

NMAP

Nmap tarama hızını ve zamanlamasını kontrol etmek için çeşitli seçenekler sunar. Taramanızı normal hızında çalıştırmak bir IDS veya diğer güvenlik çözümlerini tetikleyebilir. Bir taramanın ne kadar hızlı gitmesi gerektiğini kontrol etmek mantıklıdır.

Nmap size altı zamanlama şablonu verir ve isimler her şeyi söyler:

- paranoyak (0),
- sinsi (1),
- kibar (2),
- normal (3),
- saldırgan (4) ve
- çılgın (5).

Zamanlama şablonunu adına veya numarasına göre seçebilirsiniz.

Örneğin, en yavaş zamanlamayı seçmek için -T0 (veya -T 0) veya -T paranoid ekleyebilirsiniz.

Aşağıdaki Nmap taramalarında, en yaygın 100 TCP portunu hedefleyen bir SYN taraması başlatıyoruz, **nmap -sS 10.10.57.129 -F**.

```
root@ip-10-10-133-184:~# nmap -sS 10.10.57.129 -F
Starting Nmap 7.80 ( https://nmap.org ) at 2024-11-29 17:36 GMT
Nmap scan report for ip-10-10-57-129.eu-west-1.compute.internal (10.10.57.129)
Host is up (0.00013s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
22/tcp    open  ssh
8008/tcp  open  http
MAC Address: 02:7E:14:35:33:BB (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
```

Taramayı farklı zamanlamalarla tekrarladık: T0, T1, T2, T3 ve T4.

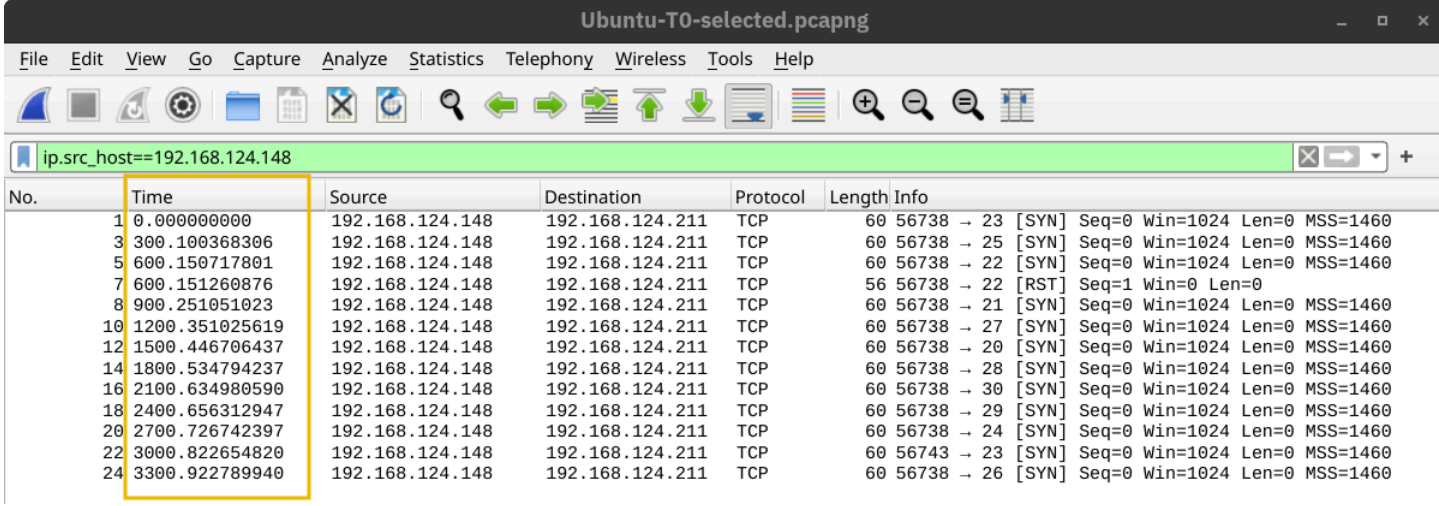
Laboratuvar kurulumumuzda, Nmap 100 portu taramak için farklı zaman

dilimleri aldı.

Aşağıdaki tablo size bir fikir verebilir, ancak ağ kurulumunuza ve hedef sisteme bağlı olarak farklı sonuçlar elde edebilirsiniz.

Zamanlama	Toplam Süre
T0 (paranoyak)	9.8 saat
T1 (gizlice)	27.53 dakika
T2 (kibar)	40.56 saniye
T3 (normal)	0.15 saniye
T4 (saldırgan)	0.13 saniye

Aşağıdaki ekran görüntülerinde, Nmap'in farklı paketleri gönderdiği zamanı görebiliriz. Aşağıdaki ekran görüntüsünde, tarama zamanlaması T0 olduğunda, Nmap'in bir sonraki porta geçmeden önce 5 dakika beklediğini görebiliriz.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.148	192.168.124.211	TCP	60	56738 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	300.100368306	192.168.124.148	192.168.124.211	TCP	60	56738 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	600.150717801	192.168.124.148	192.168.124.211	TCP	60	56738 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	600.151260876	192.168.124.148	192.168.124.211	TCP	56	56738 → 22 [RST] Seq=1 Win=0 Len=0
8	900.251051023	192.168.124.148	192.168.124.211	TCP	60	56738 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	1200.351025619	192.168.124.148	192.168.124.211	TCP	60	56738 → 27 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	1500.446706437	192.168.124.148	192.168.124.211	TCP	60	56738 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	1800.534794237	192.168.124.148	192.168.124.211	TCP	60	56738 → 28 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	2100.634980590	192.168.124.148	192.168.124.211	TCP	60	56738 → 30 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	2400.656312947	192.168.124.148	192.168.124.211	TCP	60	56738 → 29 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	2700.726742397	192.168.124.148	192.168.124.211	TCP	60	56738 → 24 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	3000.822654820	192.168.124.148	192.168.124.211	TCP	60	56743 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	3300.922789940	192.168.124.148	192.168.124.211	TCP	60	56738 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Aşağıdaki ekran görüntüsünde, zamanlamayı T1 olarak ayarladığımızda Nmap her iki port arasında 15 saniye bekledi.

Ubuntu-T1-selected.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src_host==192.168.124.148						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.148	192.168.124.211	TCP	60	40815 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000461084	192.168.124.148	192.168.124.211	TCP	56	40815 → 22 [RST] Seq=1 Win=0 Len=0
4	15.014990001	192.168.124.148	192.168.124.211	TCP	60	40815 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	30.030033139	192.168.124.148	192.168.124.211	TCP	60	40815 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	45.045108536	192.168.124.148	192.168.124.211	TCP	60	40815 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	60.060110348	192.168.124.148	192.168.124.211	TCP	60	40815 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	75.075286251	192.168.124.148	192.168.124.211	TCP	60	40815 → 28 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	90.090463412	192.168.124.148	192.168.124.211	TCP	60	40815 → 27 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	105.105599575	192.168.124.148	192.168.124.211	TCP	60	40815 → 29 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	120.120753991	192.168.124.148	192.168.124.211	TCP	60	40815 → 30 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	135.135849228	192.168.124.148	192.168.124.211	TCP	60	40815 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	150.151027421	192.168.124.148	192.168.124.211	TCP	60	40820 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
24	165.166601930	192.168.124.148	192.168.124.211	TCP	60	40815 → 24 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Daha sonra T2 için bekleme süresi aşağıda görüldüğü gibi 0,4 saniyeye düştü.

Ubuntu-T2-selected.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src_host==192.168.124.148						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.148	192.168.124.211	TCP	60	62177 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.400617264	192.168.124.148	192.168.124.211	TCP	60	62177 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	0.801103901	192.168.124.148	192.168.124.211	TCP	60	62177 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	1.201808968	192.168.124.148	192.168.124.211	TCP	60	62177 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	1.202321728	192.168.124.148	192.168.124.211	TCP	56	62177 → 22 [RST] Seq=1 Win=0 Len=0
10	1.602305554	192.168.124.148	192.168.124.211	TCP	60	62177 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
12	2.003089587	192.168.124.148	192.168.124.211	TCP	60	62177 → 28 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
14	2.403667835	192.168.124.148	192.168.124.211	TCP	60	62177 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
16	2.804154051	192.168.124.148	192.168.124.211	TCP	60	62177 → 27 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
18	3.204791920	192.168.124.148	192.168.124.211	TCP	60	62177 → 29 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	3.605332658	192.168.124.148	192.168.124.211	TCP	60	62177 → 24 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
22	4.005888721	192.168.124.148	192.168.124.211	TCP	60	62177 → 30 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Son olarak varsayılan durumda, T3'te, Nmap'in aşağıda gösterildiği gibi olabildiğince hızlı çalıştığı görülmüyordu.

Ubuntu-T3-selected.pcapng						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
ip.src_host==192.168.124.148						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.124.148	192.168.124.211	TCP	60	42990 → 22 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
2	0.000019347	192.168.124.148	192.168.124.211	TCP	60	42990 → 25 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
3	0.000030146	192.168.124.148	192.168.124.211	TCP	60	42990 → 21 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
4	0.000041207	192.168.124.148	192.168.124.211	TCP	60	42990 → 23 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
5	0.000051466	192.168.124.148	192.168.124.211	TCP	60	42990 → 24 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
6	0.000059321	192.168.124.148	192.168.124.211	TCP	60	42990 → 30 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
7	0.000067897	192.168.124.148	192.168.124.211	TCP	60	42990 → 28 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	0.000077335	192.168.124.148	192.168.124.211	TCP	60	42990 → 26 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
9	0.000086001	192.168.124.148	192.168.124.211	TCP	60	42990 → 29 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	0.000094277	192.168.124.148	192.168.124.211	TCP	60	42990 → 27 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
13	0.000215864	192.168.124.148	192.168.124.211	TCP	56	42990 → 22 [RST] Seq=1 Win=0 Len=0
22	0.000319799	192.168.124.148	192.168.124.211	TCP	60	42990 → 20 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

İkinci yararlı seçenek paralel servis araştırmalarının sayısıdır. Paralel araştırmaların sayısı **--min-parallelism <numprobes> ve --max-parallelism**

<numprobes> ile kontrol edilebilir.

Bu seçenekler, bir ana bilgisayar grubu için aynı anda etkin olan TCP ve UDP bağlantı noktası araştırmalarının sayısının minimum ve maksimumunu ayarlamak için kullanılabilir.

Benzer bir yardımcı seçenek **--min-rate <sayı> ve --max-rate <sayı>**'dır. Adlarından da anlaşılacağı gibi, nmap'in paketleri gönderdiği minimum ve maksimum oranları kontrol edebilirler.İsimlerinden de anlaşılacağı gibi, nmap'in paketleri gönderdiği minimum ve maksimum oranları kontrol edebilirler.

Ele alacağımız son seçenek **--host-timeout <time>**'dır. Bu seçenek beklemeye razı olduğunuz maksimum süreyi belirtir ve yavaş ana bilgisayarlar veya yavaş ağ bağlantıları olan ana bilgisayarlar için uygundur.