

NMAP

İlk soruyla başlayalım: kim çevrimiçi? Bu görev, canlı sunucuları keşfetmek için Nmap'in nasıl kullanılacağını bulmayı amaçlamaktadır. Nmap, canlı sunucuları keşfetmek için çeşitli karmaşık yollar kullanır.

Başlamadan önce, Nmap'in hedeflerini belirtmek için birden fazla yol kullandığını belirtmeliyiz:

- – **kullanarak IP aralığı:** 192.168.0.1'den 192.168.0.10'a kadar olan tüm IP adreslerini taramak istiyorsanız, 192.168.0.1–10 yazabilirsiniz.
- / **kullanarak IP alt ağı:** Bir alt ağı taramak istiyorsanız, bunu 192.168.0.1/24 olarak ifade edebilirsiniz ve bu da 192.168.0.0–255'e eşdeğer olacaktır.
- **Ana bilgisayar adı:** Hedefinizi ana bilgisayar adına göre de belirtebilirsiniz, örneğin, gelisim.edu

Diyelim ki bir ağdaki çevrimiçi ana bilgisayarları keşfetmek istiyorsunuz. Nmap, –sn seçeneğini, yani ping taramasını sunar. Ancak bunun ping gibi sınırlı olmasını beklemeyin. Bunu eylem halinde görelim.

Yerel” Bir Ağın Taranması

Sistemimiz 192.168.66.89 IP adresine sahip olup 192.168.66.0/24 ağına aittir. Aşağıdaki terminalde hedef ağ 192.168.11.0/24'ü tarıyoruz; burada yerel sistemimizi hedef bilgisayarlardan ayıran iki veya daha fazla yönlendirici (atlama) bulunmaktadır.

```
root@ip-10-10-70-0: ~  
File Edit View Search Terminal Help  
root@ip-10-10-70-0:~# nmap -sn 192.168.11.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-29 13:20 GMT
```

Nmap çıktısı beş ana bilgisayarın çalıştığını gösteriyor.

```
root@tryhackme:~# nmap -sn 192.168.11.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2024-08-07 14:05 EEST
Nmap scan report for 192.168.11.1
Host is up (0.018s latency).
Nmap scan report for 192.168.11.151
Host is up (0.0013s latency).
Nmap scan report for 192.168.11.152
Host is up (0.13s latency).
Nmap scan report for 192.168.11.154
Host is up (0.22s latency).
Nmap scan report for 192.168.11.155
Host is up (2.3s latency).
Nmap done: 256 IP addresses (5 hosts up) scanned in 10.67 seconds
```

Peki Nmap bunu nasıl keşfetti? Daha fazla bilgi edinmek için Nmap tarafından oluşturulan bazı örnek trafiğe bakalım. Aşağıdaki ekran görüntüsünde iki ana bilgisayardan gelen yanıtları görebiliyoruz:

- 192.168.11.1 yayında ve ICMP yankı (ping) isteğine yanıt verdi.
- 192.168.11.2 kapalı görünüyor. Nmap iki ICMP yankı (ping) isteği, iki ICMP zaman damgası isteği, SYN bayrağı ayarlanmış 443 portuna iki TCP paketi ve ACK bayrağı ayarlanmış 80 portuna iki TCP paketi gönderdi.

Hedef hiçbirine yanıt vermedi. 192.168.11.151 yönlendiricisinden birkaç ICMP hedef ulaşılamaz paketi gözlemliyoruz.

Nmap-PingScan-sn-remote-selected.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.66.89	192.168.11.1	ICMP	42	Echo (ping) request id=0x3b0e, seq=0/0, ttl=53 (reply i
2	0.000029977	192.168.66.89	192.168.11.2	ICMP	42	Echo (ping) request id=0xae0d, seq=0/0, ttl=49 (no resp
3	0.017817302	192.168.11.1	192.168.66.89	ICMP	42	Echo (ping) reply id=0x3b0e, seq=0/0, ttl=63 (request
4	1.195624726	192.168.66.89	192.168.11.2	ICMP	42	Echo (ping) request id=0x143c, seq=0/0, ttl=43 (no resp
5	1.213791211	192.168.66.89	192.168.11.2	TCP	58	55377 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	1.216488102	192.168.66.89	192.168.11.2	TCP	54	55377 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
7	1.240929833	192.168.66.89	192.168.11.2	ICMP	54	Timestamp request id=0x63e0, seq=0/0, ttl=55
8	1.600532869	192.168.66.89	192.168.11.2	TCP	58	55379 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	1.602999177	192.168.66.89	192.168.11.2	TCP	54	55379 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
10	1.627094328	192.168.66.89	192.168.11.2	ICMP	54	Timestamp request id=0xf311, seq=0/0, ttl=39
11	3.015669339	192.168.11.151	192.168.66.89	ICMP	70	Destination unreachable (Host unreachable)
12	3.015669409	192.168.11.151	192.168.66.89	ICMP	70	Destination unreachable (Host unreachable)
13	3.015669469	192.168.11.151	192.168.66.89	ICMP	86	Destination unreachable (Host unreachable)
14	3.015669529	192.168.11.151	192.168.66.89	ICMP	82	Destination unreachable (Host unreachable)
15	3.015669589	192.168.11.151	192.168.66.89	ICMP	82	Destination unreachable (Host unreachable)
16	3.015669649	192.168.11.151	192.168.66.89	ICMP	86	Destination unreachable (Host unreachable)
17	3.016195896	192.168.11.151	192.168.66.89	ICMP	82	Destination unreachable (Host unreachable)
18	3.016195967	192.168.11.151	192.168.66.89	ICMP	82	Destination unreachable (Host unreachable)

Frame 12: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on in
Ethernet II, Src: 44:df:65:d8:fe:6c, Dst: 02:83:1e:40:5d:17
Internet Protocol Version 4, Src: 192.168.11.151, Dst: 192.168.66.89
Internet Control Message Protocol
Type: 3 (Destination unreachable)
Code: 1 (Host unreachable)
Checksum: 0xfcf6 [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 192.168.66.89, Dst: 192.168.11.2
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0xe3c3 [unverified] [in ICMP error packet]
[Checksum Status: Unverified]
Identifier (BE): 5180 (0x143c)
Identifier (LE): 15380 (0x3c14)
Sequence Number (BE): 0 (0x0000)
Sequence Number (LE): 0 (0x0000)

Internet Protocol Version 4 (ip), 20 bytes

Packets: 18 · Displayed: 18 (100.0%) Profile: Default

Nmap **-sL** seçeneğiyle bir liste taraması sunar. Bu tarama aslında tarama yapmadan sadece taranacak hedefleri listeler.Örneğin, nmap -sL 192.168.0.1/24 taranacak 256 hedefi listeleyecektir. Bu seçenek gerçek taramayı çalıştırmadan önce hedefleri onaylamaya yardımcı olur.

-sn	Çalışan servisleri keşfetmeye çalışmadan canlı sunucuları keşfetmeyi amaçlar.Çok fazla gürültüye neden olmadan bir ağdaki cihazları keşfetmek istiyorsanız bu tarama faydalı olabilir.
-sL	bir liste taraması sunar. Bu tarama aslında tarama yapmadan sadece taranacak hedefleri listeler.
-sU	Udp servislerinin taramasını yapar, gizli şekilde ilerler.
-F	Hızlı mod – en yaygın 100 portu tarar
-p[range]	Bir port numarası aralığı belirtir – -p- tüm portları tarar
-sT	TCP bağlantı taraması – tam üç yönlü el sıkışmanın ilk adımı
-sS	Syn taraması yaptırır, tarama gizli şekilde ilerler.

Yaygın ağ hizmetleri arasında genellikle TCP portları 80 ve 443'ü dinleyen web sunucuları ve genellikle UDP (ve TCP) portları 53'ü dinleyen DNS sunucuları bulunur.

TCP'nin tasarımı gereği 65.535 portu vardır ve aynısı UDP için de geçerlidir. Hangi portların kendisine bağlı bir hizmeti olduğunu nasıl belirleyebiliriz? Öğrenelim.

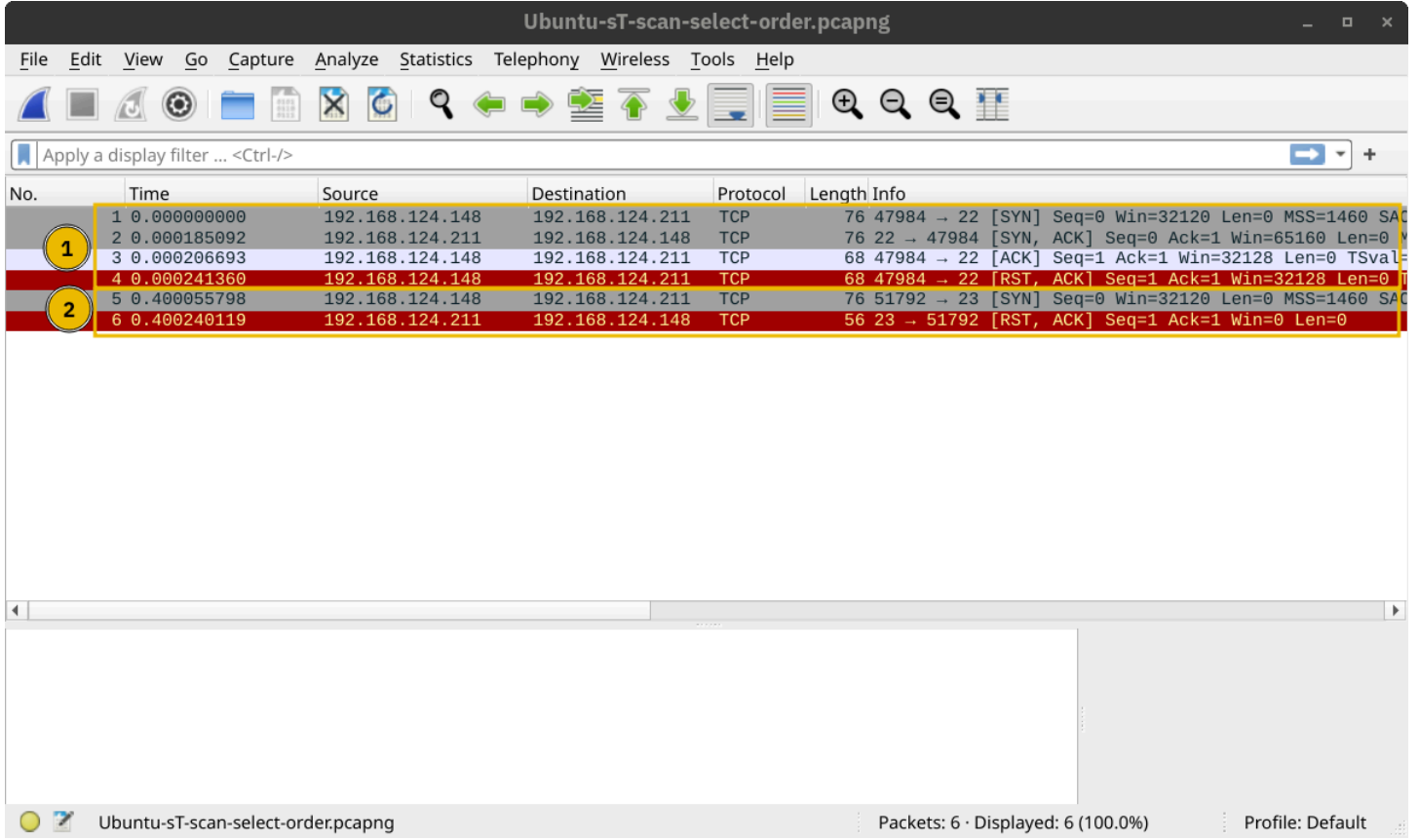
TCP Portlarını Tarama

Bir TCP portunun açık olup olmadığını anlamamanın en kolay ve temel yolu, o porta **telnet** bağlantısı kurmaya çalışmaktır. Eğer Telnet istemcisi ile tarama yapmayı düşünüyorsanız, her hedef port ile bir TCP bağlantısı kurmayı deneyin.

Başka bir deyişle, her hedef portla TCP üç yönlü el sıkışmasını tamamlamaya çalışırsınız; ancak, yalnızca açık TCP portları uygun şekilde yanıt verir ve bir TCP bağlantısının kurulmasına izin verir.

Bağlantı Taraması

Bağlantı taraması -sT kullanılarak tetiklenebilir. Her hedef TCP portuyla TCP üç yönlü el sıkışmasını tamamlamaya çalışır. TCP portu açık çıkarsa ve Nmap başarılı bir şekilde bağlanırsa, Nmap kurulan bağlantıyı keser.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.148	192.168.124.211	TCP	76	47984 → 22 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SA
2	0.000185092	192.168.124.211	192.168.124.148	TCP	76	22 → 47984 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 Y
3	0.000206693	192.168.124.148	192.168.124.211	TCP	68	47984 → 22 [ACK] Seq=1 Ack=1 Win=32128 Len=0 TSval=
4	0.000241360	192.168.124.148	192.168.124.211	TCP	68	47984 → 22 [RST, ACK] Seq=1 Ack=1 Win=32128 Len=0 I
5	0.400055798	192.168.124.148	192.168.124.211	TCP	76	51792 → 23 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SA
6	0.400240119	192.168.124.211	192.168.124.148	TCP	56	23 → 51792 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

SYN Tarama (Gizlilik)

Hedef TCP portuna bağlanmaya çalışan, yani üçlü bir el sıkışmayı tamamlamaya çalışan bağlantı taramasının aksine, SYN taraması yalnızca ilk adımı yürütür: bir TCP SYN paketi gönderir.

Sonuç olarak, TCP üç yönlü el sıkışması asla tamamlanmaz. Avantajı, bağlantı asla kurulmadığından bunun daha az günlük kaydına yol açması beklenmesidir ve bu nedenle nispeten gizli bir tarama olarak kabul edilir.

-sS bayrağını kullanarak SYN taramasını seçebilirsiniz.

Aşağıdaki ekran görüntüsünde, aynı sistemi 22 numaralı port açıkken tarıyoruz. 1 ile işaretlenen kısım, dinleme hizmetinin bir TCP SYN-ACK paketiyle yanıt verdiğini gösteriyor.

Ancak Nmap, TCP üçlü el sıkışmasını tamamlamak yerine TCP RST paketiyle yanıt verdi. 2 ile işaretlenen kısım kapalı bir porta TCP bağlantı girişimini gösterir. Bu durumda, paket değişimi bağlantı taramasındakiyle aynıdır.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.148	192.168.124.211	TCP	60	56186 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2	0.000225431	192.168.124.211	192.168.124.148	TCP	60	22 → 56186 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0
3	0.000247493	192.168.124.148	192.168.124.211	TCP	56	56186 → 22 [RST] Seq=1 Win=0 Len=0
4	0.400493120	192.168.124.148	192.168.124.211	TCP	60	56186 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	0.400734380	192.168.124.211	192.168.124.148	TCP	56	23 → 56186 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

UDP Portlarını Tarama

Çoğu hizmet iletişim için TCP kullansa da, birçoğu UDP kullanır. Örnekler arasında DNS, DHCP, NTP (Ağ Zaman Protokolü), SNMP (Basit Ağ Yönetim Protokolü) ve VoIP (IP üzerinden Ses) bulunur.

UDP, bir bağlantı kurmayı ve daha sonra bağlantıyı kesmeyi gerektirmez. Ayrıca, canlı yayınlar gibi gerçek zamanlı iletişim için çok uygundur. Tüm bunlar, UDP portlarını dinleyen servisleri taramayı ve keşfetmeyi düşünmeniz için sebeplerdir.

Nmap, UDP servislerini taramak için `-sU` seçeneğini sunar. UDP, TCP'den daha basit olduğu için trafiğin farklı olmasını bekleriz.

Aşağıdaki ekran görüntüsü, Nmap'in kapalı UDP portlarına UDP paketleri göndermesiyle oluşan birkaç ICMP hedef ulaşılamaz (port ulaşılamaz) yanıtını göstermektedir.

Ubuntu-sU-scan-select.pcapng					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl-/>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.124.148	192.168.124.211	UDP	42 50511 → 55 Len=0
2	0.000176541	192.168.124.148	192.168.124.211	UDP	42 50511 → 50 Len=0
3	0.000183264	192.168.124.148	192.168.124.211	UDP	42 50511 → 59 Len=0
4	0.000189546	192.168.124.148	192.168.124.211	UDP	42 50511 → 56 Len=0
5	0.000195417	192.168.124.148	192.168.124.211	UDP	42 50511 → 54 Len=0
6	0.000206508	192.168.124.148	192.168.124.211	DNS	72 Standard query 0x0006 TXT version.bind
7	0.000212339	192.168.124.148	192.168.124.211	DNS	54 Server status request 0x0000
8	0.000218140	192.168.124.148	192.168.124.211	UDP	42 50511 → 58 Len=0
9	0.000224051	192.168.124.148	192.168.124.211	UDP	42 50511 → 51 Len=0
10	0.000231174	192.168.124.148	192.168.124.211	UDP	42 50511 → 57 Len=0
11	0.000237857	192.168.124.148	192.168.124.211	UDP	42 50511 → 52 Len=0
12	0.000252264	192.168.124.211	192.168.124.148	ICMP	70 Destination unreachable (Port unreachable)
13	0.000449102	192.168.124.211	192.168.124.148	ICMP	70 Destination unreachable (Port unreachable)
14	0.000449222	192.168.124.211	192.168.124.148	ICMP	70 Destination unreachable (Port unreachable)
15	0.000449272	192.168.124.211	192.168.124.148	ICMP	70 Destination unreachable (Port unreachable)
16	0.000449322	192.168.124.211	192.168.124.148	ICMP	70 Destination unreachable (Port unreachable)
17	0.000449373	192.168.124.211	192.168.124.148	ICMP	100 Destination unreachable (Port unreachable)
18	1.101627483	192.168.124.148	192.168.124.211	UDP	42 50513 → 52 Len=0
19	1.101661676	192.168.124.148	192.168.124.211	UDP	42 50513 → 57 Len=0
20	1.101670713	192.168.124.148	192.168.124.211	UDP	42 50513 → 51 Len=0
21	1.101684389	192.168.124.148	192.168.124.211	UDP	42 50513 → 58 Len=0
22	1.101927786	192.168.124.211	192.168.124.148	ICMP	70 Destination unreachable (Port unreachable)
<p>Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, id 0</p> <p>Ethernet II, Src: 52:54:00:7c:d3:5b, Dst: 52:54:00:54:fa:4e</p> <p>Internet Protocol Version 4, Src: 192.168.124.148, Dst: 192.168.124.211</p> <p>User Datagram Protocol, Src Port: 50511, Dst Port: 59</p>					
<p>0000 52 54 00 54 fa 4e 52 54</p> <p>0010 00 1c 65 b1 00 00 2d 11</p> <p>0020 7c d3 c5 4f 00 3b 00 08</p>					
<p>Ubuntu-sU-scan-select.pcapng</p> <p>Packets: 31 · Displayed: 31 (100.0%)</p> <p>Profile: Default</p>					

Hedef Bağlantı Noktalarını Sınırlandırma

Nmap varsayılan olarak en yaygın 1.000 portu tarar. Ancak, bu aradığınız şey olmayabilir. Bu nedenle, Nmap size birkaç seçenek daha sunar.

- **-F**, varsayılan 1000 yerine en yaygın 100 portu tarayan Hızlı mod anlamına gelir.
- **-p[aralık]** taranacak port aralığını belirtmenize olanak tanır. Örneğin, **-p10-1024** 10 numaralı porttan 1024 numaralı porta kadar tarar, **-p-25** ise 1 ile 25 arasındaki tüm portları tarar. **p-** seçeneğinin tüm portları taradığını ve **-p1-65535** ile aynı olduğunu ve mümkün olduğunca kapsamlı olmak istiyorsanız en iyi seçenek olduğunu unutmayın.