



# **Nmap for Pentester**

## **Timing & Performance**

## Contents

Nmap Timing Template .....	3
Maximum Retries (–max-retries) .....	3
Host-timeout .....	6
Hostgroup .....	7
Scan delay .....	8
Maximum rate (max-rate) .....	9
Minimum rate (min-rate) .....	11
Parallelism .....	12
Round trip timeout .....	13
Max-rtt-timeout .....	15
Initial Round trip timeout .....	16

## Nmap Timing Template

As we have seen, Nmap has multiple timing templates that can be used differently according to the requirements. Click [here](#) to check the timing scan article. Let's see what's inside the timing template. To get the description of the timing template, we'll use the `-d` attribute.

```
nmap -T4 -d -p21-25 192.168.1.139
```

Here we have multiple arguments that collectively make a timing template. Let's have a look at them one by one.

- Host-groups
- Rtt-timeouts
- Scan-delay
- Max-retries
- Min-rates
- Parallelism

```
root@kali:~# nmap -T4 -d -p21-25 192.168.1.139

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:37 EDT
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 500, min 100, max 1250
max-scan-delay: TCP 10, UDP 1000, SCTP 10
parallelism: min 0, max 0
max-retries: 6, host-timeout: 0
min-rate: 0, max-rate: 0
-----
```

## Maximum Retries (`--max-retries`)

`-max-retries` specifies the number of times a packet is to be resent on a port to check if it is open or closed. If `-max-retries` is set to 0, the packets will be sent only once on a port and no retries will be made.

```
nmap -p21-25 192.168.1.139 --max-retries 0
```

```

root@kali:~# nmap -p21-25 192.168.1.139 --max-retries 0

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:40 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00053s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds

```

Here in Wireshark, we can see that 1-1 TCP SYN packet sent to each port from **source:** 192.168.1.126 to **destination:** 192.168.1.139 are not sent again.

No.	Time	Source	Destination	Protocol	Length	Info
...	14.630333528	192.168.1.126	192.168.1.139	TCP	58	40101 → 21 [SYN] Seq=0
...	14.630502138	192.168.1.126	192.168.1.139	TCP	58	40101 → 22 [SYN] Seq=0
...	14.630632889	192.168.1.126	192.168.1.139	TCP	58	40101 → 25 [SYN] Seq=0
...	14.630754074	192.168.1.126	192.168.1.139	TCP	58	40101 → 23 [SYN] Seq=0
...	14.630861979	192.168.1.139	192.168.1.126	TCP	60	21 → 40101 [SYN, ACK] Seq=0
...	14.630895140	192.168.1.126	192.168.1.139	TCP	54	40101 → 21 [RST] Seq=1
...	14.630998982	192.168.1.139	192.168.1.126	TCP	60	22 → 40101 [SYN, ACK] Seq=0
...	14.631018799	192.168.1.126	192.168.1.139	TCP	54	40101 → 22 [RST] Seq=1
...	14.631088195	192.168.1.139	192.168.1.126	TCP	60	25 → 40101 [SYN, ACK] Seq=0
...	14.631104983	192.168.1.126	192.168.1.139	TCP	54	40101 → 25 [RST] Seq=1
...	14.631183660	192.168.1.139	192.168.1.126	TCP	60	23 → 40101 [SYN, ACK] Seq=0
...	14.631203172	192.168.1.126	192.168.1.139	TCP	54	40101 → 23 [RST] Seq=1
...	14.631332434	192.168.1.126	192.168.1.139	TCP	58	40101 → 24 [SYN] Seq=0
...	14.631694887	192.168.1.139	192.168.1.126	TCP	60	24 → 40101 [SYN, ACK] Seq=0
...	14.631727933	192.168.1.126	192.168.1.139	TCP	54	40101 → 24 [RST] Seq=1

Now we will apply a small firewall rule on the target machine so that the packets get blocked if they come at a faster rate.

```

sudo iptables -I INPUT -p tcp -m state --state NEW -m recent --set
sudo iptables -I INPUT -p tcp -m state --state NEW -m recent --update --seconds 1 --hitcount 1 -j DROP

```

```

xander@ubuntu:~$ sudo iptables -I INPUT -p tcp -m state --state NEW -m recent --set
xander@ubuntu:~$ sudo iptables -I INPUT -p tcp -m state --state NEW -m recent --update --seconds 1 --hitcount 1 -j DROP
xander@ubuntu:~$

```

Now, the normal scan will not show any results with max-retries.

```

nmap -p21-25 192.168.1.139 --max-retries 0

```

```

root@kali:~# nmap -p21-25 192.168.1.139 --max-retries 0

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:45 EDT
Warning: 192.168.1.139 giving up on port because retransmission cap hit (0).
Nmap scan report for 192.168.1.139
Host is up (0.00030s latency).

PORT      STATE      SERVICE
21/tcp    filtered  ftp
22/tcp    filtered  ssh
23/tcp    open      telnet
24/tcp    filtered  priv-mail
25/tcp    filtered  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

```

As we can see that the ports whose packets got dropped are not sent again so their status is not determined.

.	Time	Source	Destination	Protocol	Length	Info
162	8.820434671	192.168.1.126	192.168.1.139	TCP	58	46184 → 23 [SYN] Seq=0
163	8.820728339	192.168.1.126	192.168.1.139	TCP	58	46184 → 22 [SYN] Seq=0
164	8.820884704	192.168.1.126	192.168.1.139	TCP	58	46184 → 21 [SYN] Seq=0
165	8.820999986	192.168.1.126	192.168.1.139	TCP	58	46184 → 25 [SYN] Seq=0
166	8.820996631	192.168.1.139	192.168.1.126	TCP	60	23 → 46184 [SYN, ACK]
167	8.821086895	192.168.1.126	192.168.1.139	TCP	54	46184 → 23 [RST] Seq=1
168	8.821219665	192.168.1.126	192.168.1.139	TCP	58	46184 → 24 [SYN] Seq=0

Here we can increase the max-retries value, which will bypass the specified firewall filter so that we can get the exact port status.

```
nmap -p21-25 192.168.1.139 --max-retries 5
```

```

root@kali:~# nmap -p21-25 192.168.1.139 --max-retries 5

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:47 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00060s latency).

PORT      STATE      SERVICE
21/tcp    open      ftp
22/tcp    open      ssh
23/tcp    open      telnet
24/tcp    open      priv-mail
25/tcp    open      smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.72 seconds

```



Here we can see that TCP SYN packets sent to one port from **source:** 192.168.1.126 to **destination:** 192.168.1.139 are **sent again and again** until the packets return a specified reply or the maximum retry value (here 5) is reached.

	Time	Source	Destination	Protocol	Length	Info
288	15.040965464	192.168.1.126	192.168.1.139	TCP	58	52227 → 23 [SYN] Seq=0
289	15.041154766	192.168.1.126	192.168.1.139	TCP	58	52227 → 25 [SYN] Seq=0
290	15.041280718	192.168.1.126	192.168.1.139	TCP	58	52227 → 22 [SYN] Seq=0
291	15.041389638	192.168.1.139	192.168.1.126	TCP	60	23 → 52227 [SYN, ACK]
292	15.041422649	192.168.1.126	192.168.1.139	TCP	54	52227 → 23 [RST] Seq=1
293	15.041553830	192.168.1.126	192.168.1.139	TCP	58	52227 → 21 [SYN] Seq=0
294	15.041673430	192.168.1.126	192.168.1.139	TCP	58	52227 → 24 [SYN] Seq=0
315	16.143226373	192.168.1.126	192.168.1.139	TCP	58	52228 → 24 [SYN] Seq=0
316	16.143406963	192.168.1.126	192.168.1.139	TCP	58	52228 → 21 [SYN] Seq=0
317	16.143501663	192.168.1.126	192.168.1.139	TCP	58	52228 → 22 [SYN] Seq=0
318	16.143630235	192.168.1.126	192.168.1.139	TCP	58	52228 → 25 [SYN] Seq=0
319	16.143747646	192.168.1.139	192.168.1.126	TCP	60	24 → 52228 [SYN, ACK]
320	16.143782287	192.168.1.126	192.168.1.139	TCP	54	52228 → 24 [RST] Seq=1
341	17.245774996	192.168.1.126	192.168.1.139	TCP	58	52229 → 25 [SYN] Seq=0
342	17.245951233	192.168.1.126	192.168.1.139	TCP	58	52229 → 22 [SYN] Seq=0
343	17.246495358	192.168.1.139	192.168.1.126	TCP	60	25 → 52229 [SYN, ACK]
344	17.246544048	192.168.1.126	192.168.1.139	TCP	54	52229 → 25 [RST] Seq=1
345	17.249780225	192.168.1.126	192.168.1.139	TCP	58	52229 → 21 [SYN] Seq=0
365	18.348029402	192.168.1.126	192.168.1.139	TCP	58	52230 → 21 [SYN] Seq=0
366	18.348204450	192.168.1.126	192.168.1.139	TCP	58	52230 → 22 [SYN] Seq=0
367	18.348806210	192.168.1.139	192.168.1.126	TCP	60	21 → 52230 [SYN, ACK]
368	18.348853260	192.168.1.126	192.168.1.139	TCP	54	52230 → 21 [RST] Seq=1
394	19.451211514	192.168.1.126	192.168.1.139	TCP	58	52231 → 22 [SYN] Seq=0
395	19.452501730	192.168.1.139	192.168.1.126	TCP	60	22 → 52231 [SYN, ACK]
396	19.452625958	192.168.1.126	192.168.1.139	TCP	54	52231 → 22 [RST] Seq=1

## Host-timeout

The **--host-timeout** is an attribute that specifies the scan to give up on a host after the specified time. The less the time specified, the greater the chances of inaccuracy in scan results.

We can specify the time in milliseconds (**ms**), seconds (**s**), or minutes (**m**).

```
nmap -p21-25 192.168.1.139 --host-timeout 10ms
```

```
root@kali:~# nmap -p21-25 192.168.1.139 --host-timeout 10ms

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:50 EDT
Note: Host seems down. If it is really up, but blocking our ping probes
Nmap done: 1 IP address (0 hosts up) scanned in 0.16 seconds
```

Now we will try to get the result by increasing the timeout value

```
nmap -p21-25 192.168.1.139 --host-timeout 100ms
```

```

root@kali:~# nmap -p21-25 192.168.1.139 --host-timeout 100ms

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:51 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00047s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.26 seconds

```

We can use **--host-timeout** in other scenarios also like when we need to check if the host system is live or not. Here we have shown how the host-timeout can affect the results of a ping scan.

```
nmap -sP 192.168.1.139 --host-timeout 10ms
```

The output from the above command had given **0 hosts is up**.

```
nmap -sP 192.168.1.139 --host-timeout 100ms
```

The output from the above command had given **1 host is up**.

```

root@kali:~# nmap -sP 192.168.1.139 --host-timeout 10ms

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:53 EDT
Note: Host seems down. If it is really up, but blocking our ping probes
Nmap done: 1 IP address (0 hosts up) scanned in 0.09 seconds
root@kali:~# nmap -sP 192.168.1.139 --host-timeout 100ms

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:53 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00039s latency).
MAC Address: 00:0C:29:EB:27:7A (VMware)
Nmap done: 1 IP address (1 host up) scanned in 13.13 seconds

```

## Hostgroup

The hostgroup attribute is specified to scan a specified number of hosts in the network at a time. You need to specify the minimum number of hosts, maximum number of hosts, or both, to be scanned at a time.

```
nmap -sP 192.168.1.1/24 --min-hostgroup 3 --max-hostgroup 3
```

From the given below image, you can observe that it has shown only 3 live hosts from inside the complete subnet mask, saving your time from scanning the entire network.

```

root@kali:~# nmap -sP 192.168.1.1/24 --min-hostgroup 3 --max-hostgroup 3

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:55 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0013s latency).
MAC Address: 60:E3:27:CB:B6:2A (Tp-link Technologies)
Nmap scan report for 192.168.1.105
Host is up (0.049s latency).
MAC Address: E0:2A:82:FC:CB:27 (Universal Global Scientific Industrial)
Nmap scan report for 192.168.1.106
Host is up (0.00035s latency).
MAC Address: 14:2D:27:E8:C1:07 (Hon Hai Precision Ind.)

```

## Scan delay

A scan delay is used to delay the packet until the specified time. It is very useful for evading time-based firewalls.

```
nmap -p21-25 192.168.1.139 --scan-delay 11s
```

```

root@kali:~# nmap -p21-25 192.168.1.139 --scan-delay 11s

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 07:57 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00076s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 79.36 seconds

```

here we can see the time difference in between the packets

packet 1: TCP SYN packet on port 25 at **07:58:01** from 192.168.1.126 to 192.168.1.139



.	Time	Source	Destination	Protocol	Length	Info
7...	41.914338078	192.168.1.126	192.168.1.139	TCP	58	44207 → 25 [SYN] Seq=0
770	41.915052969	192.168.1.139	192.168.1.126	TCP	60	25 → 44207 [SYN, ACK]
771	41.915141467	192.168.1.126	192.168.1.139	TCP	54	44207 → 25 [RST] Seq=1
974	52.922414782	192.168.1.126	192.168.1.139	TCP	58	44207 → 22 [SYN] Seq=0
975	52.923117648	192.168.1.139	192.168.1.126	TCP	60	22 → 44207 [SYN, ACK]
976	52.923201244	192.168.1.126	192.168.1.139	TCP	54	44207 → 22 [RST] Seq=1
1...	63.934235748	192.168.1.126	192.168.1.139	TCP	58	44207 → 23 [SYN] Seq=0
1...	63.934929658	192.168.1.139	192.168.1.126	TCP	60	23 → 44207 [SYN, ACK]
1...	63.935013823	192.168.1.126	192.168.1.139	TCP	54	44207 → 23 [RST] Seq=1
1...	74.945662781	192.168.1.126	192.168.1.139	TCP	58	44207 → 21 [SYN] Seq=0
1...	74.946397750	192.168.1.139	192.168.1.126	TCP	60	21 → 44207 [SYN, ACK]
1...	74.946485610	192.168.1.126	192.168.1.139	TCP	54	44207 → 21 [RST] Seq=1
1...	86.036862834	192.168.1.126	192.168.1.139	TCP	58	44207 → 24 [SYN] Seq=0
1...	86.037521225	192.168.1.139	192.168.1.126	TCP	60	24 → 44207 [SYN, ACK]
1...	86.037604101	192.168.1.126	192.168.1.139	TCP	54	44207 → 24 [RST] Seq=1

Frame 769: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

▶ Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 13, 2018 07:58:01.090749717 EDT

packet 2: TCP SYN packet on port 22 at **07:58:12** from 192.168.1.126 to 192.168.1.139

Now if you count the time difference between these packets, you get an 11-second time lap between these two packets.

.	Time	Source	Destination	Protocol	Length	Info
769	41.914338078	192.168.1.126	192.168.1.139	TCP	58	44207 → 25 [SYN] Seq=0
770	41.915052969	192.168.1.139	192.168.1.126	TCP	60	25 → 44207 [SYN, ACK]
771	41.915141467	192.168.1.126	192.168.1.139	TCP	54	44207 → 25 [RST] Seq=1
974	52.922414782	192.168.1.126	192.168.1.139	TCP	58	44207 → 22 [SYN] Seq=0
975	52.923117648	192.168.1.139	192.168.1.126	TCP	60	22 → 44207 [SYN, ACK]
976	52.923201244	192.168.1.126	192.168.1.139	TCP	54	44207 → 22 [RST] Seq=1
1...	63.934235748	192.168.1.126	192.168.1.139	TCP	58	44207 → 23 [SYN] Seq=0
1...	63.934929658	192.168.1.139	192.168.1.126	TCP	60	23 → 44207 [SYN, ACK]
1...	63.935013823	192.168.1.126	192.168.1.139	TCP	54	44207 → 23 [RST] Seq=1
1...	74.945662781	192.168.1.126	192.168.1.139	TCP	58	44207 → 21 [SYN] Seq=0
1...	74.946397750	192.168.1.139	192.168.1.126	TCP	60	21 → 44207 [SYN, ACK]
1...	74.946485610	192.168.1.126	192.168.1.139	TCP	54	44207 → 21 [RST] Seq=1
1...	86.036862834	192.168.1.126	192.168.1.139	TCP	58	44207 → 24 [SYN] Seq=0
1...	86.037521225	192.168.1.139	192.168.1.126	TCP	60	24 → 44207 [SYN, ACK]
1...	86.037604101	192.168.1.126	192.168.1.139	TCP	54	44207 → 24 [RST] Seq=1

Frame 974: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

▶ Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 13, 2018 07:58:12.098826421 EDT

## Maximum rate (max-rate)

Rate is an attribute that specifies at what rate the packets are to be sent, in other words, the number of packets to be sent at a time. Max-rate specifies the maximum number of packets to be sent at once.

```
nmap -p21-25 192.168.1.139 --max-rate 2
```

```

root@kali:~# nmap -p21-25 192.168.1.139 --max-rate 2

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 03:17 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00045s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.27 seconds

```

wireshark shows that the packets sending rate are less than 2, means the number of packets sent at a time is less than or equal to 2

packet 1: TCP SYN packet on port 21 at **03:17:20** from 192.168.1.126 to 192.168.1.139

No.	Time	Source	Destination	Protocol	Length	Info
14	13.085464118	192.168.1.126	192.168.1.139	TCP	58	41591 → 21 [SYN] Seq=0
15	13.086123851	192.168.1.139	192.168.1.126	TCP	60	21 → 41591 [SYN, ACK]
16	13.086272575	192.168.1.126	192.168.1.139	TCP	54	41591 → 21 [RST] Seq=1
17	13.553070699	192.168.1.126	192.168.1.139	TCP	58	41591 → 23 [SYN] Seq=0
18	13.553315324	192.168.1.139	192.168.1.126	TCP	60	23 → 41591 [SYN, ACK]
19	13.553336412	192.168.1.126	192.168.1.139	TCP	54	41591 → 23 [RST] Seq=1
20	14.052887939	192.168.1.126	192.168.1.139	TCP	58	41591 → 25 [SYN] Seq=0
21	14.053571128	192.168.1.139	192.168.1.126	TCP	60	25 → 41591 [SYN, ACK]
22	14.053619708	192.168.1.126	192.168.1.139	TCP	54	41591 → 25 [RST] Seq=1
24	14.552443786	192.168.1.126	192.168.1.139	TCP	58	41591 → 22 [SYN] Seq=0
25	14.552743062	192.168.1.139	192.168.1.126	TCP	60	22 → 41591 [SYN, ACK]
26	14.552774165	192.168.1.126	192.168.1.139	TCP	54	41591 → 22 [RST] Seq=1
27	15.052648773	192.168.1.126	192.168.1.139	TCP	58	41591 → 24 [SYN] Seq=0
28	15.053377802	192.168.1.139	192.168.1.126	TCP	60	24 → 41591 [SYN, ACK]
29	15.053466696	192.168.1.126	192.168.1.139	TCP	54	41591 → 24 [RST] Seq=1

Frame 14: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface  
 ▶ Interface id: 0 (eth0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 15, 2018 03:17:20.807234072 EDT

packet 2: TCP SYN packet on port 23 at **03:17:21** from 192.168.1.126 to 192.168.1.139

Now if you count the time difference between these packets, you get a 1 sec time-lapse between these two packets, indicating that these two packets were not sent together.

No.	Time	Source	Destination	Protocol	Length	Info
14	13.085464118	192.168.1.126	192.168.1.139	TCP	58	41591 → 21 [SYN] Seq=0
15	13.086123851	192.168.1.139	192.168.1.126	TCP	60	21 → 41591 [SYN, ACK]
16	13.086272575	192.168.1.126	192.168.1.139	TCP	54	41591 → 21 [RST] Seq=1
17	13.553070699	192.168.1.126	192.168.1.139	TCP	58	41591 → 23 [SYN] Seq=0
18	13.553315324	192.168.1.139	192.168.1.126	TCP	60	23 → 41591 [SYN, ACK]
19	13.553336412	192.168.1.126	192.168.1.139	TCP	54	41591 → 23 [RST] Seq=1
20	14.052887939	192.168.1.126	192.168.1.139	TCP	58	41591 → 25 [SYN] Seq=0
21	14.053571128	192.168.1.139	192.168.1.126	TCP	60	25 → 41591 [SYN, ACK]
22	14.053619708	192.168.1.126	192.168.1.139	TCP	54	41591 → 25 [RST] Seq=1
24	14.552443786	192.168.1.126	192.168.1.139	TCP	58	41591 → 22 [SYN] Seq=0
25	14.552743062	192.168.1.139	192.168.1.126	TCP	60	22 → 41591 [SYN, ACK]
26	14.552774165	192.168.1.126	192.168.1.139	TCP	54	41591 → 22 [RST] Seq=1
27	15.052648773	192.168.1.126	192.168.1.139	TCP	58	41591 → 24 [SYN] Seq=0
28	15.053377802	192.168.1.139	192.168.1.126	TCP	60	24 → 41591 [SYN, ACK]
29	15.053466696	192.168.1.126	192.168.1.139	TCP	54	41591 → 24 [RST] Seq=1

Frame 17: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface  
 ▶ Interface id: 0 (eth0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 15, 2018 03:17:21.274840653 EDT

## Minimum rate (min-rate)

The Min-rate specifies the maximum number of packets to be sent at once. Here, if we want at least 2 packets to be sent on the target's network at the same time, not less than that, then we need to execute the below command.

```
nmap -p21-25 192.168.1.139 --min-rate 2
```

```
root@kali:~# nmap -p21-25 192.168.1.139 --min-rate 2

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-15 03:28 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00043s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

wireshark shows that the packets sending rate are greater than 2, means the number of packets sent at a time is equal to or greater than 2

packet 1: TCP SYN packet on port 23 at **03:28:29** from 192.168.1.126 to 192.168.1.139

No.	Time	Source	Destination	Protocol	Length	Info
3	6.532761461	192.168.1.126	192.168.1.139	TCP	58	44030 → 23 [SYN] Seq=6
4	6.532852864	192.168.1.126	192.168.1.139	TCP	58	44030 → 22 [SYN] Seq=6
5	6.532908990	192.168.1.126	192.168.1.139	TCP	58	44030 → 25 [SYN] Seq=6
6	6.532957584	192.168.1.126	192.168.1.139	TCP	58	44030 → 21 [SYN] Seq=6
7	6.533002953	192.168.1.139	192.168.1.126	TCP	60	23 → 44030 [SYN, ACK]
8	6.533059929	192.168.1.126	192.168.1.139	TCP	54	44030 → 23 [RST] Seq=1
9	6.533117305	192.168.1.126	192.168.1.139	TCP	58	44030 → 24 [SYN] Seq=6
10	6.533157737	192.168.1.139	192.168.1.126	TCP	60	22 → 44030 [SYN, ACK]
11	6.533168061	192.168.1.126	192.168.1.139	TCP	54	44030 → 22 [RST] Seq=1
12	6.533201354	192.168.1.139	192.168.1.126	TCP	60	25 → 44030 [SYN, ACK]
13	6.533210305	192.168.1.126	192.168.1.139	TCP	54	44030 → 25 [RST] Seq=1
14	6.533234642	192.168.1.139	192.168.1.126	TCP	60	21 → 44030 [SYN, ACK]
15	6.533242424	192.168.1.126	192.168.1.139	TCP	54	44030 → 21 [RST] Seq=1
16	6.533284891	192.168.1.139	192.168.1.126	TCP	60	24 → 44030 [SYN, ACK]
17	6.533294004	192.168.1.126	192.168.1.139	TCP	54	44030 → 24 [RST] Seq=1

Frame 3: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0  
 ▶ Interface id: 0 (eth0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 15, 2018 03:28:29.603693453 EDT

packet 2: TCP SYN packet on port 22 at **03:28:29** from 192.168.1.126 to 192.168.1.139

Now if you will count the time difference between these packets you get only a fraction of second as time laps between these two packets indicating that these two packets were sent together.

No.	Time	Source	Destination	Protocol	Length	Info
3	6.532761461	192.168.1.126	192.168.1.139	TCP	58	44030 → 23 [SYN] Seq=6
4	6.532852864	192.168.1.126	192.168.1.139	TCP	58	44030 → 22 [SYN] Seq=6
5	6.532908990	192.168.1.126	192.168.1.139	TCP	58	44030 → 25 [SYN] Seq=6
6	6.532957584	192.168.1.126	192.168.1.139	TCP	58	44030 → 21 [SYN] Seq=6
7	6.533002953	192.168.1.139	192.168.1.126	TCP	60	23 → 44030 [SYN, ACK]
8	6.533059929	192.168.1.126	192.168.1.139	TCP	54	44030 → 23 [RST] Seq=1
9	6.533117305	192.168.1.126	192.168.1.139	TCP	58	44030 → 24 [SYN] Seq=6
10	6.533157737	192.168.1.139	192.168.1.126	TCP	60	22 → 44030 [SYN, ACK]
11	6.533168061	192.168.1.126	192.168.1.139	TCP	54	44030 → 22 [RST] Seq=1
12	6.533201354	192.168.1.139	192.168.1.126	TCP	60	25 → 44030 [SYN, ACK]
13	6.533210305	192.168.1.126	192.168.1.139	TCP	54	44030 → 25 [RST] Seq=1
14	6.533234642	192.168.1.139	192.168.1.126	TCP	60	21 → 44030 [SYN, ACK]
15	6.533242424	192.168.1.126	192.168.1.139	TCP	54	44030 → 21 [RST] Seq=1
16	6.533284891	192.168.1.139	192.168.1.126	TCP	60	24 → 44030 [SYN, ACK]
17	6.533294004	192.168.1.126	192.168.1.139	TCP	54	44030 → 24 [RST] Seq=1

Frame 4: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0  
 ▶ Interface id: 0 (eth0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 15, 2018 03:28:29.603784856 EDT

## Parallelism

The parallelism attribute is used to send multiple packets in parallel, min-parallelism means that the number of packets to be sent in parallel is to be greater than the value specified, and max-parallelism means that the number of packets to be sent in parallel is to be less than or equal to the value specified.



```
nmap -p21-25 192.168.1.139 --min-parallelism 2 --max-parallelism 2
```

```
root@kali:~# nmap -p21-25 192.168.1.139 --min-parallelism 2 --max-parallelism 2

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 08:08 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00044s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
```

In Wireshark we can see a couple of TCP-SYN packets sent in parallel from 192.168.1.126, which is neither less nor greater than 2.

.	Time	Source	Destination	Protocol	Length	Info
2...	15.113820456	192.168.1.126	192.168.1.139	TCP	58	33157 → 25 [SYN] Seq=
298	15.114028125	192.168.1.126	192.168.1.139	TCP	58	33157 → 21 [SYN] Seq=
299	15.114511298	192.168.1.139	192.168.1.126	TCP	60	25 → 33157 [SYN, ACK]
300	15.114602850	192.168.1.126	192.168.1.139	TCP	54	33157 → 25 [RST] Seq=
301	15.114686525	192.168.1.139	192.168.1.126	TCP	60	21 → 33157 [SYN, ACK]
302	15.114711125	192.168.1.126	192.168.1.139	TCP	54	33157 → 21 [RST] Seq=
303	15.114815205	192.168.1.126	192.168.1.139	TCP	58	33157 → 23 [SYN] Seq=
304	15.115161257	192.168.1.126	192.168.1.139	TCP	58	33157 → 22 [SYN] Seq=
305	15.115338186	192.168.1.139	192.168.1.126	TCP	60	23 → 33157 [SYN, ACK]
306	15.115430772	192.168.1.126	192.168.1.139	TCP	54	33157 → 23 [RST] Seq=
307	15.115621623	192.168.1.139	192.168.1.126	TCP	60	22 → 33157 [SYN, ACK]
308	15.115697971	192.168.1.126	192.168.1.139	TCP	54	33157 → 22 [RST] Seq=
309	15.115871751	192.168.1.126	192.168.1.139	TCP	58	33157 → 24 [SYN] Seq=
310	15.116269932	192.168.1.139	192.168.1.126	TCP	60	24 → 33157 [SYN, ACK]
311	15.116341992	192.168.1.126	192.168.1.139	TCP	54	33157 → 24 [RST] Seq=

## Round trip timeout

Rtt timeout is the time specified for a packet to return a reply, min-rtt-timeout specifies the minimum value of time that is to be taken by a packet to return a reply

```
nmap -p21-25 192.168.1.139 --min-rtt-timeout 5ms
```



```

root@kali:~# nmap -p21-25 192.168.1.139 --min-rtt-timeout 5ms

Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 08:10 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00067s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.32 seconds

```

Wireshark shows that the packet and its reply take more time than the min-rtt-timeout specified.

No.	Time	Source	Destination	Protocol	Length	Info
297	15.334263701	192.168.1.126	192.168.1.139	TCP	58	43793 → 25 [SYN] Seq=0
298	15.334430671	192.168.1.126	192.168.1.139	TCP	58	43793 → 22 [SYN] Seq=0
299	15.334544549	192.168.1.126	192.168.1.139	TCP	58	43793 → 21 [SYN] Seq=0
300	15.334681142	192.168.1.126	192.168.1.139	TCP	58	43793 → 23 [SYN] Seq=0
301	15.334814747	192.168.1.126	192.168.1.139	TCP	58	43793 → 24 [SYN] Seq=0
302	15.335064264	192.168.1.139	192.168.1.126	TCP	60	25 → 43793 [SYN, ACK]
303	15.335312326	192.168.1.126	192.168.1.139	TCP	54	43793 → 25 [RST] Seq=1
304	15.335413729	192.168.1.139	192.168.1.126	TCP	60	22 → 43793 [SYN, ACK]
305	15.335502972	192.168.1.126	192.168.1.139	TCP	54	43793 → 22 [RST] Seq=1
306	15.335585908	192.168.1.139	192.168.1.126	TCP	60	21 → 43793 [SYN, ACK]
307	15.335612417	192.168.1.126	192.168.1.139	TCP	54	43793 → 21 [RST] Seq=1
308	15.335742238	192.168.1.139	192.168.1.126	TCP	60	23 → 43793 [SYN, ACK]
309	15.335787189	192.168.1.126	192.168.1.139	TCP	54	43793 → 23 [RST] Seq=1
310	15.335863782	192.168.1.139	192.168.1.126	TCP	60	24 → 43793 [SYN, ACK]
311	15.335900747	192.168.1.126	192.168.1.139	TCP	54	43793 → 24 [RST] Seq=1

  

Frame 297: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Mar 13, 2018 08:10:53.232666116 EDT

packet 1: TCP SYN packet on port 25 at **08:10:53.232666116** from 192.168.1.126 to 192.168.1.139

packet 2: SYN-ACK packet from port 25 at **08:10:53.233466679** from 192.168.1.139 to 192.168.1.126

No.	Time	Source	Destination	Protocol	Length	Info
297	15.334263701	192.168.1.126	192.168.1.139	TCP	58	43793 → 25 [SYN] Seq=0
298	15.334430671	192.168.1.126	192.168.1.139	TCP	58	43793 → 22 [SYN] Seq=0
299	15.334544549	192.168.1.126	192.168.1.139	TCP	58	43793 → 21 [SYN] Seq=0
300	15.334681142	192.168.1.126	192.168.1.139	TCP	58	43793 → 23 [SYN] Seq=0
301	15.334814747	192.168.1.126	192.168.1.139	TCP	58	43793 → 24 [SYN] Seq=0
302	15.335064264	192.168.1.139	192.168.1.126	TCP	60	25 → 43793 [SYN, ACK]
303	15.335312326	192.168.1.126	192.168.1.139	TCP	54	43793 → 25 [RST] Seq=1
304	15.335413729	192.168.1.139	192.168.1.126	TCP	60	22 → 43793 [SYN, ACK]
305	15.335502972	192.168.1.126	192.168.1.139	TCP	54	43793 → 22 [RST] Seq=1
306	15.335585908	192.168.1.139	192.168.1.126	TCP	60	21 → 43793 [SYN, ACK]
307	15.335612417	192.168.1.126	192.168.1.139	TCP	54	43793 → 21 [RST] Seq=1
308	15.335742238	192.168.1.139	192.168.1.126	TCP	60	23 → 43793 [SYN, ACK]
309	15.335787189	192.168.1.126	192.168.1.139	TCP	54	43793 → 23 [RST] Seq=1
310	15.335863782	192.168.1.139	192.168.1.126	TCP	60	24 → 43793 [SYN, ACK]
311	15.335900747	192.168.1.126	192.168.1.139	TCP	54	43793 → 24 [RST] Seq=1

Frame 302: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface  
 ▶ Interface id: 0 (eth0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 13, 2018 08:10:53.233466679 EDT

## Max-rtt-timeout

A max-rtt-timeout specifies the maximum value of time that is to be taken by a packet to return a reply.

```
nmap -p21-25 192.168.1.139 --max-rtt-timeout 50ms
```

```
root@kali:~# nmap -p21-25 192.168.1.139 --max-rtt-timeout 50ms
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 08:14 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00090s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds
```

Wireshark shows that the packet and its reply take less time lesser than the max-rtt-timeout

packet 1: TCP SYN packet on port 22 at **08:15:08.171777907** from 192.168.1.126 to 192.168.1.139

No.	Time	Source	Destination	Protocol	Length	Info
190	9.434266336	192.168.1.126	192.168.1.139	TCP	58	44186 → 22 [SYN] Seq=0
191	9.434902657	192.168.1.126	192.168.1.139	TCP	58	44186 → 23 [SYN] Seq=0
192	9.435162129	192.168.1.126	192.168.1.139	TCP	58	44186 → 25 [SYN] Seq=0
193	9.435341314	192.168.1.126	192.168.1.139	TCP	58	44186 → 21 [SYN] Seq=0
194	9.435487419	192.168.1.126	192.168.1.139	TCP	58	44186 → 24 [SYN] Seq=0
195	9.435605583	192.168.1.139	192.168.1.126	TCP	60	22 → 44186 [SYN, ACK]
196	9.435732271	192.168.1.126	192.168.1.139	TCP	54	44186 → 22 [RST] Seq=1
197	9.435939167	192.168.1.139	192.168.1.126	TCP	60	23 → 44186 [SYN, ACK]
198	9.436031389	192.168.1.126	192.168.1.139	TCP	54	44186 → 23 [RST] Seq=1
199	9.436212979	192.168.1.139	192.168.1.126	TCP	60	25 → 44186 [SYN, ACK]
200	9.436290631	192.168.1.126	192.168.1.139	TCP	54	44186 → 25 [RST] Seq=1
201	9.436373547	192.168.1.139	192.168.1.126	TCP	60	21 → 44186 [SYN, ACK]
202	9.436410247	192.168.1.126	192.168.1.139	TCP	54	44186 → 21 [RST] Seq=1
203	9.436489429	192.168.1.139	192.168.1.126	TCP	60	24 → 44186 [SYN, ACK]
204	9.436562788	192.168.1.126	192.168.1.139	TCP	54	44186 → 24 [RST] Seq=1

Frame 189: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0  
 ▶ Interface id: 0 (eth0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 13, 2018 08:15:08.171777907 EDT

packet 2: SYN-ACK packet from port 22 at **08:15:08.173117154** from 192.168.1.139 to 192.168.1.126

No.	Time	Source	Destination	Protocol	Length	Info
189	9.434266336	192.168.1.126	192.168.1.139	TCP	58	44186 → 22 [SYN] Seq=0
190	9.434902657	192.168.1.126	192.168.1.139	TCP	58	44186 → 23 [SYN] Seq=0
191	9.435162129	192.168.1.126	192.168.1.139	TCP	58	44186 → 25 [SYN] Seq=0
192	9.435341314	192.168.1.126	192.168.1.139	TCP	58	44186 → 21 [SYN] Seq=0
193	9.435487419	192.168.1.126	192.168.1.139	TCP	58	44186 → 24 [SYN] Seq=0
194	9.435605583	192.168.1.139	192.168.1.126	TCP	60	22 → 44186 [SYN, ACK] Seq=0
195	9.435732271	192.168.1.126	192.168.1.139	TCP	54	44186 → 22 [RST] Seq=1
196	9.435939167	192.168.1.139	192.168.1.126	TCP	60	23 → 44186 [SYN, ACK] Seq=0
197	9.436031389	192.168.1.126	192.168.1.139	TCP	54	44186 → 23 [RST] Seq=1
198	9.436212979	192.168.1.139	192.168.1.126	TCP	60	25 → 44186 [SYN, ACK] Seq=0
199	9.436290631	192.168.1.126	192.168.1.139	TCP	54	44186 → 25 [RST] Seq=1
200	9.436373547	192.168.1.139	192.168.1.126	TCP	60	21 → 44186 [SYN, ACK] Seq=0
201	9.436410247	192.168.1.126	192.168.1.139	TCP	54	44186 → 21 [RST] Seq=1
202	9.436489429	192.168.1.139	192.168.1.126	TCP	60	24 → 44186 [SYN, ACK] Seq=0
203	9.436562788	192.168.1.126	192.168.1.139	TCP	54	44186 → 24 [RST] Seq=1

Frame 194: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0  
 ▶ Interface id: 0 (eth0)  
 Encapsulation type: Ethernet (1)  
 Arrival Time: Mar 13, 2018 08:15:08.173117154 EDT

## Initial Round trip timeout

Initial-rtt-timeout specifies the initial value of time to be taken by a packet to return a reply. The return time can be greater or less than the initial-rtt-timeout because of the max-rtt-timeout and min-rtt-timeout specifications, but the packet attempts to return a reply at the time specified in initial-rtt-timeout.

```
nmap -p21-25 192.168.1.139 --initial-rtt-timeout 50ms
```

```

root@kali:~# nmap -p21-25 192.168.1.139 --initial-rtt-timeout 50ms
Starting Nmap 7.60 ( https://nmap.org ) at 2018-03-13 08:18 EDT
Nmap scan report for 192.168.1.139
Host is up (0.00042s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
24/tcp    open  priv-mail
25/tcp    open  smtp
MAC Address: 00:0C:29:EB:27:7A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.28 seconds

```

Wireshark shows that the time taken by the packet to return reply is around the same time as specified in initial-rtt-timeout

packet 1: TCP SYN packet on port 23 at **08:18:45.342395520** from 192.168.1.126 to 192.168.1.139

	Time	Source	Destination	Protocol	Length	Info
3...	17.721306146	192.168.1.126	192.168.1.139	TCP	58	39233 → 23 [SYN] Seq=0
335	17.721476100	192.168.1.126	192.168.1.139	TCP	58	39233 → 21 [SYN] Seq=0
336	17.721612159	192.168.1.126	192.168.1.139	TCP	58	39233 → 22 [SYN] Seq=0
337	17.721734558	192.168.1.126	192.168.1.139	TCP	58	39233 → 25 [SYN] Seq=0
338	17.721841588	192.168.1.139	192.168.1.126	TCP	60	23 → 39233 [SYN, ACK]
339	17.721874995	192.168.1.126	192.168.1.139	TCP	54	39233 → 23 [RST] Seq=1
340	17.721948469	192.168.1.139	192.168.1.126	TCP	60	21 → 39233 [SYN, ACK]
341	17.721966162	192.168.1.126	192.168.1.139	TCP	54	39233 → 21 [RST] Seq=1
342	17.722037302	192.168.1.139	192.168.1.126	TCP	60	22 → 39233 [SYN, ACK]
343	17.722210665	192.168.1.126	192.168.1.139	TCP	54	39233 → 22 [RST] Seq=1
344	17.722293506	192.168.1.139	192.168.1.126	TCP	60	25 → 39233 [SYN, ACK]
345	17.722315347	192.168.1.126	192.168.1.139	TCP	54	39233 → 25 [RST] Seq=1
346	17.722458122	192.168.1.126	192.168.1.139	TCP	58	39233 → 24 [SYN] Seq=0
347	17.722964866	192.168.1.139	192.168.1.126	TCP	60	24 → 39233 [SYN, ACK]
348	17.723008782	192.168.1.126	192.168.1.139	TCP	54	39233 → 24 [RST] Seq=1

```

Frame 334: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface
  Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Mar 13, 2018 08:18:45.342395520 EDT

```

packet 2: SYN-ACK packet from port 23 at **08:18:45.342930962** from 192.168.1.139 to 192.168.1.126

	Time	Source	Destination	Protocol	Length	Info
334	17.721306146	192.168.1.126	192.168.1.139	TCP	58	39233 → 23 [SYN] Seq=0
335	17.721476100	192.168.1.126	192.168.1.139	TCP	58	39233 → 21 [SYN] Seq=0
336	17.721612159	192.168.1.126	192.168.1.139	TCP	58	39233 → 22 [SYN] Seq=0
337	17.721734558	192.168.1.126	192.168.1.139	TCP	58	39233 → 25 [SYN] Seq=0
338	17.721841588	192.168.1.139	192.168.1.126	TCP	60	23 → 39233 [SYN, ACK] Seq=0
339	17.721874995	192.168.1.126	192.168.1.139	TCP	54	39233 → 23 [RST] Seq=1
340	17.721948469	192.168.1.139	192.168.1.126	TCP	60	21 → 39233 [SYN, ACK] Seq=0
341	17.721966162	192.168.1.126	192.168.1.139	TCP	54	39233 → 21 [RST] Seq=1
342	17.722037302	192.168.1.139	192.168.1.126	TCP	60	22 → 39233 [SYN, ACK] Seq=0
343	17.722210665	192.168.1.126	192.168.1.139	TCP	54	39233 → 22 [RST] Seq=1
344	17.722293506	192.168.1.139	192.168.1.126	TCP	60	25 → 39233 [SYN, ACK] Seq=0
345	17.722315347	192.168.1.126	192.168.1.139	TCP	54	39233 → 25 [RST] Seq=1
346	17.722458122	192.168.1.126	192.168.1.139	TCP	58	39233 → 24 [SYN] Seq=0
347	17.722964866	192.168.1.139	192.168.1.126	TCP	60	24 → 39233 [SYN, ACK] Seq=0
348	17.723008782	192.168.1.126	192.168.1.139	TCP	54	39233 → 24 [RST] Seq=1

Frame 338: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

► Interface id: 0 (eth0)

Encapsulation type: Ethernet (1)

Arrival Time: Mar 13, 2018 08:18:45.342930962 EDT



# JOIN OUR TRAINING PROGRAMS

