığımız yanıta göre bir TCP portunun açık olup olmadığını anlayabiliriz.

Güvenlik araştırmacıları ve hackerlar aşağıdaki şekilde gösterilen ve bir önceki odada açıklanan TCP bayrakları üzerinde düşündüler ve denemeler yapmaya başladılar. Devam eden herhangi bir TCP bağlantısının parçası olmayan bir TCP paketini bir veya daha fazla bayrak ayarlı olarak gönderirsek ne olacağını bilmek istediler.



Örneğin, alınan verileri onaylamak istediğinizde bir ACK bayrağı ayarlanır. Bir ACK taraması, ilk etapta ne gönderilen ne de alınan verileri onaylamaya çalışmak gibidir. Şu basit benzetmeyi düşünün, siz hiçbir şey söylememişken birisi size birdenbire gelip "evet, sizi duyuyorum, lütfen devam edin" diyor.

Bu odada gelişmiş tarama türleri ve tarama seçenekleri açıklanmaktadır. Bu tarama türlerinden bazıları belirli sistemlere karşı yararlı olabilirken, diğerleri belirli ağ kurulumlarında yararlıdır. Aşağıdaki port tarama türlerini ele alacağız:

- Null Scan
- FIN Scan
- Xmas Scan
- Maimon Scan
- ACK Scan
- Window Scan
- Custom Scan

Ayrıca, aşağıdakileri de ele alacağız:

- Spoofing IP
- Spoofing MAC
- Decoy Scan
- Fragmented Packets
- Idle/Zombie Scan

Güvenlik duvarlarından ve IDS sistemlerinden kaçmak için seçenekleri ve teknikleri tartışacağız. Ayrıca Nmap'ten daha ayrıntılı bilgi almak için seçenekleri de ele alacağız.

Soru ⇒ AttackBox'ı Start AttackBox düğmesini kullanarak başlatın ve farklı sanal makinelere karşı farklı Nmap tarama türlerini denemeye hazır olun.

Cevap ⇒ Cevap Gerekmemektedir.

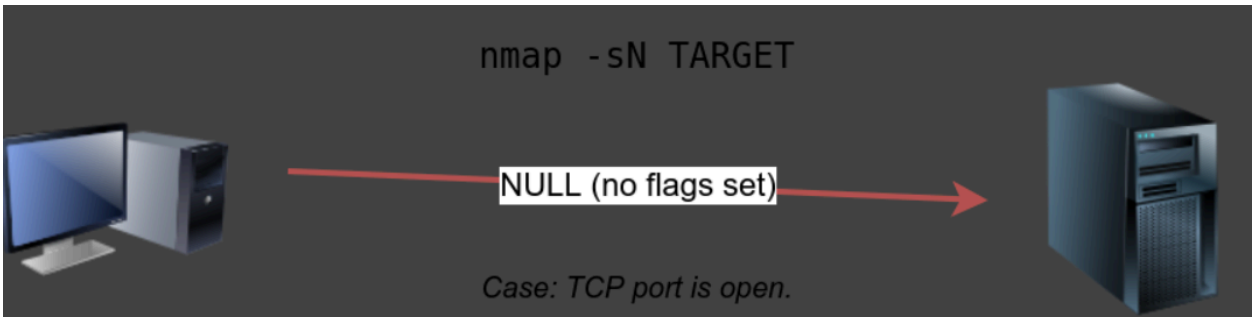
Task 2 TCP Null Scan, FIN Scan, and Xmas Scan (Görev 2 TCP Null Taraması, FIN Taraması ve Xmas Taraması)

Aşağıdaki üç tarama türü ile başlayalım:

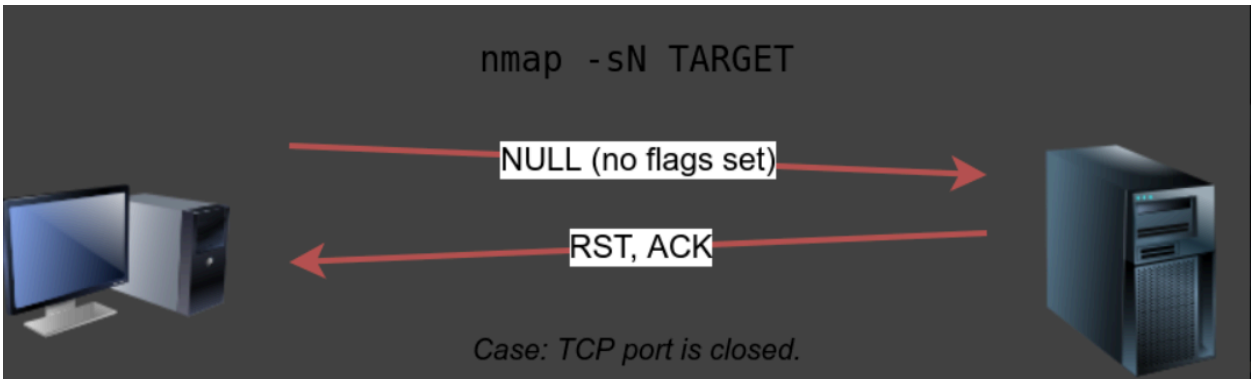
- Null Scan (Null Tarama)
- FIN Scan (FIN Tarama)
- Xmas Scan (Xmas Tarama)

Null Scan

Null taraması herhangi bir bayrak ayarlamaz; altı bayrak bitinin tümü sıfıra ayarlanır. Bu taramayı -sN seçeneğini kullanarak seçebilirsiniz. Bayrakları ayarlanmamış bir TCP paketi, aşağıdaki şekilde gösterildiği gibi açık bir bağlantı noktasına ulaştığında herhangi bir yanıtı tetiklemeyecektir. Bu nedenle, Nmap'in bakış açısına göre, bir null taramasında yanıt alınamaması ya portun açık olduğunu ya da bir güvenlik duvarının paketi engellediğini gösterir.



Ancak, port kapalıysa hedef sunucunun bir RST paketiyle yanıt vermesini bekleriz. Sonuç olarak, kapalı olmayan portları bulmak için RST yanıtının eksikliğini kullanabiliriz: açık veya filtrelenmiş.



Aşağıda bir Linux sunucusuna karşı yapılan null tarama örneği yer almaktadır. Gerçekleştirdiğimiz null taraması hedef sistemdeki altı açık portu başarıyla tespit etmiştir. Boş tarama, bağlantı noktasının kapalı olmadığı sonucuna varmak için bir yanıtın olmamasına dayandığından, bu bağlantı noktalarının açık olduğunu kesin olarak gösteremez; bağlantı noktalarının bir güvenlik duvarı kuralı nedeniyle yanıt vermemesi olasılığı vardır.

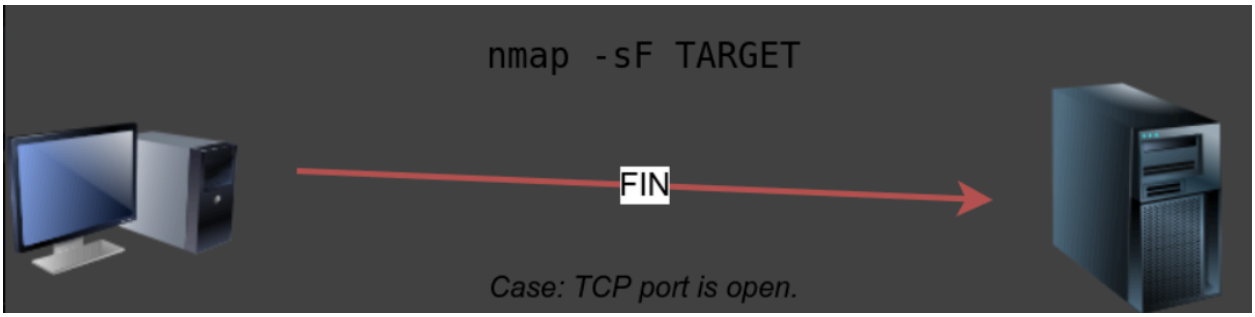
```
pentester@TryHackMe$ sudo nmap -sN MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-08-30 10:30 BST
Nmap scan report for MACHINE_IP
Host is up (0.00066s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
```

```
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 96.50 seconds
```

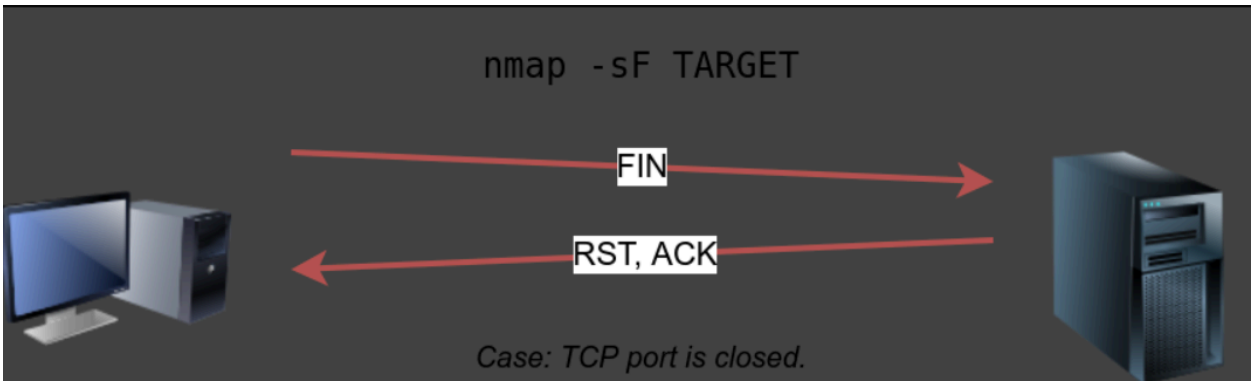
Birçok Nmap seçeneğinin root ayrıcalıkları gerektirdiğini unutmayın. Nmap'i root olarak çalıştırmıyorsanız, yukarıdaki örnekte olduğu gibi -sN seçeneğini kullanarak sudo kullanmanız gerekir.

FIN Scan

FIN taraması FIN bayrağı ayarlanmış bir TCP paketi gönderir. Bu tarama türünü -sF seçeneğini kullanarak seçebilirsiniz. Benzer şekilde, TCP portu açıksa hiçbir yanıt gönderilmeyecektir. Yine, Nmap bağlantı noktasının açık olup olmadığından veya bir güvenlik duvarının bu TCP bağlantı noktasıyla ilgili trafiği engelleyip engellemediğinden emin olamaz.



Ancak, port kapalıysa hedef sistem bir RST ile yanıt vermelidir. Sonuç olarak, hangi portların kapalı olduğunu bilebilir ve bu bilgiyi açık veya filtrelenmiş portları çıkarmak için kullanabiliriz. Bazı güvenlik duvarlarının bir RST göndermeden trafiği 'sessizce' bırakacağını belirtmek gerekir.



Aşağıda bir Linux sunucusuna karşı FIN taramasının bir örneği yer almaktadır. Sonuç, daha önce null taraması kullanarak elde ettiğimiz sonuca oldukça benzemektedir.

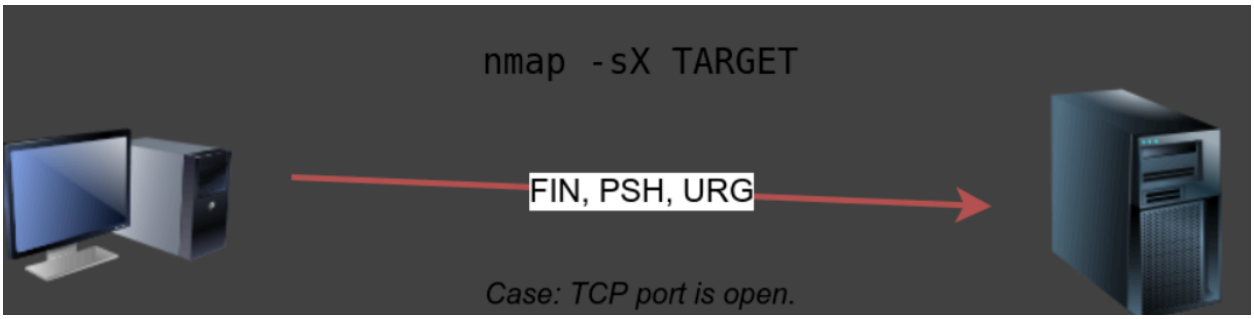
```
pentester@TryHackMe$ sudo nmap -sF MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-08-30 10:32 BST
Nmap scan report for MACHINE_IP
Host is up (0.0018s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 96.52 seconds
```

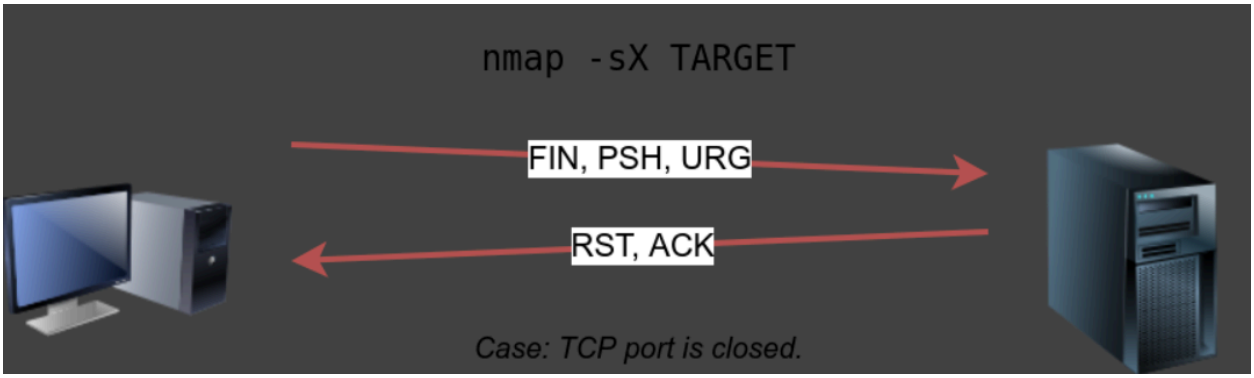
Xmas Scan

Xmas taraması adını Noel ağacı ışıklarından alır. Bir Xmas taraması FIN, PSH ve URG bayraklarını aynı anda ayarlar. Xmas taramasını -sX seçeneği ile seçebilirsiniz.

Null tarama ve FIN tarama gibi, eğer bir RST paketi alınırsa, bu portun kapalı olduğu anlamına gelir. Aksi takdirde, açık|filtreli olarak raporlanacaktır.

Aşağıdaki iki şekil TCP portunun açık olduğu durumu ve TCP portunun kapalı olduğu durumu göstermektedir.





Aşağıdaki konsol çıktısı bir Linux sunucusuna karşı yapılan Xmas taramasının bir örneğini göstermektedir. Elde edilen sonuçlar null taraması ve FIN taraması ile oldukça benzerdir.

```
pentester@TryHackMe$ sudo nmap -sX MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-08-30 10:34 BST
Nmap scan report for MACHINE_IP
Host is up (0.00087s latency).
Not shown: 994 closed ports
PORT    STATE         SERVICE
22/tcp  open|filtered ssh
25/tcp  open|filtered smtp
80/tcp  open|filtered http
110/tcp open|filtered pop3
111/tcp open|filtered rpcbind
143/tcp open|filtered imap
```

```
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 84.85 seconds
```

Bu üç tarama türünün verimli olabileceği bir senaryo, durum bilgisi olmayan (statüsüz) bir güvenlik duvarının arkasındaki bir hedefin taranmasıdır. Durum bilgisi olmayan bir güvenlik duvarı, bir bağlantı girişimini tespit etmek için gelen paketin SYN bayrağına sahip olup olmadığını kontrol edecektir. SYN paketiyle eşleşmeyen bir bayrak kombinasyonu kullanmak, güvenlik duvarını aldatmayı ve arkasındaki sisteme ulaşmayı mümkün kılar. Ancak, durum bilgisine sahip bir güvenlik duvarı bu tür hazırlanmış paketlerin tümünü pratikte engelleyecek ve bu tür bir taramayı işe yaramaz hale getirecektir.

Sorular

Soru ⇒ Bir null taramasında, kaç bayrak 1'e ayarlanır?

Cevap ⇒ 0

Soru ⇒ Bir FIN taramasında, kaç bayrak 1'e ayarlanır?

Cevap ⇒ 1

Soru ⇒ Bir Noel taramasında, kaç bayrak 1 olarak ayarlanır?

Cevap ⇒ 3

Soru ⇒ Sanal makineyi başlatın ve AttackBox'ı yükleyin. Her ikisi de hazır olduğunda, AttackBox'ta terminali açın ve hedef VM'ye karşı bir FIN taraması başlatmak için nmap kullanın. Kaç port açık|filtrelenmiş olarak görünüyor?

Cevap ⇒ 9

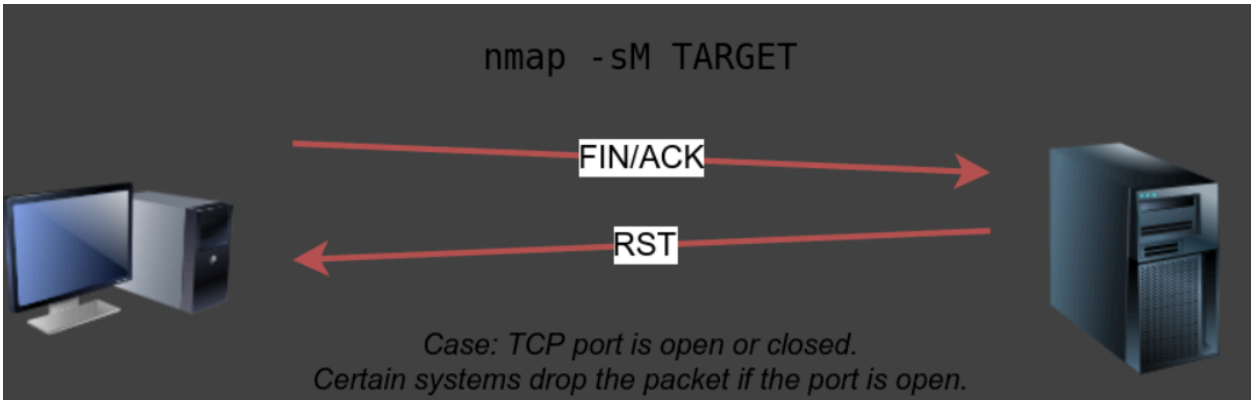
Soru ⇒ Hedef VM'ye karşı bir null tarama başlatarak taramanızı tekrarlayın. Kaç bağlantı noktası açık|filtrelenmiş olarak görünüyor?

Cevap ⇒ 9

Task 3 TCP Maimon Scan (Görev 3 TCP Maimon Taraması)

Uriel Maimon bu taramayı ilk olarak 1996 yılında tanımlamıştır. Bu taramada FIN ve ACK bitleri ayarlanır. Hedef yanıt olarak bir RST paketi göndermelidir. Ancak, bazı BSD türevi sistemler açık portları açığa çıkaran açık bir port ise paketi düşürür. Bu tarama modern ağlarda karşılaşılan çoğu hedef üzerinde çalışmayacaktır; ancak port tarama mekanizmasını ve bilgisayar korsanlığı zihniyetini daha iyi anlamak için bu odaya dahil ediyoruz. Bu tarama türünü seçmek için -sM seçeneğini kullanın.

Çoğu hedef sistem TCP portunun açık olup olmadığına bakmaksızın bir RST paketi ile yanıt verir. Böyle bir durumda, açık portları keşfetmemiz mümkün olmayacaktır. Aşağıdaki şekil hem açık hem de kapalı TCP portları durumunda beklenen davranışı göstermektedir.



Aşağıdaki konsol çıktısı bir Linux sunucusuna karşı TCP Maimon taramasının bir örneğidir. Belirtildiği gibi, açık portlar ve kapalı portlar aynı şekilde davrandığından, Maimon taraması hedef sistemde herhangi bir açık port bulamamıştır.

```
pentester@TryHackMe$ sudo nmap -sM 10.10.252.27Starting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-08-30 10:36 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.
27)
Host is up (0.00095s latency).
All 1000 scanned ports on ip-10-10-252-27.eu-west-1.compute.internal (10.10.
252.27) are closed
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
```

Bu tür bir tarama, bir sistemi keşfetmek için seçilecek ilk tarama değildir; ancak ne zaman işe yarayacağını bilemeyeceğiniz için bunu bilmek önemlidir.

Soru ⇒ Maimon taramasında kaç bayrak ayarlanır?

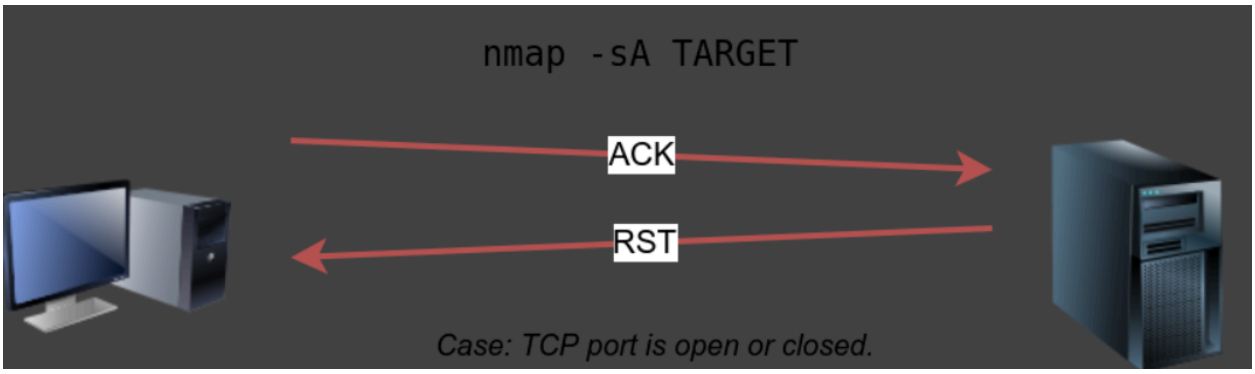
Cevap ⇒ 2

Task 4 TCP ACK, Window, and Custom Scan (TCP ACK, Pencere ve Özel Tarama)

Bu görev, TCP ACK taramasının, TCP pencere taramasının nasıl gerçekleştirileceğini ve özel bayrak taramanızı nasıl oluşturacağınızı kapsayacaktır.

TCP ACK Scan

TCP ACK taraması ile başlayalım. Adından da anlaşılacağı gibi, bir ACK taraması ACK bayrağı ayarlanmış bir TCP paketi gönderir. Bu taramayı seçmek için -sA seçeneğini kullanın. Aşağıdaki şekilde gösterdiğimiz gibi, hedef, portun durumuna bakılmaksızın ACK'ye RST ile yanıt verecektir. Bu davranış, ACK bayrağı ayarlanmış bir TCP paketinin, bizim durumumuzdan farklı olarak, yalnızca bazı verilerin alındığını onaylamak için alınan bir TCP paketine yanıt olarak gönderilmesi gerektiğinden kaynaklanır. Dolayısıyla, bu tarama bize hedef portun basit bir kurulumda açık olup olmadığını söylemeyecektir.



Aşağıdaki örnekte, hedef sanal makineye bir güvenlik duvarı kurmadan önce tarama yaptık. Beklendiği gibi, hangi portların açık olduğunu öğrenemedik.

```
pentester@TryHackMe$ sudo nmap -sA MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-08-30 10:37 BST
Nmap scan report for MACHINE_IP
Host is up (0.0013s latency).
All 1000 scanned ports on MACHINE_IP are unfiltered
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.68 seconds
```

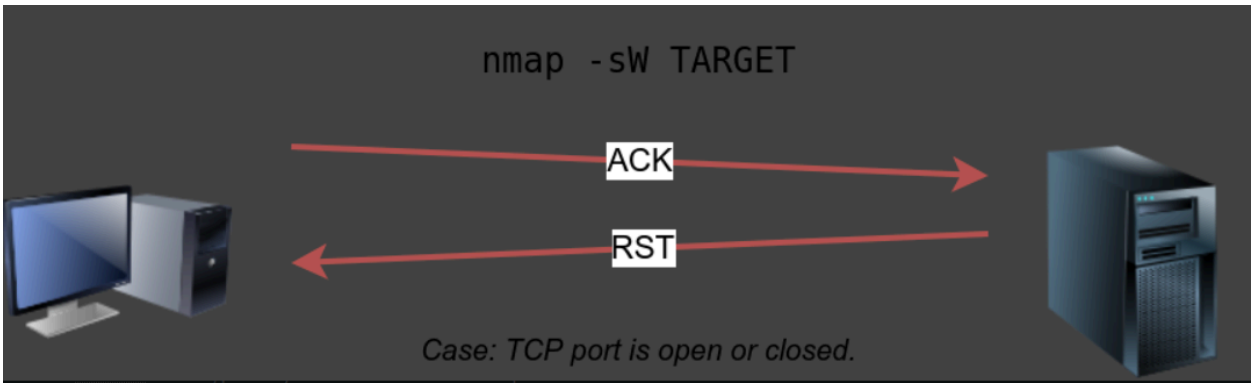
Bu tür bir tarama, hedefin önünde bir güvenlik duvarı varsa yararlı olacaktır. Sonuç olarak, hangi ACK paketlerinin yanıtlarla sonuçlandığına bağlı olarak, hangi bağlantı noktalarının güvenlik duvarı tarafından engellenmediğini öğreneceksiniz. Başka bir deyişle, bu tür bir tarama güvenlik duvarı kural setlerini ve yapılandırmasını keşfetmek için daha uygundur.

Hedef VM MACHINE_IP'yi bir güvenlik duvarı ile kurduktan sonra ACK taramasını tekrarladık. Bu sefer, bazı ilginç sonuçlar aldık. Aşağıdaki konsol çıktısında görüldüğü gibi, güvenlik duvarı tarafından engellenmeyen üç portumuz var. Bu sonuç, güvenlik duvarının bu üç port dışında diğer tüm portları engellediğini gösterir.

```
pentester@TryHackMe$ sudo nmap -sA MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-09-07 11:34 BST
Nmap scan report for MACHINE_IP
Host is up (0.00046s latency).
Not shown: 997 filtered ports
PORT    STATE      SERVICE
22/tcp  unfiltered ssh
25/tcp  unfiltered smtp
80/tcp  unfiltered http
MAC Address: 02:78:C0:D0:4E:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 15.45 seconds
```

Window Scan

Benzer bir başka tarama da TCP pencere taramasıdır. TCP pencere taraması ACK taramasıyla hemen hemen aynıdır; ancak, geri dönen RST paketlerinin TCP Pencere alanını inceler. Belirli sistemlerde, bu portun açık olduğunu ortaya çıkarabilir. Bu tarama türünü -sW seçeneği ile seçebilirsiniz. Aşağıdaki şekilde gösterildiği gibi, portun açık veya kapalı olmasına bakılmaksızın, "davetsiz" ACK paketlerimize yanıt olarak bir RST paketi almayı bekliyoruz.



Benzer şekilde, güvenlik duvarı olmayan bir Linux sistemine karşı TCP pencere taraması başlatmak da fazla bilgi sağlamayacaktır. Aşağıdaki konsol çıktısında görebileceğimiz gibi, güvenlik duvarı olmayan bir Linux sunucusuna karşı pencere taramasının sonuçları, daha önce yürütülen ACK taramasına kıyasla herhangi bir ekstra bilgi vermedi.

```
pentester@TryHackMe$ sudo nmap -sW MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-08-30 10:38 BST
Nmap scan report for MACHINE_IP
Host is up (0.0011s latency).
All 1000 scanned ports on ip-10-10-252-27.eu-west-1.compute.internal (10.10.
252.27) are closed
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Ancak, tahmin edebileceğiniz gibi, TCP pencere taramamızı bir güvenlik duvarının arkasındaki bir sunucuya karşı tekrarlarsak, daha tatmin edici sonuçlar almayı bekleriz. Aşağıda gösterilen konsol çıktısında, TCP pencere taraması üç portun kapalı olarak algılandığını göstermiştir. (Bu, aynı üç bağlantı noktasını

filtrelenmemiş olarak etiketleyen ACK taramasının tersidir). Bu üç portun kapalı olmadığını bilmemize rağmen, güvenlik duvarının bunları engellemediğini gösteren farklı yanıtlar verdiklerini fark ettik.

```
pentester@TryHackMe$ sudo nmap -sW MACHINE_IPStarting Nmap 7.60 ( htt
ps://nmap.org ) at 2021-09-07 11:39 BST
Nmap scan report for MACHINE_IP
Host is up (0.00040s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
22/tcp  closed ssh
25/tcp  closed smtp
80/tcp  closed http
MAC Address: 02:78:C0:D0:4E:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.84 seconds
```

Custom Scan

Yerleşik TCP tarama türlerinin ötesinde yeni bir TCP bayrağı kombinasyonu denemek istiyorsanız, bunu --scanflags kullanarak yapabilirsiniz. Örneğin, SYN, RST ve FIN'i aynı anda ayarlamak istiyorsanız, bunu --scanflags RSTSYNFIN kullanarak yapabilirsiniz. Aşağıdaki şekilde gösterildiği gibi, özel taramanızı geliştirirseniz, farklı senaryolarda sonuçları doğru yorumlamak için farklı bağlantı noktalarının nasıl davranacağını bilmeniz gerekir.

Son olarak, ACK taramasının ve pencere taramasının güvenlik duvarı kurallarını belirlememize yardımcı olma konusunda çok etkili olduğunu belirtmek gerekir. Bununla birlikte, bir güvenlik duvarının belirli bir bağlantı noktasını engellemiyor olmasının, bir hizmetin o bağlantı noktasını dinlediği anlamına gelmediğini unutmamak çok önemlidir. Örneğin, güvenlik duvarı kurallarının son hizmet değişikliklerini yansıtacak şekilde güncellenmesi gerekebilir. Bu nedenle, ACK ve pencere taramaları hizmetleri değil, güvenlik duvarı kurallarını açığa çıkarır.

Sorular

Soru ⇒ TCP Pencere taramasında kaç bayrak ayarlanır?

Cevap ⇒ 1

Soru ⇒ Sıfırlama bayrağı ayarlanmış özel bir TCP taraması denemeye karar verdiniz. --scanflags komutundan sonra ne eklersiniz(İpucu ⇒ Sıfırlama bayrağı RST'dir)?

Cevap ⇒ RST

Soru ⇒ Sanal makine, güvenlik duvarı kural kümesinde bir güncelleme aldı. Artık güvenlik duvarı tarafından yeni bir bağlantı noktasına izin verilmektedir. Sanal makineyi Görev 2'den sonlandırdığınızdan emin olduktan sonra, bu görev için sanal makineyi başlatın. Henüz yapmadıysanız AttackBox'ı başlatın. Her ikisi de hazır olduğunda, AttackBox'ta terminali açın ve hedef sanal makineye karşı bir ACK taraması başlatmak için Nmap'i kullanın. Filtrelenmemiş kaç port görünüyor?

Cevap ⇒ 4

Soru ⇒ Ortaya çıkan yeni bağlantı noktası numarası nedir?

Cevap ⇒ 443

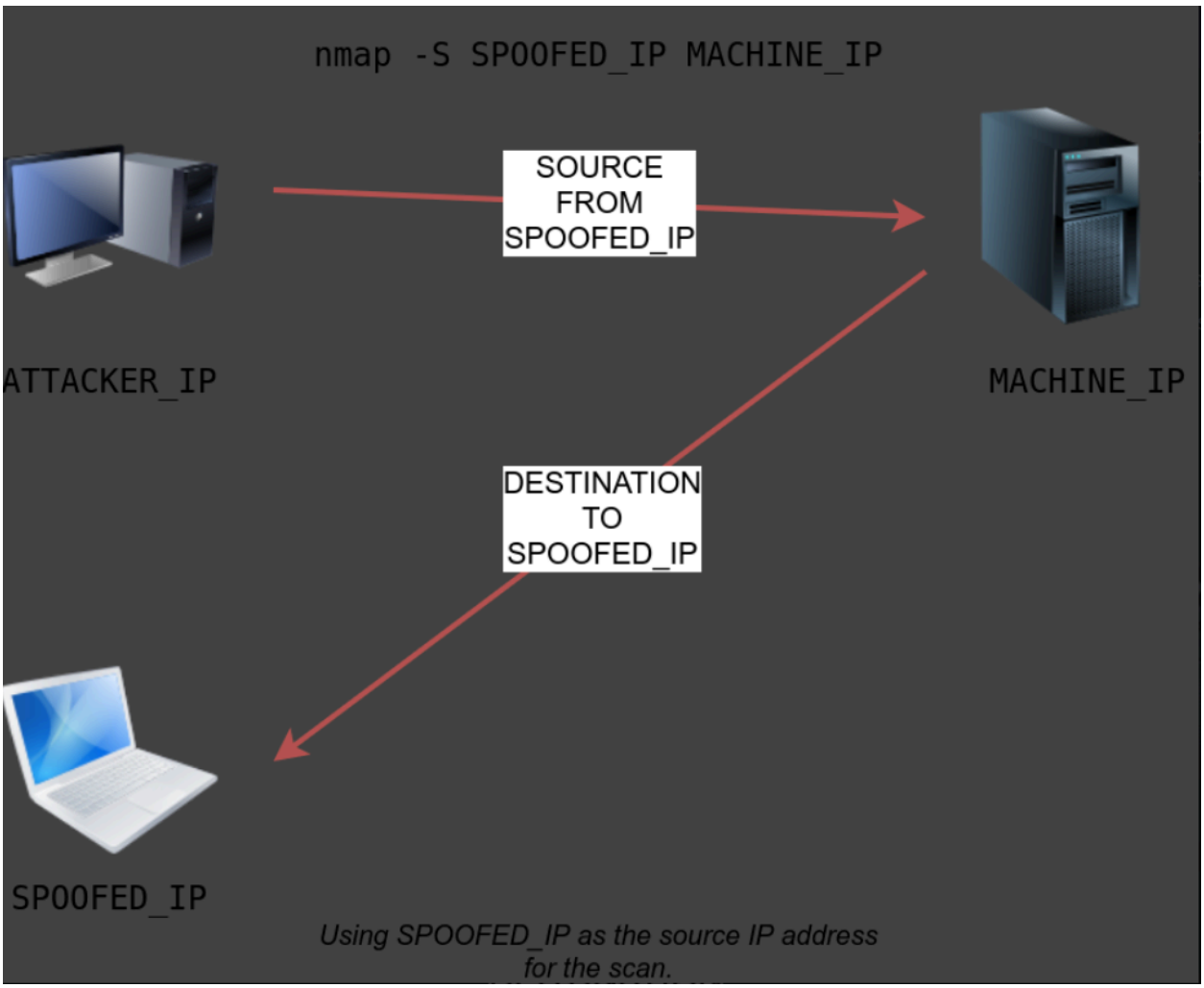
Soru ⇒ Yeni keşfedilen bağlantı noktası numarasının arkasında herhangi bir hizmet var mı? (Y/N)(İpucu ⇒ AttakBox üzerinde Firefox tarayıcısını kullanın ve https://MACHINE_IP adresine göz atın)

Cevap ⇒ N

Task 5 Spoofing and Decoys (Görev 5 Spoofing ve Tuzaklar)

Bazı ağ kurulumlarında, sahte bir IP adresi ve hatta sahte bir MAC adresi kullanarak hedef sistemi tarayabilirsiniz. Böyle bir tarama yalnızca yanıtı yakalamayı garanti edebileceğiniz bir durumda faydalıdır. Sahte bir IP adresi kullanarak rastgele bir ağdan bir hedefi taramaya çalışırsanız, büyük olasılıkla size yönlendirilen herhangi bir yanıt alamazsınız ve tarama sonuçları güvenilmez olabilir.

Aşağıdaki şekilde saldırganın nmap -S SPOOFED_IP MACHINE_IP komutunu başlatması gösterilmektedir. Sonuç olarak, Nmap sağlanan kaynak IP adresi SPOOFED_IP'yi kullanarak tüm paketleri oluşturacaktır. Hedef makine, gelen paketlere SPOOFED_IP hedef IP adresine yanıtlar göndererek yanıt verecektir. Bu taramanın çalışması ve doğru sonuçlar vermesi için saldırganın yanıtları analiz etmek üzere ağ trafiğini izlemesi gerekir.



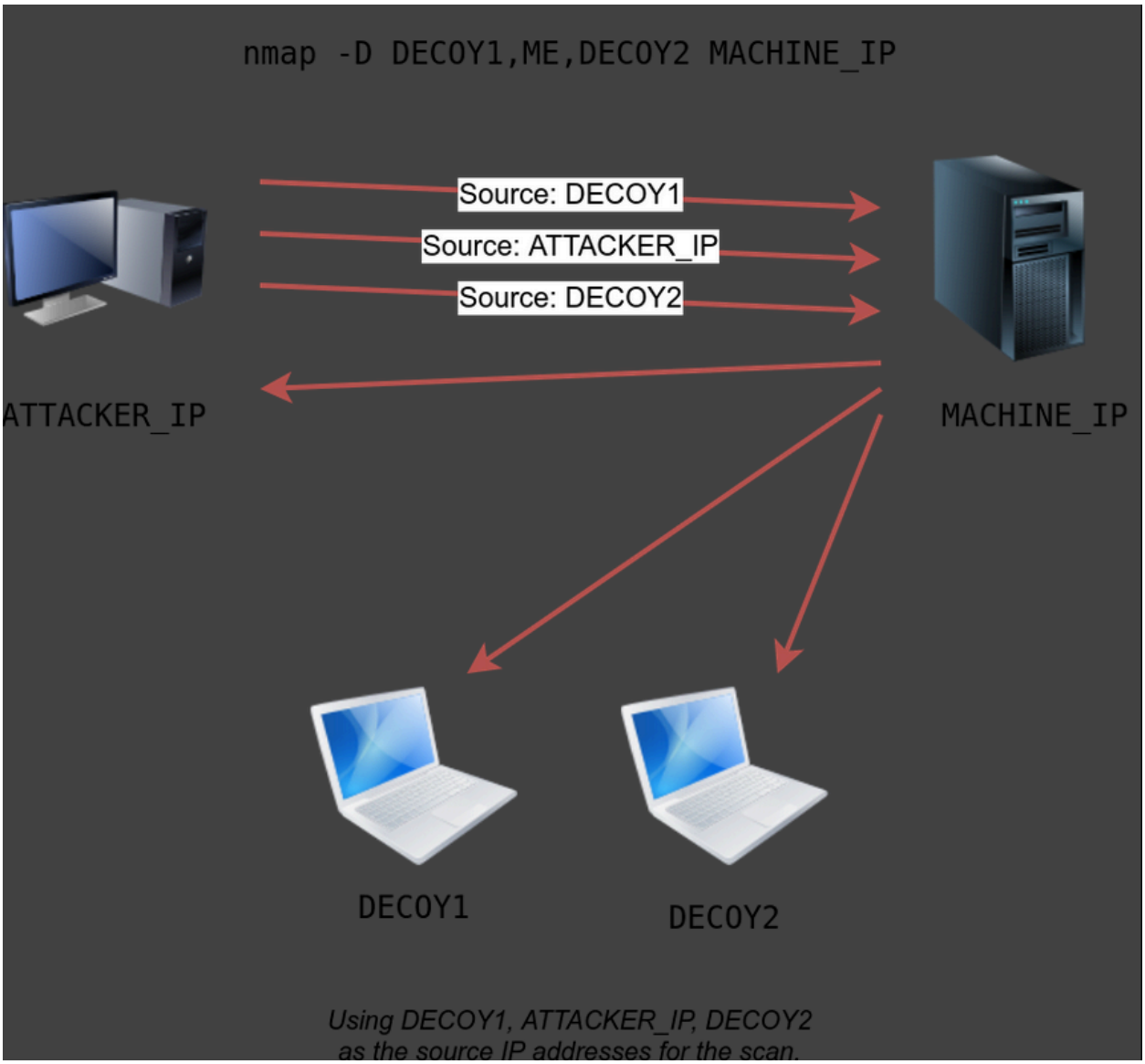
Kısaca, sahte bir IP adresi ile tarama üç adımdan oluşur:

1. Saldırgan, hedef makineye sahte bir kaynak IP adresi içeren bir paket gönderir.
2. Hedef makine hedef olarak sahte IP adresine yanıt verir.
3. Saldırgan açık portları bulmak için yanıtları yakalar.

Genel olarak, -e kullanarak ağ arayüzünü belirtmeyi ve -Pn ping taramasını açıkça devre dışı bırakmayı beklersiniz. Bu nedenle, nmap -S SPOOFED_IP MACHINE_IP yerine, Nmap'e hangi ağ arayüzünü kullanacağını ve ping yanıtı almayı beklememesini açıkça söylemek için nmap -e NET_INTERFACE -Pn -S SPOOFED_IP MACHINE_IP komutunu vermeniz gerekecektir. Saldırgan sistem yanıtlar için ağı izleyemiyorsa bu taramanın işe yaramayacağını tekrarlamakta fayda var.

Hedef makine ile aynı alt ağda olduğunuzda, MAC adresinizi de taklit edebilirsiniz. Kaynak MAC adresini --spoof-mac SPOOFED_MAC kullanarak belirtebilirsiniz. Bu adres sahteciliği yalnızca saldırgan ve hedef makine aynı Ethernet (802.3) ağında veya aynı WiFi (802.11) ağındaysa mümkündür.

Spoofing yalnızca belirli koşulların karşılandığı çok az sayıda durumda işe yarar. Bu nedenle, saldırgan tespit edilmeyi daha zor hale getirmek için tuzaklara başvurabilir. Konsept basittir, taramanın birçok IP adresinden geliyormuş gibi görünmesini sağlayın, böylece saldırganın IP adresi bunların arasında kaybolacaktır. Aşağıdaki şekilde gördüğümüz gibi, hedef makinenin taraması 3 farklı kaynaktan geliyor gibi görünecek ve sonuç olarak yanıtlar da tuzaklara gidecektir.



D'den sonra belirli veya rastgele bir IP adresi belirterek sahte bir tarama başlatabilirsiniz. Örneğin, nmap -D 10.10.0.1,10.10.0.2,ME MACHINE_IP, MACHINE_IP taramasının 10.10.0.1, 10.10.0.2 ve ardından IP adresinizin üçüncü sırada görünmesi gerektiğini belirtmek için ME IP adreslerinden geliyor gibi görünmesini sağlayacaktır. Başka bir örnek komut nmap -D 10.10.0.1,10.10.0.2,RND,RND,ME MACHINE_IP şeklinde olabilir; burada üçüncü ve dördüncü kaynak IP adresleri rastgele atanırken, beşinci kaynak saldırganın IP adresi olacaktır. Başka bir deyişle, ikinci komutu her çalıştırdığınızda, iki yeni rastgele IP adresinin üçüncü ve dördüncü yem kaynaklar olmasını beklersiniz.

Sorular

Soru ⇒ Taramanın IP adresiniz yerine 10.10.10.11 kaynak IP adresinden geliyormuş gibi görünmesini sağlamak için sudo nmap MACHINE_IP komutuna ne eklemeniz gerekiyor?

Cevap ⇒ -S 10.10.10.11

Soru ⇒ Taramanın IP adresinize ek olarak 10.10.20.21 ve 10.10.20.28 kaynak IP adreslerinden geliyormuş gibi görünmesini sağlamak için sudo nmap MACHINE_IP komutuna ne eklemeniz gerekiyor?

Cevap ⇒ -D 10.10.20.21,10.10.20.28,ME

Task 6 Fragmented Packets (Görev 6 Parçalanmış Paketler)

Firewall

Güvenlik duvarı, paketlerin geçmesine izin veren veya onları engelleyen bir yazılım veya donanım parçasıdır. İstisnalar dışında tüm trafiği engelleme veya istisnalar dışında tüm trafiğe izin verme olarak özetlenen güvenlik duvarı kurallarına göre çalışır. Örneğin, web sunucunuza gelenler dışında sunucunuza gelen tüm trafiği engelleyebilirsiniz. Geleneksel bir güvenlik duvarı en azından IP başlığını ve taşıma katmanı başlığını inceler. Daha sofistike bir güvenlik duvarı, taşıma katmanı tarafından taşınan verileri de incelemeye çalışır.

IDS

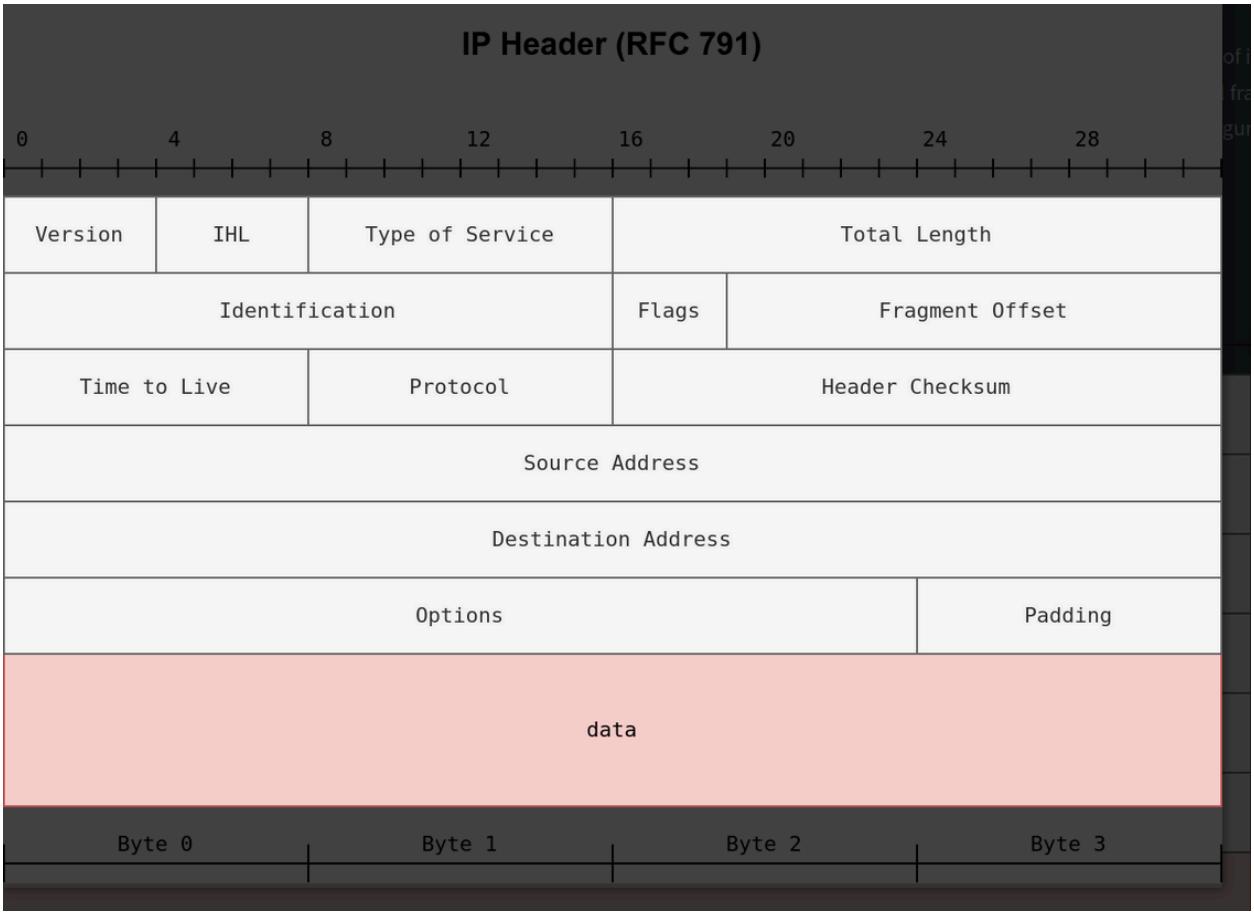
Bir saldırı tespit sistemi (IDS), belirli davranış kalıpları veya belirli içerik imzaları için ağ paketlerini inceler. Kötü niyetli bir kural karşılandığında bir uyarı verir. IP başlığına ve aktarım katmanı başlığına ek olarak, bir IDS aktarım katmanındaki veri içeriğini inceleyecek ve herhangi bir kötü niyetli kalıpla eşleşip eşleşmediğini kontrol edecektir. Geleneksel bir güvenlik duvarı/IDS'in Nmap etkinliğinizi tespit etme olasılığını nasıl azaltabilirsiniz? Buna cevap vermek kolay değildir; ancak, güvenlik duvarı/IDS türüne bağlı olarak, paketi daha küçük paketlere bölmenin faydasını görebilirsiniz.

Fragmented Packets

Nmap paketleri parçalamak için -f seçeneğini sunar. Bir kez seçildiğinde, IP verisi 8 ya da daha az bayta bölünecektir. Başka bir -f (-f -f veya -ff) eklendiğinde veri 8

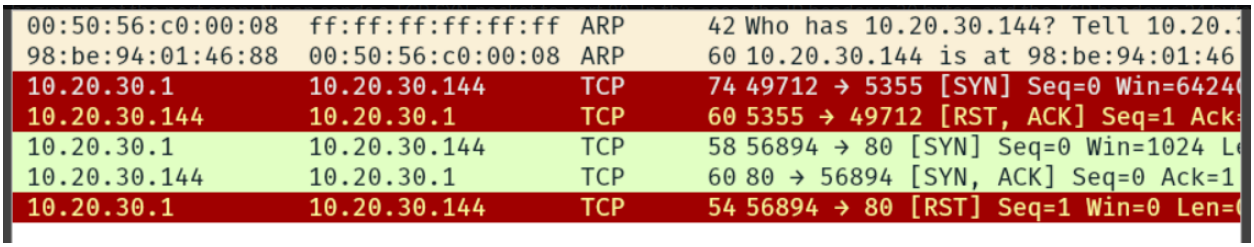
yerine 16 baytlık parçalara bölünecektir. --mtu kullanarak varsayılan değeri değiştirebilirsiniz; ancak her zaman 8'in katlarını seçmelisiniz.

Parçalanmayı doğru bir şekilde anlamak için aşağıdaki şekilde IP başlığına bakmamız gerekir. İlk başta karmaşık görünebilir, ancak alanlarının çoğunu bildiğimizi fark ederiz. Özellikle, kaynak adresin dördüncü satırda 32 bit (4 bayt) aldığına, hedef adresin ise beşinci satırda 4 bayt daha aldığına dikkat edin. Birden fazla pakete böleceğimiz veriler kırmızıyla vurgulanmıştır. Alıcı tarafında yeniden birleştirmeye yardımcı olmak için IP, aşağıdaki şeklin ikinci satırında gösterilen kimlik (ID) ve parça ofsetini kullanır.

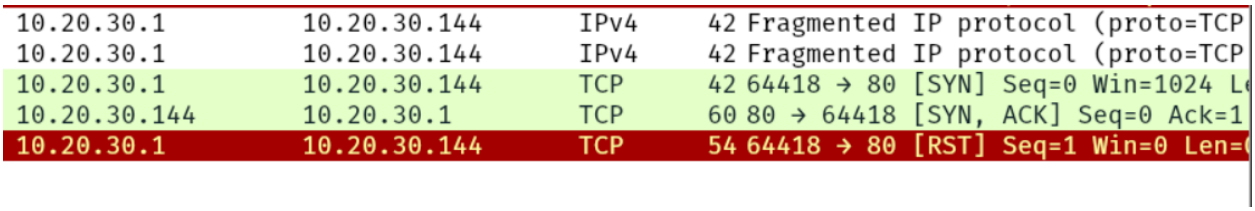


sudo nmap -sS -p80 10.20.30.144 ve sudo nmap -sS -p80 -f 10.20.30.144 komutlarını karşılaştıralım. Şimdiye kadar bildiğiniz gibi, bu 80 numaralı bağlantı noktasında gizli TCP SYN taraması kullanacaktır; ancak ikinci komutta Nmap'ten IP paketlerini parçalamasını istiyoruz.

İlk iki satırda bir ARP sorgusu ve yanıtı görebiliriz. Hedef aynı Ethernet üzerinde olduğu için Nmap bir ARP sorgusu yayınlamıştır. İkinci iki satır bir TCP SYN ping'ini ve bir yanıtı gösterir. Beşinci satır port taramasının başlangıcıdır; Nmap 80 numaralı porta bir TCP SYN paketi gönderir. Bu durumda, IP başlığı 20 bayt ve TCP başlığı 24 bayttır. TCP başlığının minimum boyutunun 20 bayt olduğunu unutmayın.



f ile parçalama istendiğinde, TCP başlığının 24 baytı 8 baytın katlarına bölünecek ve son parça TCP başlığının 8 baytını ya da daha azını içerecektir. 24, 8'e bölünebildiği için 3 IP parçamız var; her birinde 20 bayt IP başlığı ve 8 bayt TCP başlığı var. Üç parçayı beşinci ve yedinci satırlar arasında görebiliriz.



Eğer -ff (veya -f -f) eklerseniz, verinin parçalanmasının 16'nın katları şeklinde olacağını unutmayın. Başka bir deyişle, bu durumda TCP başlığının 24 baytı, ilki 16 bayt ve ikincisi TCP başlığının 8 baytını içeren iki IP parçasına bölünecektir.

Öte yandan, paketlerinizin zararsız görünmesi için boyutlarını artırmak isterseniz, --data-length NUM seçeneğini kullanabilirsiniz; burada num, paketlerinize eklemek istediğiniz bayt sayısını belirtir.

Soru ⇒ TCP segmentinin boyutu 64 ise ve -ff seçeneği kullanılıyorsa, kaç tane IP parçası alırsınız?

Cevap ⇒ 4

Task 7 Idle/Zombie Scan (Görev 7 Idle/Zombi taraması)

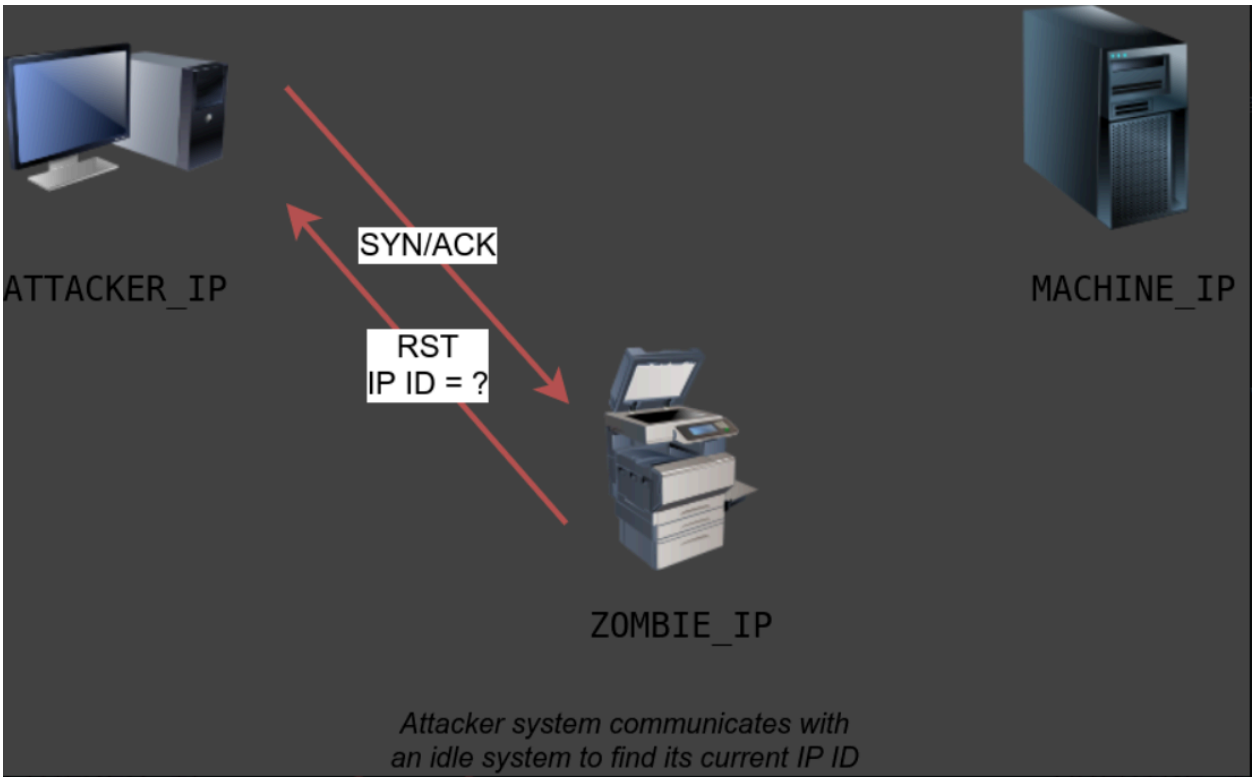
Kaynak IP adresini yanıltmak, gizlice tarama yapmak için harika bir yaklaşım olabilir. Ancak, sahtecilik yalnızca belirli ağ kurulumlarında işe yarayacaktır. Trafiği izleyebileceğiniz bir konumda olmanızı gerektirir. Bu sınırlamalar göz önüne alındığında, IP adresinizi yanıltmanın çok az faydası olabilir; ancak, boşta tarama ile bir yükseltme yapabiliriz.

Boşta tarama veya zombi taraması, iletişim kurabileceğiniz ağa bağlı boşta bir sistem gerektirir. Pratik olarak, Nmap her bir probun boşta olan (zombi) ana bilgisayardan geliyormuş gibi görünmesini sağlar, ardından boşta olan (zombi) ana bilgisayarın sahte proba herhangi bir yanıt alıp almadığına dair göstergeleri kontrol eder. Bu, IP başlığındaki IP tanımlama (IP ID) değeri kontrol edilerek gerçekleştirilir. nmap -sI ZOMBIE_IP MACHINE_IP kullanarak boşta bir tarama çalıştırabilirsiniz; burada ZOMBIE_IP boştaki ana bilgisayarın (zombi) IP adresidir.

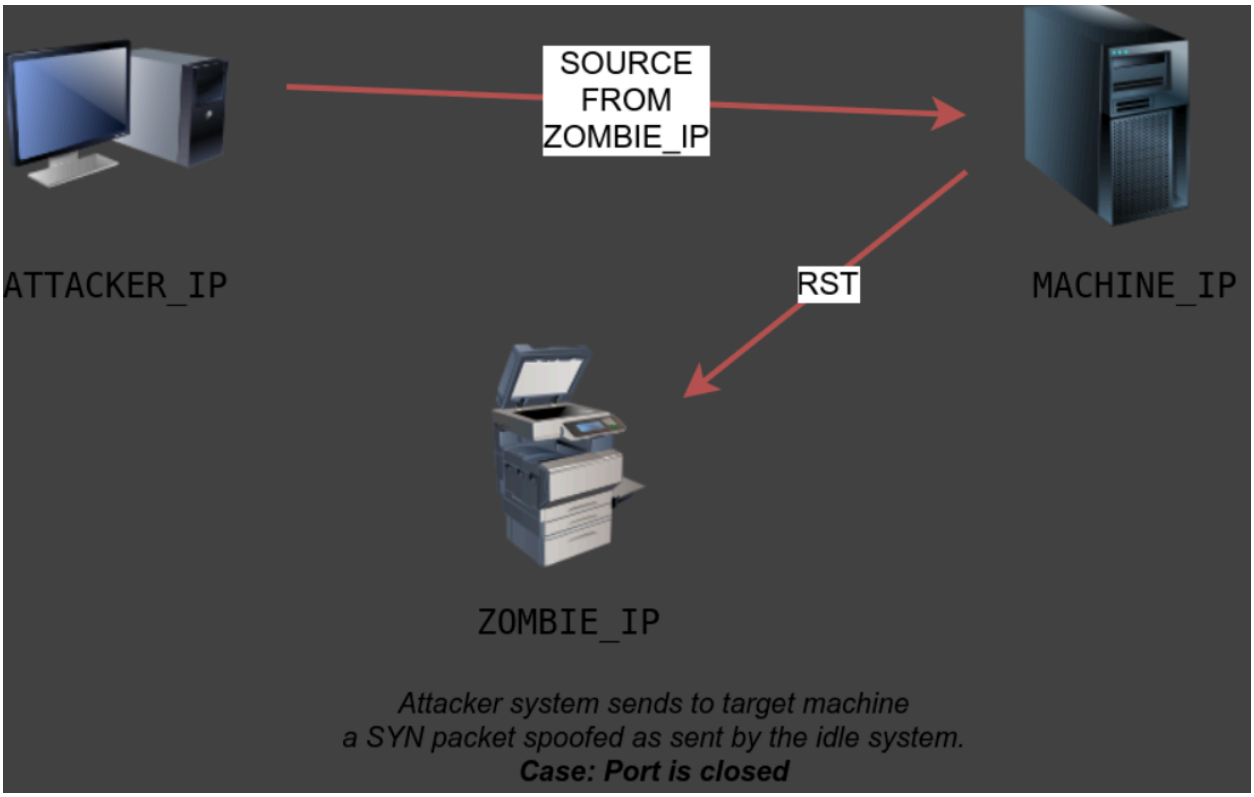
Boşta (zombi) tarama, bir bağlantı noktasının açık olup olmadığını keşfetmek için aşağıdaki üç adımı gerektirir:

1. Boşta kalan ana bilgisayarın yanıt vermesini tetikleyin, böylece boşta kalan ana bilgisayardaki geçerli IP kimliğini kaydedebilirsiniz.
2. Hedef üzerindeki bir TCP portuna SYN paketi gönderin. Paket, boşta duran ana bilgisayar (zombi) IP adresinden geliyormuş gibi görünecek şekilde sahte olmalıdır.
3. Boştaki makineyi yanıt vermesi için tekrar tetikleyin, böylece yeni IP kimliğini daha önce alınanla karşılaştırabilirsiniz.

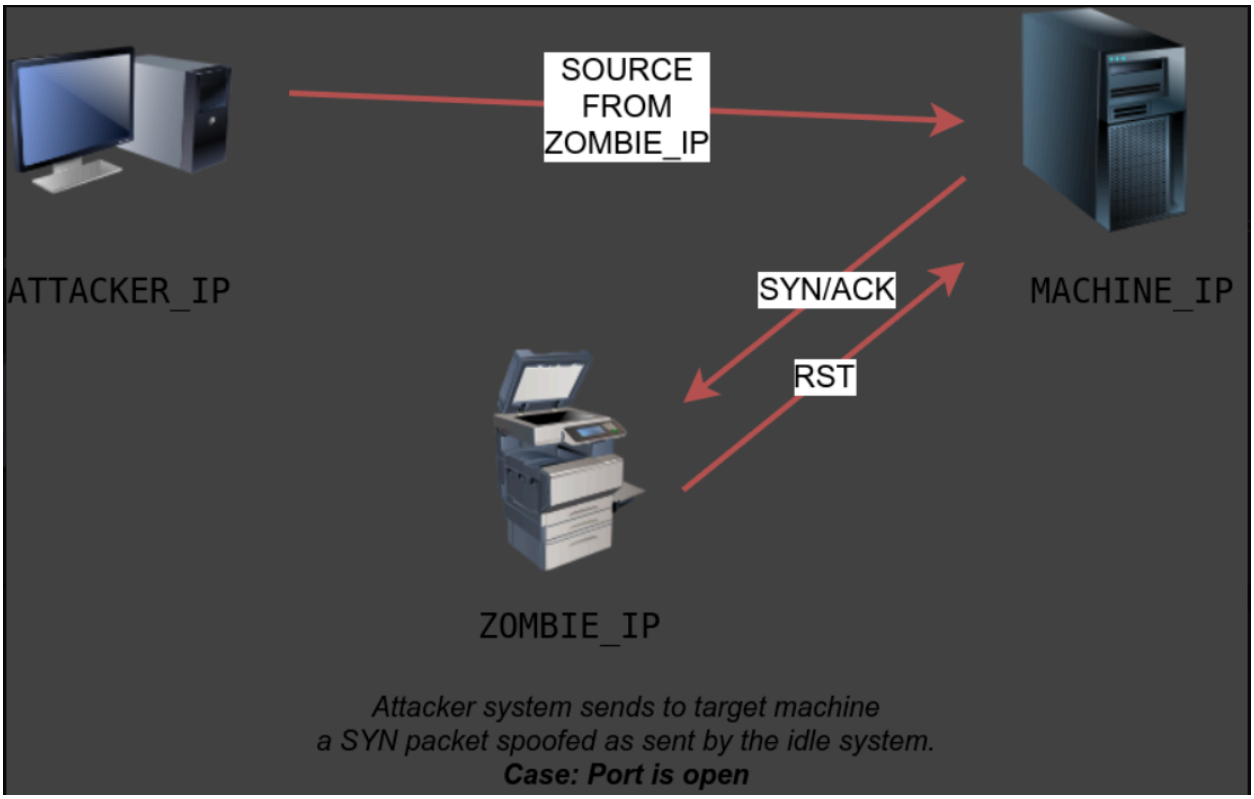
Şekillerle açıklayalım. Aşağıdaki şekilde, saldırgan sistem boşta olan bir makineyi, çok fonksiyonlu bir yazıcıyı araştırıyor. Bir SYN/ACK göndererek, yeni artırılmış IP ID'sini içeren bir RST paketi ile yanıt verir.



Saldırgan bir sonraki adımda hedef makinede kontrol etmek istediği TCP portuna bir SYN paketi gönderecektir. Ancak bu paket kaynak olarak boştaki ana bilgisayarın (zombi) IP adresini kullanacaktır. Üç senaryo ortaya çıkacaktır. Aşağıdaki şekilde gösterilen ilk senaryoda, TCP bağlantı noktası kapalıdır; bu nedenle, hedef makine boştaki ana bilgisayara bir RST paketi ile yanıt verir. Boşta kalan ana bilgisayar yanıt vermez; dolayısıyla IP Kimliği artırılmaz.



İkinci senaryoda, aşağıda gösterildiği gibi, TCP bağlantı noktası açıktır, bu nedenle hedef makine boştaki ana bilgisayara (zombi) bir SYN/ACK ile yanıt verir. Boşta kalan ana bilgisayar bu beklenmedik pakete bir RST paketiyle yanıt verir ve böylece IP kimliğini artırır.



Üçüncü senaryoda, hedef makine güvenlik duvarı kuralları nedeniyle hiç yanıt vermez. Bu yanıt eksikliği, kapalı bağlantı noktasıyla aynı sonuca yol açacaktır; boşta kalan ana bilgisayar IP kimliğini artırmayacaktır.

Son adımda saldırgan boştaki ana bilgisayara bir SYN/ACK daha gönderir. Boşta kalan ana bilgisayar, IP kimliğini tekrar bir artırarak bir RST paketiyle yanıt verir. Saldırganın ilk adımda alınan RST paketinin IP ID'sini bu üçüncü adımda alınan RST paketinin IP ID'si ile karşılaştırması gerekir. Fark 1 ise, hedef makinedeki bağlantı noktası kapatılmış veya filtrelenmiş demektir. Ancak, fark 2 ise, hedef üzerindeki bağlantı noktasının açık olduğu anlamına gelir.

Bu taramanın boşta tarama olarak adlandırıldığını tekrarlamakta fayda var çünkü boşta bir ana bilgisayar seçmek taramanın doğruluğu için vazgeçilmezdir. Eğer "boştaki ana bilgisayar" meşgulse, döndürülen tüm IP ID'leri işe yaramaz.

Soru ⇒ IP adresi 10.10.5.5 olan nadiren kullanılan bir ağ yazıcısı keşfettiniz ve bunu boşta taramanızda bir zombi olarak kullanmaya karar verdiniz. Nmap komutunuza hangi argümanı eklemelisiniz?

Cevap ⇒ -sI 10.10.5.5

Task 8 Getting More Details (Görev 8 Daha Fazla Ayrıntı Almak)

Nmap'in muhakeme ve sonuçlarıyla ilgili daha fazla ayrıntı vermesini istiyorsanız --reason eklemeyi düşünebilirsiniz. Sisteme aşağıdaki iki taramayı düşünün; ancak ikincisi --reason ekler.

```
pentester@TryHackMe$ sudo nmap -sS 10.10.252.27Starting Nmap 7.60 ( http
s://nmap.org ) at 2021-08-30 10:39 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.
27)
Host is up (0.0020s latency).
Not shown: 994 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
80/tcp  open  http
110/tcp open  pop3
111/tcp open  rpcbind
143/tcp open  imap
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

```
pentester@TryHackMe$ sudo nmap -sS --reason 10.10.252.27Starting Nmap
7.60 ( https://nmap.org ) at 2021-08-30 10:40 BST
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.
27)
Host is up, received arp-response (0.0020s latency).
Not shown: 994 closed ports
Reason: 994 resets
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 64
```

```
25/tcp  open  smtp    syn-ack ttl 64
80/tcp  open  http    syn-ack ttl 64
110/tcp open  pop3    syn-ack ttl 64
111/tcp open  rpcbind syn-ack ttl 64
143/tcp open  imap    syn-ack ttl 64
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
```

--reason bayrağının sağlanması bize Nmap'in sistemin açık olduğu ya da belirli bir portun açık olduğu sonucuna varmasının açık nedenini verir. Yukarıdaki konsol çıktısında, Nmap "arp yanıtı aldığı" için bu sistemin çevrimiçi olarak kabul edildiğini görebiliriz. Öte yandan, Nmap bir "syn-ack" paketi geri aldığı için SSH portunun açık olarak kabul edildiğini biliyoruz.

Daha ayrıntılı çıktı için ayrıntılı çıktı için -v veya daha fazla ayrıntı için -vv kullanmayı düşünebilirsiniz.

```
pentester@TryHackMe$ sudo nmap -sS -vv 10.10.252.27Starting Nmap 7.60 (
https://nmap.org ) at 2021-08-30 10:41 BST
Initiating ARP Ping Scan at 10:41
Scanning 10.10.252.27 [1 port]
Completed ARP Ping Scan at 10:41, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:41
Completed Parallel DNS resolution of 1 host. at 10:41, 0.00s elapsed
Initiating SYN Stealth Scan at 10:41
Scanning ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.27) [1000 po
rts]
Discovered open port 22/tcp on 10.10.252.27
Discovered open port 25/tcp on 10.10.252.27
Discovered open port 80/tcp on 10.10.252.27
Discovered open port 110/tcp on 10.10.252.27
Discovered open port 111/tcp on 10.10.252.27
Discovered open port 143/tcp on 10.10.252.27
Completed SYN Stealth Scan at 10:41, 1.25s elapsed (1000 total ports)
Nmap scan report for ip-10-10-252-27.eu-west-1.compute.internal (10.10.252.
```

```
27)
Host is up, received arp-response (0.0019s latency).
Scanned at 2021-08-30 10:41:02 BST for 1s
Not shown: 994 closed ports
Reason: 994 resets
PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack ttl 64
25/tcp  open  smtp    syn-ack ttl 64
80/tcp  open  http    syn-ack ttl 64
110/tcp open  pop3    syn-ack ttl 64
111/tcp open  rpcbind syn-ack ttl 64
143/tcp open  imap    syn-ack ttl 64
MAC Address: 02:45:BF:8A:2D:6B (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
           Raw packets sent: 1002 (44.072KB) | Rcvd: 1002 (40.092KB)
```

Eğer -vv merakınızı gidermiyorsa, hata ayıklama detayları için -d veya daha fazla detay için -dd kullanabilirsiniz. d kullanarak tek bir ekranın ötesine uzanan bir çıktı oluşturacağınızı garanti edebilirsiniz.

Soru ⇒ Henüz yapmadıysanız AttackBox'ı başlatın. Sanal makineyi Görev 4'ten sonlandırdığınızdan emin olduktan sonra, bu görev için sanal makineyi başlatın. Tamamen yüklenmesini bekleyin, ardından AttackBox'ta terminali açın ve VM'yi taramak için nmap -sS -F --reason MACHINE_IP ile Nmap kullanın. Belirtilen port(lar)ın açık olmasının nedeni nedir?

Cevap ⇒ syn-ack

Task 9 Summary (Görev 9 Özet)

Bu oda aşağıdaki tarama türlerini kapsamaktadır.

Port Scan Type	Example Command

TCP Null Scan	`sudo nmap -sN MACHINE_IP`
TCP FIN Scan	`sudo nmap -sF MACHINE_IP`
TCP Xmas Scan	`sudo nmap -sX MACHINE_IP`
TCP Maimon Scan	`sudo nmap -sM MACHINE_IP`
TCP ACK Scan	`sudo nmap -sA MACHINE_IP`
TCP Window Scan	`sudo nmap -sW MACHINE_IP`
Custom TCP Scan	`sudo nmap --scanflags URGACKPSHRSTSYNFIN MACHINE_IP`
Spoofed Source IP	`sudo nmap -S SPOOFED_IP MACHINE_IP`
Spoofed MAC Address	`--spoof-mac SPOOFED_MAC`
Decoy Scan	`nmap -D DECOY_IP,ME MACHINE_IP`
Idle (Zombie) Scan	`sudo nmap -sI ZOMBIE_IP MACHINE_IP`
Fragment IP data into 8 bytes	`-f`
Fragment IP data into 16 bytes	`-ff`

Option	Purpose
`--source-port PORT_NUM`	specify source port number
`--data-length NUM`	append random data to reach given length

Bu tarama türleri, bağlantı noktalarından yanıt istemek için TCP bayraklarını beklenmedik şekillerde ayarlamaya dayanır. Null, FIN ve Xmas taramaları kapalı portlardan yanıt alınmasını sağlarken, Maimon, ACK ve Window taramaları açık ve kapalı portlardan yanıt alınmasını sağlar.

Option	Purpose
`--reason`	explains how Nmap made its conclusion
`-v`	verbose
`-vv`	very verbose
`-d`	debugging
`-dd`	more details for debugging

Soru ⇒ Bu odada açıklanan tüm Nmap seçeneklerini not aldığınızdan emin olun. Lütfen bu Nmap serisinin son odası olan Nmap Port Taramaları Sonrası odasına katılın.

Cevap ⇒ Cevap Gerekmemektedir.