

Nmap Basic Port Scans

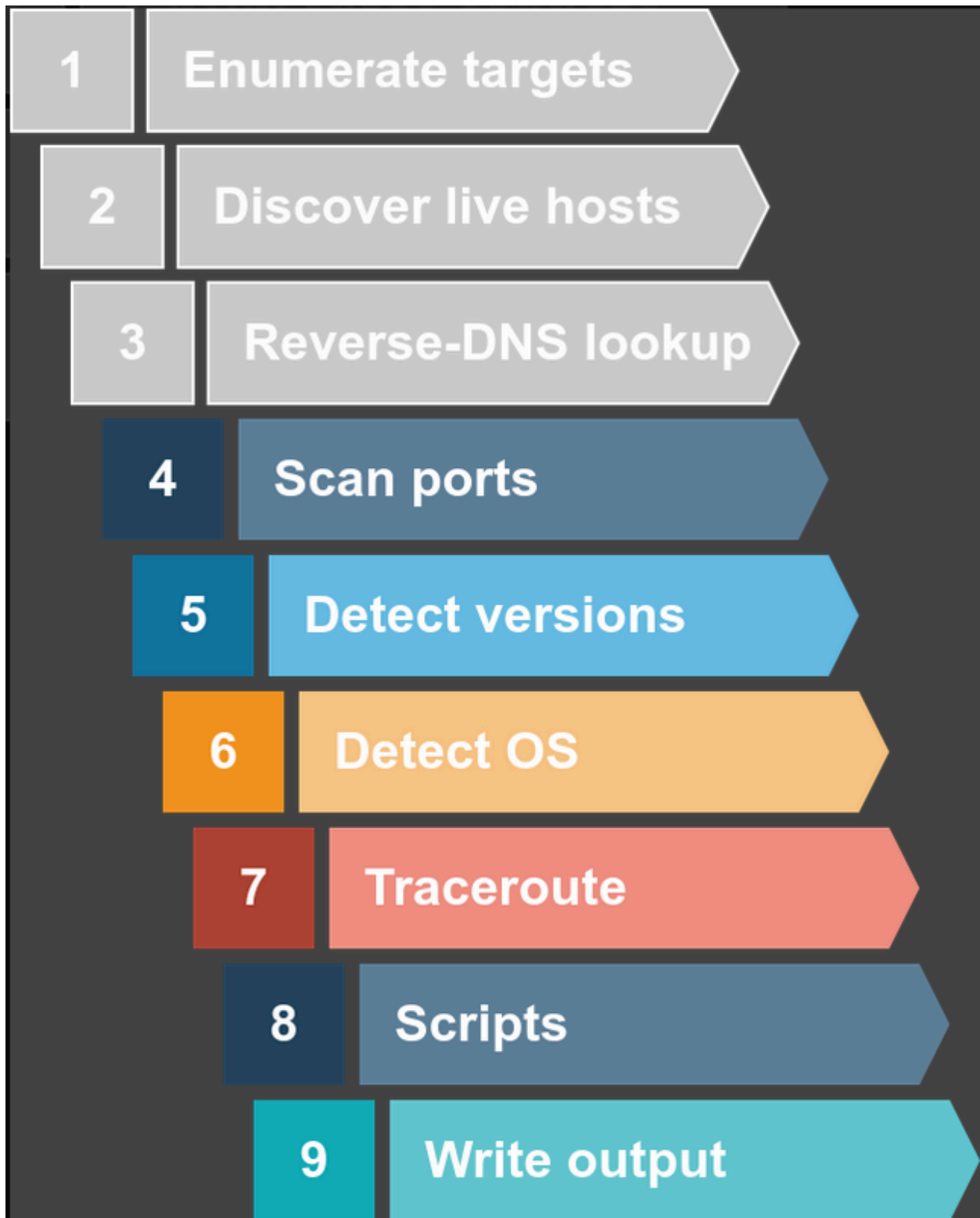
Task 1 Introduction (Görev 1 Giriş)

Bu oda Nmap serisinin ikincisidir (Ağ Güvenliğine Giriş modülünün bir parçası).

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)

Bir önceki odada, çevrimiçi sistemleri keşfetmeye odaklandık. Şimdiye kadar, bir Nmap taramasının üç adımını ele aldık:

1. Hedefleri numaralandırın
2. Canlı sunucuları keşfedin
3. Ters-DNS araması



Bir sonraki adım, hangi portların açık ve dinleniyor olduğunu ve hangi portların kapalı olduğunu kontrol etmek olacaktır. Bu nedenle, bu odada ve bir sonraki

odada, port taramasına ve nmap tarafından kullanılan farklı port tarama türlerine odaklanıyoruz. Bu oda açıklamaktadır:

1. TCP connect port scan (TCP bağlantı noktası taraması)
2. TCP SYN port scan (TCP SYN bağlantı noktası taraması)
3. UDP port scan (UDP bağlantı noktası taraması)

Ayrıca, bağlantı noktalarını, tarama hızını ve paralel prob sayısını belirlemek için farklı seçenekleri tartışıyoruz.

Soru ⇒ AttackBox'ı Başlat düğmesini kullanarak AttackBox'ı başlatın. Nmap temel tarama türleri hakkında sağlam bir bilgi edinmek için hedef sanal makineye karşı farklı tarama türleri başlatacaksınız.

Cevap ⇒ **Cevap Gerekmemektedir.**

Task 2 TCP and UDP Ports (Görev 2 TCP ve UDP Portları)

Bir IP adresinin diğerleri arasında bir ağdaki bir ana bilgisayarı belirtmesiyle aynı anlamda, bir TCP bağlantı noktası veya UDP bağlantı noktası, o ana bilgisayarda çalışan bir ağ hizmetini tanımlamak için kullanılır. Bir sunucu ağ hizmeti sağlar ve belirli bir ağ protokolüne bağlıdır. Örnekler arasında zaman sağlama, DNS sorgularına yanıt verme ve web sayfaları sunma yer alır. Bir bağlantı noktası genellikle o belirli bağlantı noktası numarasını kullanan bir hizmetle bağlantılıdır. Örneğin, bir HTTP sunucusu varsayılan olarak TCP bağlantı noktası 80'e bağlanır; ayrıca, HTTP sunucusu SSL/TLS'yi destekliyorsa, TCP bağlantı noktası 443'ü dinler. (TCP bağlantı noktaları 80 ve 443, HTTP ve HTTPS için varsayılan bağlantı noktalarıdır; ancak web sunucusu yöneticisi gerekirse başka bağlantı noktası numaraları da seçebilir). Ayrıca, herhangi bir TCP veya UDP bağlantı noktasını (aynı IP adresi üzerinde) birden fazla hizmet dinleyemez.

Aşırı basitleştirme riskini göze alarak, limanları iki durumda sınıflandırabiliriz:

1. Açık port, o portta dinleme yapan bir hizmet olduğunu gösterir.
2. Kapalı port, o portta dinleme yapan bir hizmet olmadığını gösterir.

Ancak, pratik durumlarda, güvenlik duvarlarının etkisini göz önünde bulundurmamız gerekir. Örneğin, bir bağlantı noktası açık olabilir, ancak bir güvenlik duvarı paketleri engelliyor olabilir. Bu nedenle, Nmap aşağıdaki altı durumu dikkate alır:

1. **Open** (Açık): bir hizmetin belirtilen bağlantı noktasını dinlediğini gösterir.
2. **Close** (Kapalı): port erişilebilir olmasına rağmen belirtilen portta hiçbir hizmetin dinlenmediğini gösterir. Erişilebilir derken, erişilebilir olduğunu ve bir güvenlik duvarı veya diğer güvenlik cihazları/programları tarafından engellenmediğini kastediyoruz.
3. **Filtered**(Filtrelenmiş): Nmap'in portun açık mı yoksa kapalı mı olduğunu belirleyemediği anlamına gelir çünkü port erişilebilir değildir. Bu durum genellikle Nmap'in o porta ulaşmasını engelleyen bir güvenlik duvarından kaynaklanır. Nmap'in paketlerinin bağlantı noktasına ulaşması engellenmiş olabilir; alternatif olarak, yanıtların Nmap'in ana bilgisayarına ulaşması engellenir.
4. **Unfiltered** (Filtrelenmemiş): port erişilebilir olmasına rağmen Nmap'in portun açık mı yoksa kapalı mı olduğunu belirleyemediği anlamına gelir. Bu durumla ACK tarama -sA kullanıldığında karşılaşılır.
5. **Open|Filtered** (Açık|Filtrelenmiş): Bu, Nmap'in bağlantı noktasının açık mı yoksa filtrelenmiş mi olduğunu belirleyemediği anlamına gelir.
6. **Closed|Filtered** (Kapalı|Filtreli): Bu, Nmap'in bir bağlantı noktasının kapalı mı yoksa filtrelenmiş mi olduğuna karar veremediği anlamına gelir.

Sorular

Soru ⇒ Hangi hizmet varsayılan olarak UDP bağlantı noktası 53'ü kullanır (İpucu ⇒ Harici araştırma gerektirir.)?

Cevap ⇒ **DNS**

Soru ⇒ Hangi hizmet varsayılan olarak TCP bağlantı noktası 22'yi kullanır(İpucu ⇒ Harici araştırma gerektirir.)?

Cevap ⇒ **SSH**

Soru = Nmap kaç port durumunu dikkate alır?

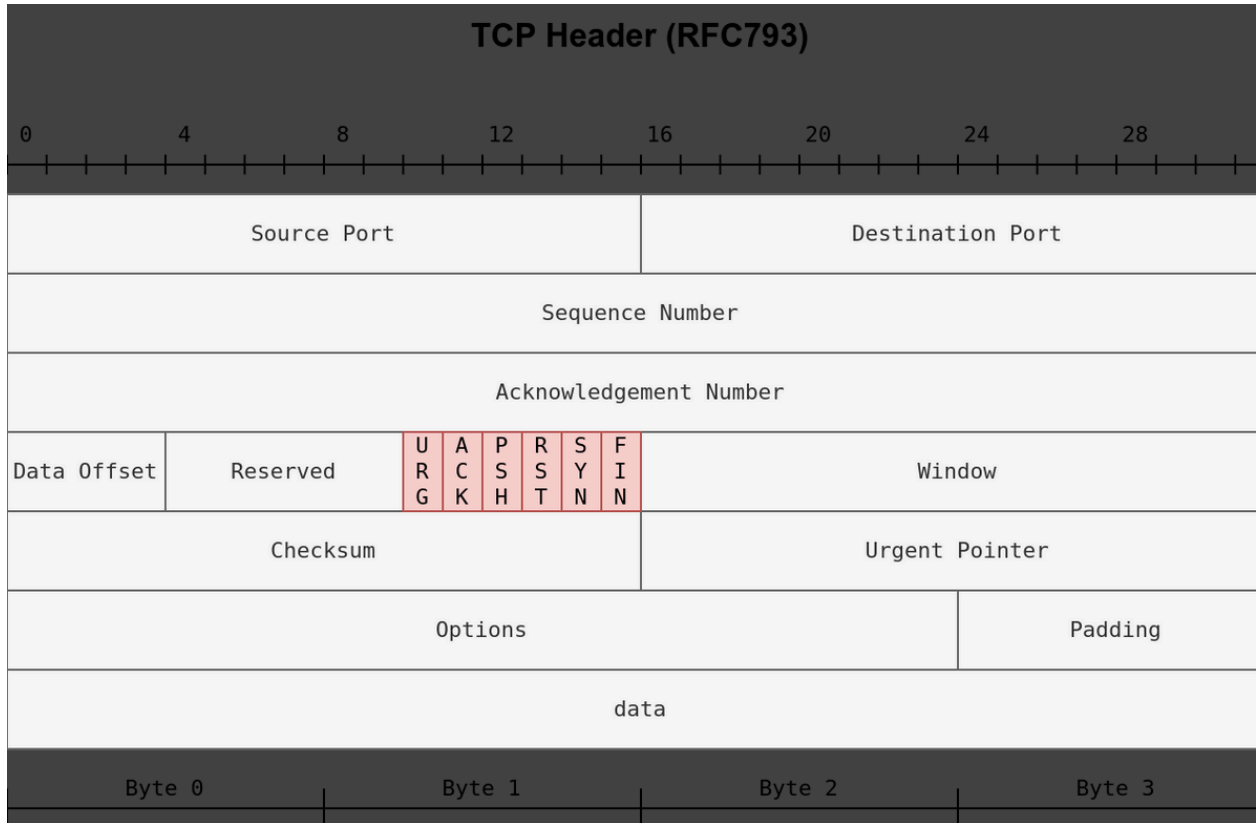
Cevap ⇒ **6**

Soru ⇒ Bir pentester olarak keşfedilmesi en ilginç liman durumu hangisidir?

Cevap ⇒ **Open**

Task 3 TCP Flags (Görev 3 TCP Bayrakları)

Nmap farklı türde TCP port taramalarını destekler. Bu port taramaları arasındaki farkı anlamak için TCP başlığını gözden geçirmemiz gerekir. TCP başlığı, bir TCP segmentinin ilk 24 baytıdır. Aşağıdaki şekil RFC 793'te tanımlanan TCP başlığını göstermektedir. Bu şekil ilk bakışta karmaşık görünebilir; ancak anlaşılması oldukça basittir. İlk satırda kaynak TCP port numarası ve hedef port numarası yer almaktadır. Port numarasına 16 bit (2 bayt) ayrıldığını görebiliriz. İkinci ve üçüncü satırlarda sıra numarası ve onay numarası yer alır. Her satıra 32 bit (4 bayt) ayrılmıştır ve toplam altı satır 24 bayt oluşturur.



Özellikle, Nmap'in ayarlayabileceği veya ayarını kaldırabileceği bayraklara odaklanmamız gerekir. TCP bayraklarını kırmızı ile vurguladık. Bir bayrak bitinin ayarlanması, değerinin 1'e ayarlanması anlamına gelir. Soldan sağa doğru TCP başlık bayrakları şunlardır:

1. **URG**: Acil bayrağı, dosyalanan acil işaretçisinin önemli olduğunu gösterir. Acil işaretçisi, gelen verinin acil olduğunu ve URG bayrağı ayarlanmış bir TCP segmentinin daha önce gönderilen TCP segmentlerini beklemek zorunda kalmadan hemen işlendiğini gösterir.
2. **ACK**: Onay bayrağı, onay numarasının anlamlı olduğunu gösterir. Bir TCP segmentinin alındığını bildirmek için kullanılır.
3. **PSH**: TCP'den verileri uygulamaya hemen iletmesini isteyen itme bayrağı.
4. **RST**: Sıfırlama bayrağı bağlantıyı sıfırlamak için kullanılır. Güvenlik duvarı gibi başka bir cihaz TCP bağlantısını koparmak için gönderebilir. Bu bayrak, bir ana bilgisayara veri gönderildiğinde ve alıcı uçta yanıt verecek bir hizmet olmadığında da kullanılır.
5. **SYN**: Senkronize bayrağı, TCP 3 yönlü el sıkışmasını başlatmak ve sıra numaralarını diğer ana bilgisayarla senkronize etmek için kullanılır. Sıra numarası TCP bağlantısı kurulurken rastgele ayarlanmalıdır.
6. **FIN**: Göndericinin gönderecek başka verisi kalmamıştır.

Sorular

Soru ⇒ Sıfırlama bayrağını hangi 3 harf temsil eder?

Cevap ⇒ **RST**

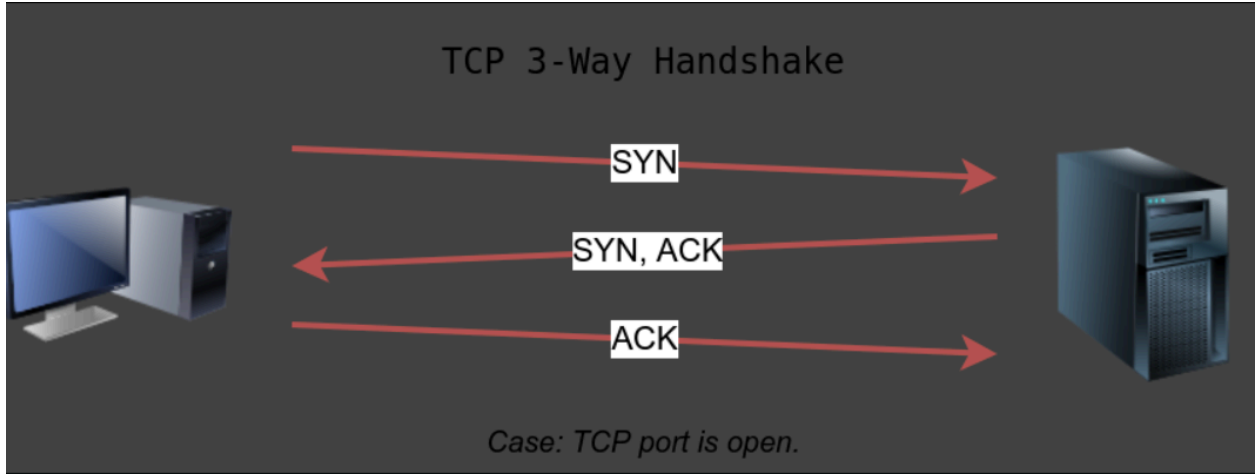
Soru ⇒ Bir TCP bağlantısı başlattığınızda (TCP 3 yönlü el sıkışmasının ilk paketi) hangi bayrağın ayarlanması gerekir?

Cevap ⇒ **SYN**

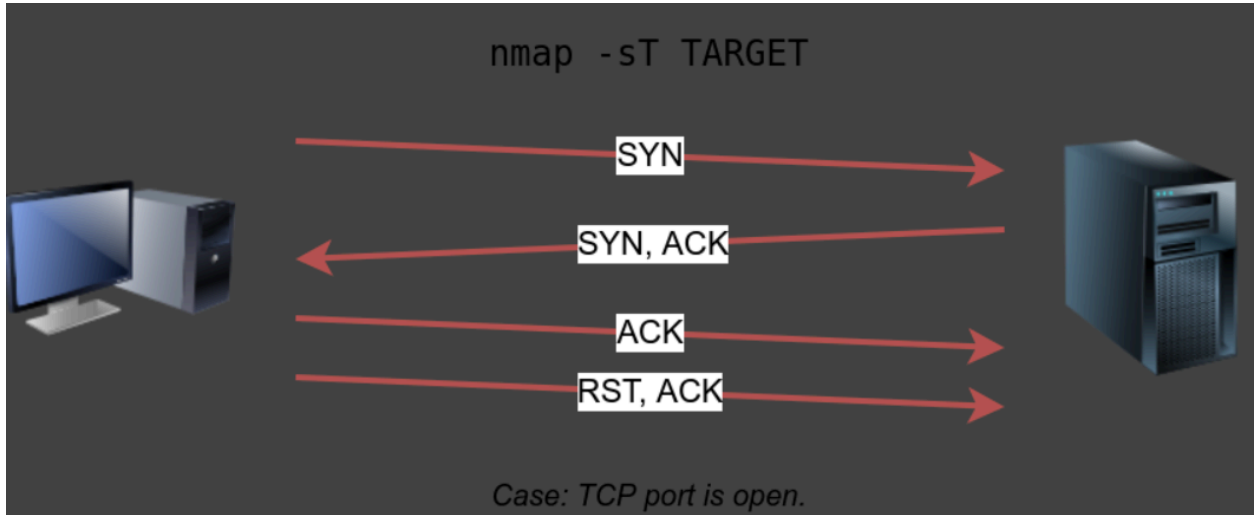
Task 4 TCP Connect Scan (Görev 4 TCP Bağlantı Taraması)

TCP bağlantı taraması, TCP 3 yönlü el sıkışmasını tamamlayarak çalışır. Standart TCP bağlantı kuruluşunda, istemci SYN bayrağı ayarlanmış bir TCP paketi gönderir

ve sunucu port açıksa SYN/ACK ile yanıt verir; son olarak, istemci bir ACK göndererek 3 yönlü el sıkışmayı tamamlar.



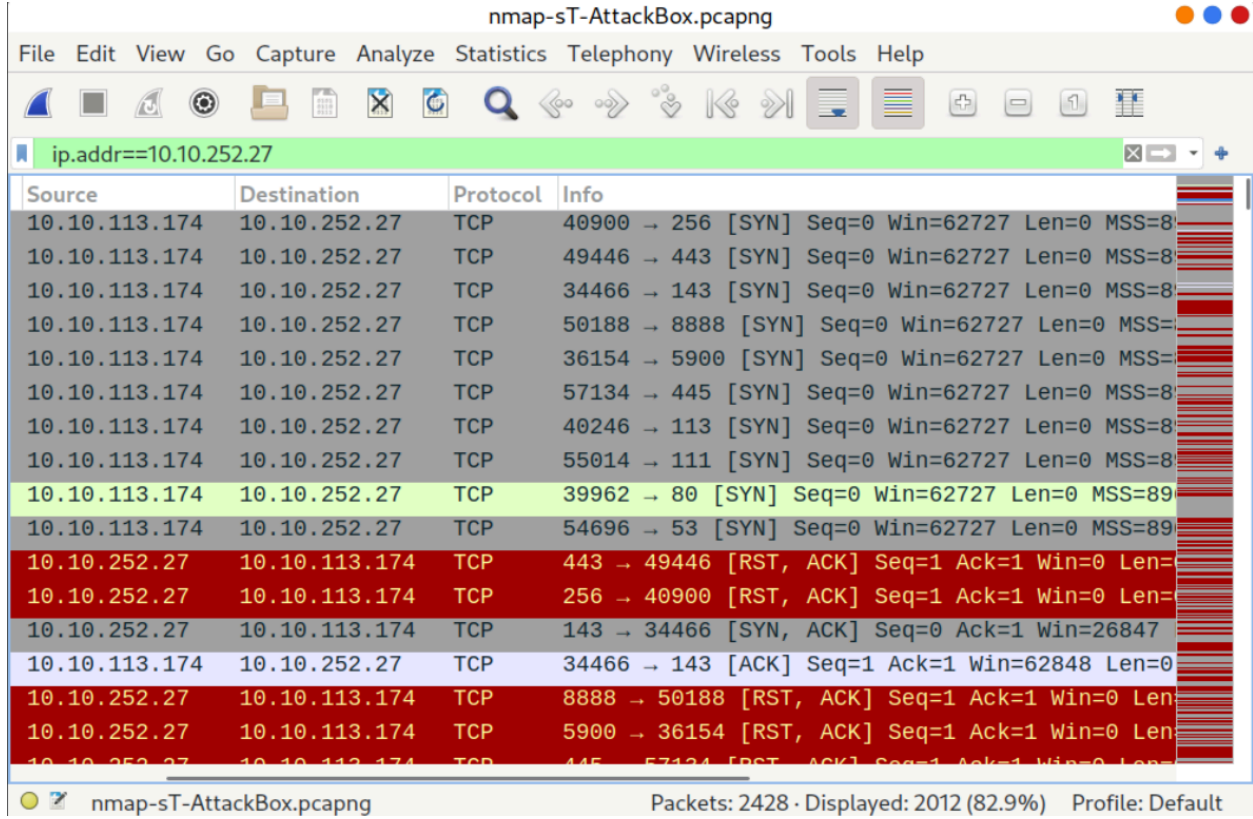
Biz bir TCP bağlantısı kurmakla değil, TCP portunun açık olup olmadığını öğrenmekle ilgileniyoruz. Bu nedenle bağlantı, durumu bir RST/ACK gönderilerek onaylanır onaylanmaz kopar. TCP bağlantı taramasını -sT kullanarak çalıştırmayı seçebilirsiniz.



Ayrıcalıklı bir kullanıcı (root veya sudoer) değilseniz, TCP bağlantı taramasının açık TCP bağlantı noktalarını keşfetmek için mümkün olan tek seçenek olduğunu unutmamak önemlidir.

Aşağıdaki Wireshark paket yakalama penceresinde, Nmap'in SYN bayrağı ayarlı TCP paketlerini 256, 443, 143 gibi çeşitli portlara gönderdiğini görüyoruz.

Varsayılan olarak, Nmap en yaygın 1000 porta bağlanmaya çalışacaktır. Kapalı bir TCP portu, açık olmadığını belirtmek için bir SYN paketine RST/ACK ile yanıt verir. Bu model, TCP ile 3 yönlü bir el sıkışma başlatmaya çalıştığımızda tüm kapalı portlar için tekrarlanacaktır.



The screenshot shows the Nmap packet capture window for 'nmap-sT-AttackBox.pcapng'. The filter is 'ip.addr==10.10.252.27'. The packet list shows a series of SYN packets from 10.10.113.174 to 10.10.252.27. The 10th packet (Seq=39962) is highlighted in green, indicating a successful connection. The 11th packet (Seq=54696) is also highlighted in green. The 12th packet (Seq=443) is highlighted in red, indicating a failed connection (RST, ACK). The 13th packet (Seq=256) is highlighted in red, indicating a failed connection (RST, ACK). The 14th packet (Seq=143) is highlighted in blue, indicating a successful connection (SYN, ACK). The 15th packet (Seq=34466) is highlighted in blue, indicating a successful connection (ACK). The 16th packet (Seq=8888) is highlighted in red, indicating a failed connection (RST, ACK). The 17th packet (Seq=5900) is highlighted in red, indicating a failed connection (RST, ACK). The 18th packet (Seq=445) is highlighted in red, indicating a failed connection (RST, ACK). The status bar at the bottom shows 'Packets: 2428 · Displayed: 2012 (82.9%) Profile: Default'.

Source	Destination	Protocol	Info
10.10.113.174	10.10.252.27	TCP	40900 → 256 [SYN] Seq=0 Win=62727 Len=0 MSS=8
10.10.113.174	10.10.252.27	TCP	49446 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8
10.10.113.174	10.10.252.27	TCP	34466 → 143 [SYN] Seq=0 Win=62727 Len=0 MSS=8
10.10.113.174	10.10.252.27	TCP	50188 → 8888 [SYN] Seq=0 Win=62727 Len=0 MSS=
10.10.113.174	10.10.252.27	TCP	36154 → 5900 [SYN] Seq=0 Win=62727 Len=0 MSS=
10.10.113.174	10.10.252.27	TCP	57134 → 445 [SYN] Seq=0 Win=62727 Len=0 MSS=8
10.10.113.174	10.10.252.27	TCP	40246 → 113 [SYN] Seq=0 Win=62727 Len=0 MSS=8
10.10.113.174	10.10.252.27	TCP	55014 → 111 [SYN] Seq=0 Win=62727 Len=0 MSS=8
10.10.113.174	10.10.252.27	TCP	39962 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=89
10.10.113.174	10.10.252.27	TCP	54696 → 53 [SYN] Seq=0 Win=62727 Len=0 MSS=89
10.10.252.27	10.10.113.174	TCP	443 → 49446 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
10.10.252.27	10.10.113.174	TCP	256 → 40900 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
10.10.252.27	10.10.113.174	TCP	143 → 34466 [SYN, ACK] Seq=0 Ack=1 Win=26847
10.10.113.174	10.10.252.27	TCP	34466 → 143 [ACK] Seq=1 Ack=1 Win=62848 Len=0
10.10.252.27	10.10.113.174	TCP	8888 → 50188 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
10.10.252.27	10.10.113.174	TCP	5900 → 36154 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
10.10.252.27	10.10.113.174	TCP	445 → 57134 [RST, ACK] Seq=1 Ack=1 Win=0 Len=

Port 143'ün açık olduğunu fark ettik, bu yüzden bir SYN/ACK ile cevap verdi ve Nmap bir ACK göndererek 3 yönlü el sıkışmayı tamamladı. Aşağıdaki şekil Nmap ana bilgisayarımız ile hedef sistemin 143 numaralı portu arasında değiş tokuş edilen tüm paketleri göstermektedir. İlk üç paket TCP 3 yönlü el sıkışmasının tamamlanmasıdır. Ardından, dördüncü paket bir RST/ACK paketiyle bunu bozar.

nmap-sT-AttackBox.pcapng

Source	Destination	Protocol	Info
10.10.113.174	10.10.252.27	TCP	34466 → 143 [SYN] Seq=0 Win=62727 Len=0 MSS=8961
10.10.252.27	10.10.113.174	TCP	143 → 34466 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0
10.10.113.174	10.10.252.27	TCP	34466 → 143 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSv
10.10.113.174	10.10.252.27	TCP	34466 → 143 [RST, ACK] Seq=1 Ack=1 Win=62848 Len=0

sT'yi (TCP bağlantı taraması) göstermek için, aşağıdaki komut örneği açık bağlantı noktalarının ayrıntılı bir listesini döndürür.

```
pentester@TryHackMe$ nmap -sT MACHINE_IP
Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 09:53 BST
Nmap scan report for MACHINE_IP
Host is up (0.0024s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
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 0.40 seconds
```

Hızlı modu etkinleştirmek ve taranan port sayısını 1000'den en yaygın 100 porta düşürmek için -F kullanabileceğimizi unutmayın.

Portları rastgele sıralama yerine ardışık sırayla taramak için -r seçeneğinin de eklenebileceğini belirtmek gerekir. Bu seçenek, örneğin bir hedef açıldığında bağlantı noktalarının tutarlı bir şekilde açılıp açılmadığını test ederken kullanışlıdır.

Sorular

Soru ⇒ Sanal makineyi başlatın. AttackBox'ı açın ve terminal üzerinden `nmap -sT MACHINE_IP` komutunu çalıştırın. Son taramamızdan bu yana bu sanal makineye yeni bir hizmet yüklendi. Yukarıdaki taramada hangi port numarası kapalıydı ancak şimdi bu hedef VM'de açık?

Cevap ⇒ **110**

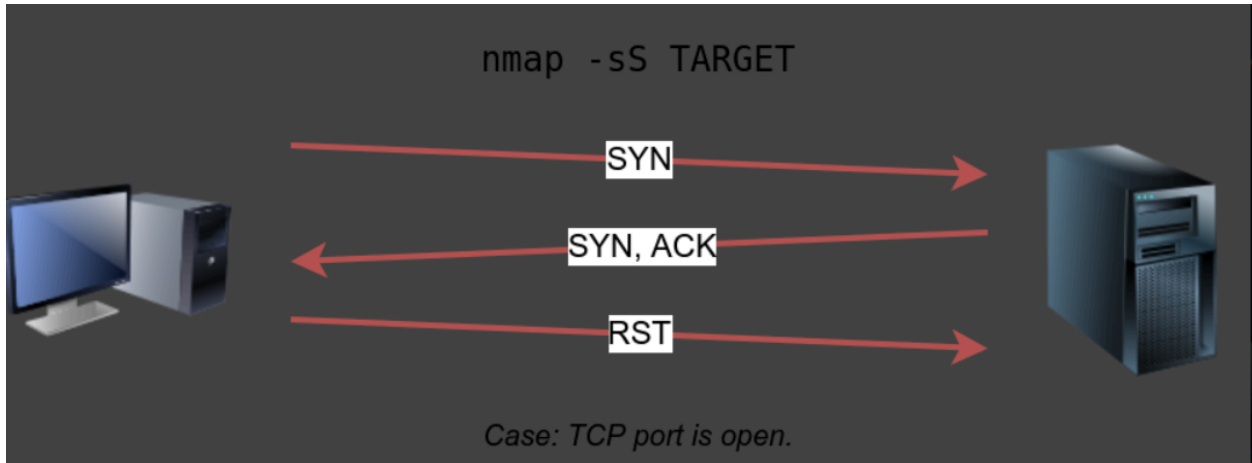
Soru ⇒ Nmap'in yeni yüklenen hizmet hakkındaki tahmini nedir?

Cevap ⇒ Nmap'in yeni yüklenen hizmet hakkındaki tahmini nedir?

Cevap ⇒ **POP3**

Task 5 TCP SYN Scan (Görev 5 TCP SYN Taraması)

Ayrıcalıksız kullanıcılar bağlantı taraması ile sınırlıdır. Ancak, varsayılan tarama modu SYN taramasıdır ve çalıştırmak için ayrıcalıklı (root veya sudoer) bir kullanıcı gerektirir. SYN taraması TCP 3 yönlü el sıkışmasını tamamlamak zorunda değildir; bunun yerine, sunucudan bir yanıt aldığında bağlantıyı keser. Bir TCP bağlantısı kurmadığımız için, bu taramanın günlüğe kaydedilme olasılığını azaltır. Bu tarama türünü `-sS` seçeneğini kullanarak seçebiliriz. Aşağıdaki şekil TCP SYN taramasının TCP 3 yönlü el sıkışmasını tamamlamadan nasıl çalıştığını göstermektedir.



Wireshark'tan alınan aşağıdaki ekran görüntüsü bir TCP SYN taramasını göstermektedir. Kapalı TCP bağlantı noktaları durumunda davranış TCP bağlantı taramasıyla benzerdir.

nmap-sS-AttackBox.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.10.252.27

Source	Destination	Protocol	Info
10.10.113.174	10.10.252.27	TCP	46095 → 1720 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 5900 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 135 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 554 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 199 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 143 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 8080 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.113.174	10.10.252.27	TCP	46095 → 3389 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.252.27	10.10.113.1...	TCP	1720 → 46095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.10.252.27	10.10.113.1...	TCP	25 → 46095 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=6
10.10.113.174	10.10.252.27	TCP	46095 → 25 [RST] Seq=1 Win=0 Len=0
10.10.252.27	10.10.113.1...	TCP	5900 → 46095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
10.10.252.27	10.10.113.1...	TCP	80 → 46095 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=6
10.10.113.174	10.10.252.27	TCP	46095 → 80 [RST] Seq=1 Win=0 Len=0
10.10.252.27	10.10.113.1...	TCP	135 → 46095 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

nmap-sS-AttackBox.pcapng Packets: 2417 · Displayed: 2008 (83.1%) Profile: Default

İki tarama arasındaki farkı daha iyi görmek için aşağıdaki ekran görüntüsüne bakın. Aşağıdaki şeklin üst yarısında, bir TCP bağlantı taraması -sT trafiğini görebiliriz. Herhangi bir açık TCP portu, Nmap'in bağlantıyı kapatmadan önce TCP 3 yönlü el sıkışmasını tamamlamasını gerektirecektir. Aşağıdaki şeklin alt yarısında, bir SYN taramasının -sS'nin TCP 3 yönlü el sıkışmasını nasıl tamamlaması gerektiğini görüyoruz; bunun yerine, bir SYN/ACK paketi alındığında Nmap bir RST paketi gönderir.

nmap-sT-AttackBox.pcapng			
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help			
ip.addr==10.10.252.27 && tcp.port==80			
Source	Destination	Protocol	Info
10.10.113.174	10.10.252.27	TCP	39962 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SAC
10.10.252.27	10.10.113.174	TCP	80 → 39962 [SYN, ACK] Seq=0 Ack=1 Win=26847 Len=0 M
10.10.113.174	10.10.252.27	TCP	39962 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=
10.10.113.174	10.10.252.27	TCP	39962 → 80 [RST, ACK] Seq=1 Ack=1 Win=62848 Len=0 T

nmap-sS-AttackBox.pcapng			
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help			
ip.addr==10.10.252.27 && tcp.port==80			
Source	Destination	Protocol	Info
10.10.113.174	10.10.252.27	TCP	46095 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10.10.252.27	10.10.113.174	TCP	80 → 46095 [SYN, ACK] Seq=0 Ack=1 Win=26883 Len=0
10.10.113.174	10.10.252.27	TCP	46095 → 80 [RST] Seq=1 Win=0 Len=0

TCP SYN taraması, Nmap'i ayrıcalıklı bir kullanıcı olarak çalıştırırken, root olarak çalıştırırken veya sudo kullanırken varsayılan tarama modudur ve çok güvenilir bir seçimdir. Daha önce TCP bağlantı taraması ile bulduğunuz açık portları başarıyla keşfetti, ancak hedefle tam olarak TCP bağlantısı kurulmadı.

```
pentester@TryHackMe$ sudo nmap -sS MACHINE_IP
Starting Nmap 7.60 ( http://nmap.org ) at 2021-08-30 09:53 BST
```

```
Nmap scan report for MACHINE_IP
```

```
Host is up (0.0073s 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

Sorular

Soru ⇒ Sanal makineyi başlatın. Son taramamızdan bu yana bazı yeni sunucu yazılımları yüklendi. AttackBox üzerinde, `nmap -sS MACHINE_IP` komutunu çalıştırmak için terminali kullanın. Yeni açık port nedir?

Cevap ⇒ **6667**

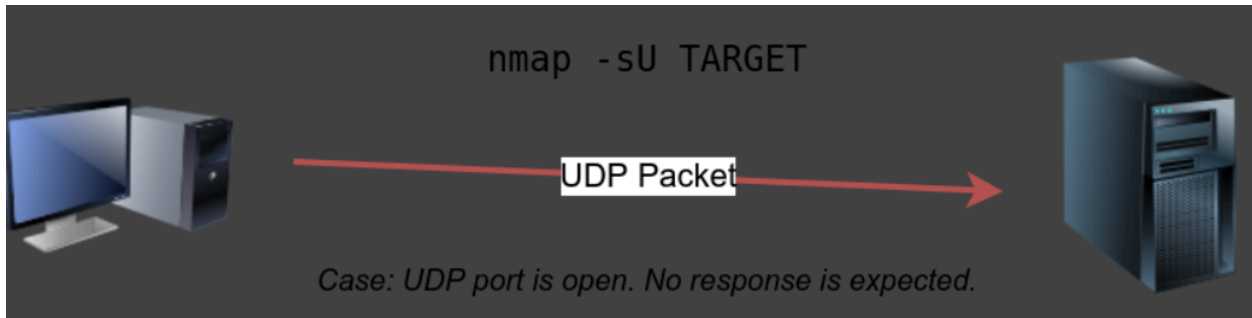
Soru ⇒ Nmap'in hizmet adı tahmini nedir?

Cevap ⇒ **IRC**

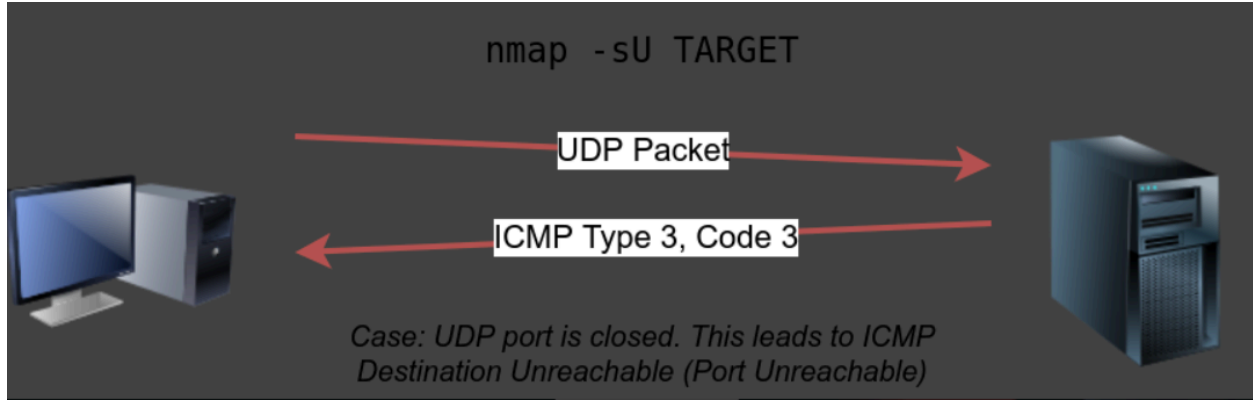
Task 6 UDP Scan (Görev 6 UDP Scan)

UDP bağlantısız bir protokoldür ve bu nedenle bağlantı kurulması için herhangi bir el sıkışma gerektirmez. Bir UDP portunu dinleyen bir hizmetin paketlerimize yanıt vereceğini garanti edemeyiz. Ancak, kapalı bir porta bir UDP paketi gönderilirse, bir ICMP portuna ulaşamıyor hatası (tip 3, kod 3) döndürülür. UDP taramasını `-sU` seçeneğini kullanarak seçebilirsiniz; dahası, bunu başka bir TCP taramasıyla birleştirebilirsiniz.

Aşağıdaki şekil, açık bir UDP portuna bir UDP paketi gönderirsek, karşılığında herhangi bir yanıt bekleyemeyeceğimizi göstermektedir. Bu nedenle, açık bir porta UDP paketi göndermek bize hiçbir şey söylemez.



Ancak, aşağıdaki şekilde gösterildiği gibi, tip 3, hedefe ulaşamıyor ve kod 3, porta ulaşamıyor şeklinde bir ICMP paketi almayı bekliyoruz. Başka bir deyişle, herhangi bir yanıt üretmeyen UDP bağlantı noktaları, Nmap'in açık olarak belirteceği bağlantı noktalarıdır.



Aşağıdaki Wireshark yakalamasında, her kapalı portun bir ICMP paketi hedefe ulaşamaz (port unreachable) oluşturacağını görebiliriz.

Source	Destination	Protocol	Info
10.10.113.174	10.10.252.27	UDP	55642 → 19995 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 27892 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 21834 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 17592 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 16711 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 20 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 42557 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 40019 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 19605 Len=0
10.10.113.174	10.10.252.27	UDP	55642 → 989 Len=0
10.10.252.27	10.10.113.174	ICMP	Destination unreachable (Port unreachable)
10.10.252.27	10.10.113.174	ICMP	Destination unreachable (Port unreachable)
10.10.252.27	10.10.113.174	ICMP	Destination unreachable (Port unreachable)
10.10.252.27	10.10.113.174	ICMP	Destination unreachable (Port unreachable)
10.10.252.27	10.10.113.174	ICMP	Destination unreachable (Port unreachable)
10.10.252.27	10.10.113.174	ICMP	Destination unreachable (Port unreachable)

nmap-sU-AttackBox.pcapng Packets: 87775 · Displayed: 2580 (2.9%) Profile: Default

Bu Linux sunucusuna karşı bir UDP taraması başlatmanın değerli olduğu kanıtlandı ve gerçekten de 111 numaralı portun açık olduğunu öğrendik. Öte yandan, Nmap UDP bağlantı noktası 68'in açık mı yoksa filtrelenmiş mi olduğunu belirleyemiyor.

```
pentester@TryHackMe$ sudo nmap -sU MACHINE_IP
Starting Nmap 7.60 ( https://nmap.org ) at 2021-08-30 09:54 BST
Nmap scan report for MACHINE_IP
Host is up (0.00061s latency).
Not shown: 998 closed ports
PORT      STATE      SERVICE
68/udp    open|filtered dhcpc
111/udp   open       rpcbind
MAC Address: 02:45:BF:8A:2D:6B (Unknown)
```

Nmap done: 1 IP address (1 host up) scanned in 1085.05 seconds

Sorular

Soru ⇒ Sanal makineyi başlatın. AttackBox üzerinde, terminali kullanarak `nmap -sU -F -v MACHINE_IP` komutunu çalıştırın. Son taramadan bu yana yeni bir hizmet yüklendi. Şu anda açık olan UDP bağlantı noktası nedir (İpucu ⇒ UDP port taraması TCP port taramalarından daha uzun sürer. Taramayı hızlandırmak için `-F` bayrağı eklendi (1000 yerine en yaygın 100 tarama). Ayrıca tarama ilerledikçe güncellemeleri almak için `-v` ekledik.)?

Cevap ⇒ 53

Soru ⇒ Nmap'e göre hizmet adı nedir?

Cevap ⇒ domain

Task 7 Fine-Tuning Scope and Performance (Görev 7 Kapsam ve Performansın İnce Ayarı)

Varsayılan 1000 port yerine taramak istediğiniz portları belirtebilirsiniz. Portları belirtmek artık sezgiseldir. Bazı örnekler görelim:

- port listesi: -p22,80,443 22, 80 ve 443 numaralı portları tarayacaktır.
- port aralığı: -p1-1023, 1 ile 1023 arasındaki tüm portları tararken -p20-25, 20 ile 25 arasındaki portları tarayacaktır.

Tüm 65535 portu tarayacak olan -p- kullanarak tüm portların taranmasını isteyebilirsiniz. En yaygın 100 bağlantı noktasını taramak istiyorsanız -F ekleyin. Top-ports 10 kullanmak en yaygın on bağlantı noktasını kontrol edecektir.

Tarama zamanlamasını -T<0-5> kullanarak kontrol edebilirsiniz. -T0 en yavaş (paranoyak), -T5 ise en hızlısıdır. Nmap kılavuz sayfasına göre altı şablon vardır:

- paranoid (0) paranoyak (0)
- sneaky (1) sinsi (1)
- polite (2) kibar (2)
- normal (3) normal (3)
- aggressive (4) agresif (4)
- insane (5) deli (5)

IDS uyarılarından kaçınmak için -T0 veya -T1'i düşünebilirsiniz. Örneğin, -T0 her seferinde bir bağlantı noktasını tarar ve her sonda gönderimi arasında 5 dakika bekler, böylece bir hedefin taranmasının ne kadar süreceğini tahmin edebilirsiniz. Herhangi bir zamanlama belirtmezseniz, Nmap normal -T3'ü kullanır. T5'in hız açısından en agresif olduğunu unutmayın; ancak bu, paket kaybı olasılığının artması nedeniyle tarama sonuçlarının doğruluğunu etkileyebilir. T4'ün genellikle CTF'ler sırasında ve alıştırma hedeflerini taramayı öğrenirken kullanıldığını, -T1'in ise genellikle gizliliğin daha önemli olduğu gerçek çatışmalar sırasında kullanıldığını unutmayın.

Alternatif olarak, --min-rate <sayı> ve --max-rate <sayı> kullanarak paket hızını kontrol etmeyi seçebilirsiniz. Örneğin, --max-rate 10 veya --max-rate=10 tarayıcınızın saniyede ondan fazla paket göndermemesini sağlar.

Ayrıca, --min-parallelism <numprobes> ve --max-parallelism <numprobes> kullanarak problema paralelleştirmesini kontrol edebilirsiniz. Nmap, hangi ana bilgisayarların canlı olduğunu ve hangi bağlantı noktalarının açık olduğunu keşfetmek için hedefleri araştırır; problema paralelleştirme, paralel olarak çalıştırılabilecek bu tür problemlerin sayısını belirtir. Örneğin, --min-parallelism=512

Nmap'i en az 512 probu paralel olarak sürdürmeye iter; bu 512 prob ana bilgisayar keşfi ve açık portlarla ilgilidir.

Sorular

Soru ⇒ 5000-5500 arasındaki tüm TCP bağlantı noktalarını tarama seçeneği nedir (İpucu ⇒ Port aralığını belirtmek için -p seçeneğini kullanarak cevabınızı oluşturun.)?

Cevap ⇒ **-p5000-5500**

Soru ⇒ Nmap'in paralel olarak en az 64 prob çalıştırmalarını nasıl sağlayabilirsiniz (İpucu ⇒)?

Cevap ⇒ **--min-parallelism=64**

Soru ⇒ Nmap'i çok yavaş ve paranoyak yapmak için hangi seçeneği eklersiniz?

Cevap ⇒ **-T0**

Task 8 Summary (Görev 8 Özet)

Bu oda üç tür taramayı kapsıyordu.

Port Scan Type	Example Command
TCP Connect Scan	nmap -sT MACHINE_IP
TCP SYN Scan	sudo nmap -sS MACHINE_IP
UDP Scan	sudo nmap -sU MACHINE_IP

Bu tarama türleri, hedef ana bilgisayarda çalışan TCP ve UDP hizmetlerini keşfetmeye başlamanızı sağlayacaktır.

Option	Purpose
-p-	all ports
-p1-1023	scan ports 1 to 1023
-F	100 most common ports
-r	scan ports in consecutive order
-T<0-5>	-T0 being the slowest and T5 the fastest

<code>--max-rate 50</code>	rate <= 50 packets/sec
<code>--min-rate 15</code>	rate >= 15 packets/sec
<code>--min-parallelism 100</code>	at least 100 probes in parallel

Soru ⇒ Bu odada ele alınan tüm tarama seçeneklerini not aldığınızdan emin olun. Nmap Gelişmiş Port Taramaları odasına katılarak daha gelişmiş port tarama tekniklerini öğrenmenin zamanı geldi.

Cevap ⇒ **Cevap Gerekmemektedir.**