Nmap for Pentester: Timing Scan

February 26, 2018 By Raj Chandel

In this article we are going to scan the target machine with normal Nmap scan along with the Timing template and the time between packets can be confirmed by analysis of Nmap traffic through Wireshark.

Timing template in the nmap is defined by –T<0-5> having -T0 as the slowest and –T5 as the fastest. By default, all nmap scans run on –T3 timing template. Timing template in Nmap is used to optimize and improve the quality and performance of the scan to get desired results.

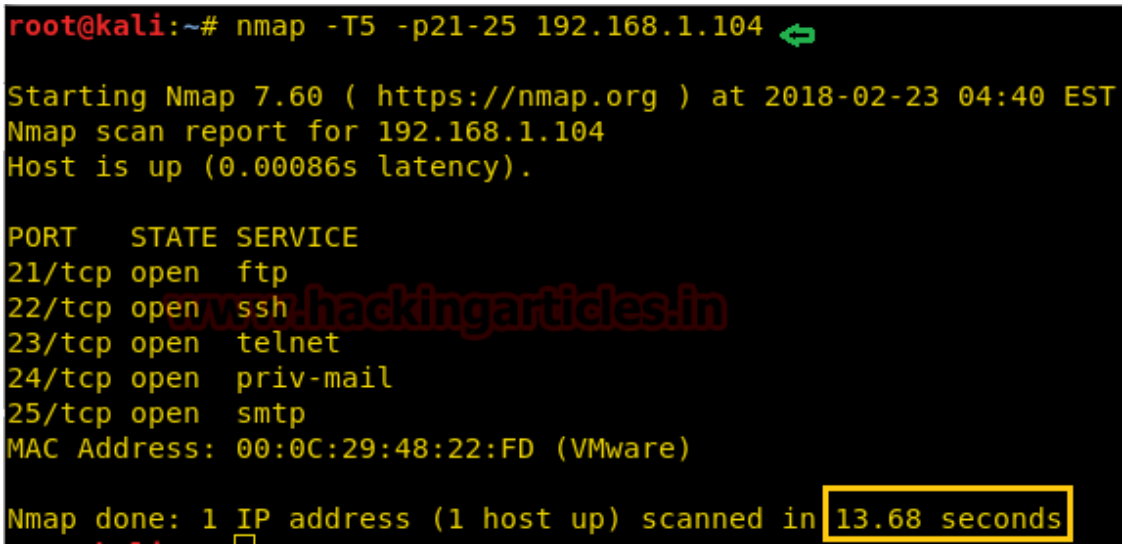
Let's start!!

Nmap Insane (-T5) Scan

This template is used for sending packets insanely fast and **waits only 0.3 seconds** for the response. The time difference between the two packets sent is up to 5 milliseconds. This timing template makes the scan superfast but the accuracy is sacrificed sometimes. Nmap gives-up on a host if it couldn't complete the scan within 15 minutes. Other than that, -T5 should be used only on a fast network and high-end systems as sending packets this fast can affect the working of the network or system and can result in system failure.

For using timing template use the **attribute –T<0-5>** after Nmap while scanning a target network

```
nmap -T5 -p21-25 192.168.1.104
```



Here are the packets sent to the target IP are sent by a maximum difference of 5 milliseconds or 0.005 seconds

Packet 1 has Arrival Time of 04:41:04.557153433

.	Time	Source	Destination	Protocol	Length	Info
36	25.323572963	192.168.1.105	192.168.1.104	TCP	58	36290 → 23 [SYN]
37	25.323644834	192.168.1.105	192.168.1.104	TCP	58	36290 → 21 [SYN]
38	25.323698518	192.168.1.105	192.168.1.104	TCP	58	36290 → 25 [SYN]
39	25.323765959	192.168.1.105	192.168.1.104	TCP	58	36290 → 22 [SYN]
40	25.323835462	192.168.1.105	192.168.1.104	TCP	58	36290 → 24 [SYN]

```
Frame 36: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inte
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 04:41:04.557153433 EST
```

Packet 2 has Arrival Time of 04:41:04.557225304

The difference between the arrival time of Packet 1 and Packet 2 is about **0.07 milliseconds**.

.	Time	Source	Destination	Protocol	Length	Info
36	25.323572963	192.168.1.105	192.168.1.104	TCP	58	36290 → 23 [SYN]
37	25.323644834	192.168.1.105	192.168.1.104	TCP	58	36290 → 21 [SYN]
38	25.323698518	192.168.1.105	192.168.1.104	TCP	58	36290 → 25 [SYN]
39	25.323765959	192.168.1.105	192.168.1.104	TCP	58	36290 → 22 [SYN]
40	25.323835462	192.168.1.105	192.168.1.104	TCP	58	36290 → 24 [SYN]

```
Frame 37: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inte
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 04:41:04.557225304 EST
```

Nmap Aggressive (-T4) Scan

This template is used for sending packets very fast and **waits only 1.25 seconds** for the response. The time difference between the two packets sent is up to 10 milliseconds. Nmap official documentation recommends using –T4 for "reasonably modern and reliable networks".

```
nmap -T4 –p21-25 192.168.1.104
```

```
root@kali:~# nmap -T4 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 05:58 EST
Nmap scan report for 192.168.1.104
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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds
```

Here are the packets sent to the target IP are sent by a maximum difference of 5 milliseconds or 0.005 seconds

Packet 1 has Arrival Time of 05:58:34.636899267

.	Time	Source	Destination	Protocol	Length	Info
53	16.913359323	192.168.1.105	192.168.1.104	TCP	58	43423 → 21 [SYN]
54	16.913582952	192.168.1.105	192.168.1.104	TCP	58	43423 → 25 [SYN]
55	16.913732633	192.168.1.105	192.168.1.104	TCP	58	43423 → 22 [SYN]
56	16.913871832	192.168.1.105	192.168.1.104	TCP	58	43423 → 23 [SYN]
57	16.914010842	192.168.1.105	192.168.1.104	TCP	58	43423 → 24 [SYN]

```
Frame 53: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inte
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 05:58:34.636899267 EST
```

Packet 2 has Arrival Time of 05:58:34.637122896

The difference between the arrival time of Packet 1 and Packet 2 is about **0.2 milliseconds**.

.	Time	Source	Destination	Protocol	Length	Info
53	16.913359323	192.168.1.105	192.168.1.104	TCP	58	43423 → 21 [SYN]
54	16.913582952	192.168.1.105	192.168.1.104	TCP	58	43423 → 25 [SYN]
55	16.913732633	192.168.1.105	192.168.1.104	TCP	58	43423 → 22 [SYN]
56	16.913871832	192.168.1.105	192.168.1.104	TCP	58	43423 → 23 [SYN]
57	16.914010842	192.168.1.105	192.168.1.104	TCP	58	43423 → 24 [SYN]

```
Frame 54: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inte
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 05:58:34.637122896 EST
```

Nmap Normal (-T3) Scan

This is the default nmap timing template which is used when -T argument is not specified.

```
nmap -T3 -p21-25 192.168.1.104
```

```
root@kali:~# nmap -T3 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 06:00 EST
Nmap scan report for 192.168.1.104
Host is up (0.00074s 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:29:48:22:FD (VMware)

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

Packet 1 has Arrival Time of 06:01:12.574866212

	Time	Source	Destination	Protocol	Length	Info
29	22.296345921	192.168.1.105	192.168.1.104	TCP	58	35908 → 21 [SYN]
30	22.296538742	192.168.1.105	192.168.1.104	TCP	58	35908 → 23 [SYN]
31	22.296667002	192.168.1.105	192.168.1.104	TCP	58	35908 → 22 [SYN]
32	22.296837162	192.168.1.105	192.168.1.104	TCP	58	35908 → 25 [SYN]
33	22.296946335	192.168.1.105	192.168.1.104	TCP	58	35908 → 24 [SYN]

```
Frame 29: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inte
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:01:12.574866212 EST
```

Packet 1 has Arrival Time of 06:01:12.575059033

The difference between the arrival time of Packet 1 and Packet 2 is about **0.1 milliseconds**.

	Time	Source	Destination	Protocol	Length	Info
29	22.296345921	192.168.1.105	192.168.1.104	TCP	58	35908 → 21 [SYN]
30	22.296538742	192.168.1.105	192.168.1.104	TCP	58	35908 → 23 [SYN]
31	22.296667002	192.168.1.105	192.168.1.104	TCP	58	35908 → 22 [SYN]
32	22.296837162	192.168.1.105	192.168.1.104	TCP	58	35908 → 25 [SYN]
33	22.296946335	192.168.1.105	192.168.1.104	TCP	58	35908 → 24 [SYN]

```
Frame 30: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inte
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:01:12.575059033 EST
```

Nmap Polite (-T2) Scan

This template is used for sending packets quickly then –T0 and –T1 but still slower than a normal scan. The time difference between the two packets sent is 0.4 seconds.

```
nmap -T2 -p21-25 192.168.1.104
```

```
root@kali:~# nmap -T2 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 06:07 EST
Nmap scan report for 192.168.1.104
Host is up (0.00071s 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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.57 seconds
```

Packet 1 has Arrival Time of 06:07:38.139876513

.	Time	Source	Destination	Protocol	Leng	Info
24	15.984265893	192.168.1.105	192.168.1.104	TCP	58	39068 → 25 [SYN]
27	16.385075833	192.168.1.105	192.168.1.104	TCP	58	39068 → 23 [SYN]
30	16.785604785	192.168.1.105	192.168.1.104	TCP	58	39068 → 22 [SYN]
33	17.186596738	192.168.1.105	192.168.1.104	TCP	58	39068 → 21 [SYN]
36	17.587308350	192.168.1.105	192.168.1.104	TCP	58	39068 → 24 [SYN]

```
Frame 24: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inte
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:07:38.139876513 EST
```

Packet 2 has Arrival Time of 06:01:38.540686453

.	Time	Source	Destination	Protocol	Leng	Info
24	15.984265893	192.168.1.105	192.168.1.104	TCP	58	39068 → 25 [SYN]
27	16.385075833	192.168.1.105	192.168.1.104	TCP	58	39068 → 23 [SYN]
30	16.785604785	192.168.1.105	192.168.1.104	TCP	58	39068 → 22 [SYN]
33	17.186596738	192.168.1.105	192.168.1.104	TCP	58	39068 → 21 [SYN]
36	17.587308350	192.168.1.105	192.168.1.104	TCP	58	39068 → 24 [SYN]

```
Frame 27: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inter
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:07:38.540686453 EST
```

Nmap Sneaky (-T1) Scan

This template is used for sending packets quickly but still slower than a normal scan. The time difference between the two packets sent is 15 seconds.

```
nmap -T1 -p21-25 192.168.1.104
```

```
root@kali:~# nmap -T1 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 06:16 EST
Nmap scan report for 192.168.1.104
Host is up (0.00075s 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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 103.24 seconds
```

Packet 1 has Arrival Time of 06:17:02.354879724

.	Time	Source	Destination	Protocol	Leng	Info
42	43.840844796	192.168.1.105	192.168.1.104	TCP	58	33641 → 23 [SYN]
59	58.857028678	192.168.1.105	192.168.1.104	TCP	58	33641 → 22 [SYN]
77	73.859991390	192.168.1.105	192.168.1.104	TCP	58	33641 → 25 [SYN]
88	88.876012345	192.168.1.105	192.168.1.104	TCP	58	33641 → 21 [SYN]
106	103.891642670	192.168.1.105	192.168.1.104	TCP	58	33641 → 24 [SYN]

```
Frame 42: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inter
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:17:02.354879724 EST
```

Packet 2 has Arrival Time of 06:17:17.371063606

The difference between the arrival time of Packet 1 and Packet 2 is about **15 seconds**.

.	Time	Source	Destination	Protocol	Leng	Info
42	43.840844796	192.168.1.105	192.168.1.104	TCP	58	33641 → 23 [SYN]
59	58.857028678	192.168.1.105	192.168.1.104	TCP	58	33641 → 22 [SYN]
77	73.859991390	192.168.1.105	192.168.1.104	TCP	58	33641 → 25 [SYN]
88	88.876012345	192.168.1.105	192.168.1.104	TCP	58	33641 → 21 [SYN]
106	103.891642670	192.168.1.105	192.168.1.104	TCP	58	33641 → 24 [SYN]

```
Frame 59: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on inter
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:17:17.371063606 EST
```

Nmap Paranoid (-T0) Scan

This template is used for sending packets very slowly as only one port is scanned at a time. The time difference between the two packets sent is 5 minutes.

```
nmap -T0 -p21-25 192.168.1.104
```

```
root@kali:~# nmap -T0 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 06:22 EST
Stats: 0:05:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 0.00% done
Nmap scan report for 192.168.1.104
Host is up (0.00097s 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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1813.56 seconds
```

Packet 1 has Arrival Time of 06:32:25.043303267

.	Time	Source	Destination	Protocol	Length	Info
651	617.455539292	192.168.1.105	192.168.1.104	TCP	58	47584 → 21 [SYN]
958	917.493040954	192.168.1.105	192.168.1.104	TCP	58	47584 → 22 [SYN]
1782	1217.5864065…	192.168.1.105	192.168.1.104	TCP	58	47584 → 23 [SYN]
2063	1517.6853343…	192.168.1.105	192.168.1.104	TCP	58	47584 → 25 [SYN]
2355	1817.6855536…	192.168.1.105	192.168.1.104	TCP	58	47584 → 24 [SYN]

```
Frame 651: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interfac
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:32:25.043303267 EST
```

Packet 2 has Arrival Time of 06:37:25.080804929

The difference between the arrival time of Packet 1 and Packet 2 is about **5 minutes**.

.	Time	Source	Destination	Protocol	Length	Info
651	617.455539292	192.168.1.105	192.168.1.104	TCP	58	47584 → 21 [SYN]
958	917.493040954	192.168.1.105	192.168.1.104	TCP	58	47584 → 22 [SYN]
1782	1217.5864065…	192.168.1.105	192.168.1.104	TCP	58	47584 → 23 [SYN]
2063	1517.6853343…	192.168.1.105	192.168.1.104	TCP	58	47584 → 25 [SYN]
2355	1817.6855536…	192.168.1.105	192.168.1.104	TCP	58	47584 → 24 [SYN]

```
Frame 958: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interfa
▸ Interface id: 0 (eth0)
  Encapsulation type: Ethernet (1)
  Arrival Time: Feb 23, 2018 06:37:25.080804929 EST
```

Evading Time-Based Firewall rules using timing templates

Block Insane T5 scan

Even though we can speed up the scan by –T5 and –T4 templates, there are chances that the target system is using some kind of firewall rules to secure itself. Here are some examples of the firewall rules and methods to bypass them.

This rule will block TCP packets from an IP address if the packet count goes more than 1. In other words, only the first packet will be responded from an IP address in 1 second.

```
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
```

```
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:~$
```


If you're scanning more than 1 port on a target system having above rule, the result will not be as desired. Like if we use -T5 or -T4 in nmap scan, the time difference between packets is very much less than 1 second so if we scan five ports at a time it will show one as open/closed and others as filtered. But -T5 has also **–max-retries set to 2 means** it will retry to get the reply from ports 2 more times hence there will be **3 out 5 ports** with accurate open/close status and the rest 2 with the filtered status

```
nmap -T5 -p21-25 192.168.1.104
```

From given below image you can observe that it has shown **3 ports** are **open** and **2 ports** are **filtered**.

```
root@kali:~# nmap -T5 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 07:01 EST
Warning: 192.168.1.104 giving up on port because retransmission cap hit (2).
Nmap scan report for 192.168.1.104
Host is up (0.00050s latency).

PORT   STATE    SERVICE
21/tcp open     ftp
22/tcp filtered ssh
23/tcp filtered telnet
24/tcp open     priv-mail
25/tcp open     smtp
MAC Address: 00:0C:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 15.42 seconds
```


The packet transfer between the target and the victim is captured through Wireshark, it clearly shows that the TCP SYN packets are sent multiple times on ports 22 and 23 and didn't receive any reply packet for those request packet.

	Time	Source	Destination	Protoc	Length	Info
66	14.878423265	192.168.1.105	192.168.1.104	TCP	58	33256 → 21 [SYN] Seq=
67	14.878628199	192.168.1.105	192.168.1.104	TCP	58	33256 → 25 [SYN] Seq=
68	14.878791354	192.168.1.105	192.168.1.104	TCP	58	33256 → 23 [SYN] Seq=
69	14.878926055	192.168.1.105	192.168.1.104	TCP	58	33256 → 22 [SYN] Seq=
71	14.879183239	192.168.1.105	192.168.1.104	TCP	54	1 33256 → 21 [RST]
72	14.879325380	192.168.1.105	192.168.1.104	TCP	58	33256 → 24 [SYN] Seq=
77	15.930759725	192.168.1.105	192.168.1.104	TCP	58	33257 → 24 [SYN] Seq=
78	15.931001497	192.168.1.105	192.168.1.104	TCP	58	33257 → 22 [SYN] Seq=
79	15.931141604	192.168.1.105	192.168.1.104	TCP	58	33257 → 23 [SYN] Seq=
81	15.931442150	192.168.1.105	192.168.1.104	TCP	54	2 33257 → 24 [RST]
82	15.931573165	192.168.1.105	192.168.1.104	TCP	58	33257 → 25 [SYN] Seq=
86	16.983167084	192.168.1.105	192.168.1.104	TCP	58	33258 → 25 [SYN] Seq=
87	16.983390197	192.168.1.105	192.168.1.104	TCP	58	33258 → 23 [SYN] Seq=
88	16.983524227	192.168.1.105	192.168.1.104	TCP	58	33258 → 22 [SYN] Seq=
90	16.984010160	192.168.1.105	192.168.1.104	TCP	54	3 33258 → 25 [RST]

Bypass Insane T5 Firewall filter

1st method

Use **–max-retries** argument to increase the –max-retries value so that each retry gives the accurate status of one port at a time. Execute given below command for increasing maximum retries with T5 scan here I had 4 you can modify it as per your requirement.

```
nmap -T5 -p21-25 192.168.1.104 --max-retries 4
```

now if you notice from given below image you can observe that it has shown all **5 ports** are **open**.

```
root@kali:~# nmap -T5 -p21-25 192.168.1.104 --max-retries 4

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 07:05 EST
Nmap scan report for 192.168.1.104
Host is up (0.00062s 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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.43 seconds
```

Here, the packet transfer shows that in each retry one different port sends the reply in order to confirm its status as shown in the given below image.

	Time	Source	Destination	Protocol	Length	Info
75	31.984483659	192.168.1.105	192.168.1.104	TCP	58	43646 → 23 [SYN] Seq=
76	31.984659685	192.168.1.105	192.168.1.104	TCP	58	43646 → 21 [SYN] Seq=
77	31.984934060	192.168.1.105	192.168.1.104	TCP	58	43646 → 22 [SYN] Seq=
78	31.985043904	192.168.1.105	192.168.1.104	TCP	58	43646 → 25 [SYN] Seq=
79	31.985205109	192.168.1.105	192.168.1.104	TCP	58	43646 → 24 [SYN] Seq=
81	31.985533418	192.168.1.105	192.168.1.104	TCP	54	1 43646 → 23 [RST]
98	33.036429708	192.168.1.105	192.168.1.104	TCP	58	43647 → 24 [SYN] Seq=
99	33.036619781	192.168.1.105	192.168.1.104	TCP	58	43647 → 25 [SYN] Seq=
100	33.036727207	192.168.1.105	192.168.1.104	TCP	58	43647 → 22 [SYN] Seq=
101	33.036875561	192.168.1.105	192.168.1.104	TCP	58	43647 → 21 [SYN] Seq=
103	33.037243490	192.168.1.105	192.168.1.104	TCP	54	2 43647 → 24 [RST]
107	34.089191660	192.168.1.105	192.168.1.104	TCP	58	43648 → 21 [SYN] Seq=
108	34.089341524	192.168.1.105	192.168.1.104	TCP	58	43648 → 22 [SYN] Seq=
109	34.089408273	192.168.1.105	192.168.1.104	TCP	58	43648 → 25 [SYN] Seq=
111	34.089706235	192.168.1.105	192.168.1.104	TCP	54	3 43648 → 21 [RST]
112	35.142129599	192.168.1.105	192.168.1.104	TCP	58	43649 → 25 [SYN] Seq=
113	35.142936295	192.168.1.105	192.168.1.104	TCP	58	43649 → 22 [SYN] Seq=
115	35.143397140	192.168.1.105	192.168.1.104	TCP	54	4 43649 → 25 [RST]
117	36.195907583	192.168.1.105	192.168.1.104	TCP	58	43650 → 22 [SYN] Seq=
119	36.196796448	192.168.1.105	192.168.1.104	TCP	54	5 43650 → 22 [RST]

2nd Method

The second method is to use a timing template which has a greater time difference between the packets like here we can use the timing template below T5 i.e. from T4 to T0 to bypass above rule.

```
nmap -T4 -p21-25 192.168.1.104
or
nmap -T3 -p21-25 192.168.1.104
or
nmap -T2 -p21-25 192.168.1.104
or
nmap -T1 -p21-25 192.168.1.104
or
nmap -T0 -p21-25 192.168.1.104
```

```
root@kali:~# nmap -T4 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 07:11 EST
Nmap scan report for 192.168.1.104
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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.62 seconds
```

Here, the packet transfer shows that each port has sent the reply but the first reply was instantly and other ports replied one by one after some time.

	Time	Source	Destination	Protocol	Length	Info
54	14.544158607	192.168.1.105	192.168.1.104	TCP	58	40511 → 22 [SYN] Seq=
55	14.544359544	192.168.1.105	192.168.1.104	TCP	58	40511 → 23 [SYN] Seq=
56	14.544502155	192.168.1.105	192.168.1.104	TCP	58	40511 → 21 [SYN] Seq=
57	14.544653152	192.168.1.105	192.168.1.104	TCP	58	40511 → 25 [SYN] Seq=
58	14.544748103	192.168.1.105	192.168.1.104	TCP	58	40511 → 24 [SYN] Seq=
60	14.545223396	192.168.1.105	192.168.1.104	TCP	54	1 40511 → 22 [RST]
63	15.647670168	192.168.1.105	192.168.1.104	TCP	58	40512 → 24 [SYN] Seq=
64	15.647901158	192.168.1.105	192.168.1.104	TCP	58	40512 → 25 [SYN] Seq=
65	15.648019730	192.168.1.105	192.168.1.104	TCP	58	40512 → 21 [SYN] Seq=
66	15.648164531	192.168.1.105	192.168.1.104	TCP	58	40512 → 23 [SYN] Seq=
68	15.648382634	192.168.1.105	192.168.1.104	TCP	54	2 40512 → 24 [RST]
70	16.750473752	192.168.1.105	192.168.1.104	TCP	58	40513 → 23 [SYN] Seq=
71	16.750685645	192.168.1.105	192.168.1.104	TCP	58	40513 → 21 [SYN] Seq=
72	16.750878115	192.168.1.105	192.168.1.104	TCP	58	40513 → 25 [SYN] Seq=
74	16.751251946	192.168.1.105	192.168.1.104	TCP	54	3 40513 → 23 [RST]
76	17.852533293	192.168.1.105	192.168.1.104	TCP	58	40514 → 25 [SYN] Seq=
77	17.852739192	192.168.1.105	192.168.1.104	TCP	58	40514 → 21 [SYN] Seq=
79	17.853391622	192.168.1.105	192.168.1.104	TCP	54	4 40514 → 25 [RST]
82	18.955524281	192.168.1.105	192.168.1.104	TCP	58	40515 → 21 [SYN] Seq=
84	18.955954654	192.168.1.105	192.168.1.104	TCP	54	5 40515 → 21 [RST]

Block Aggressive T4, Normal T3 & Polite T2 Scan

Now given below rules will block TCP packets from an IP address if the packet count **goes more than 1**. In other words, only the first packet will be responded from an IP address in 3 seconds.

```
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 3
```

```
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 3 --hitcount 1 -j DROP
xander@ubuntu:~$
```


Here we are using -T4 for scanning 5 ports, the time difference between packets is very much less than 1 second so if we scan five ports at a time it will show one as open/closed and others as filtered. But -T4 has also –max-retries set to 6 means it will retry to get the reply from ports 6 more times but as the time limit exceeds the total time taken by all retries it will show all ports filtered

```
nmap -T4 -p21-25 192.168.1.104
or
nmap -T3 -p21-25 192.168.1.104
or
nmap -T2 -p21-25 192.168.1.104
```

The Result of T4, T3, and T2 scan can be as **either** all port will be filtered **or** anyone port can show open/closed state. From given below image you can observe that it has shown **all 5 ports** are **filtered**.

```
root@kali:~# nmap -T4 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 07:17 EST
Nmap scan report for 192.168.1.104
Host is up (0.00038s latency).

PORT   STATE    SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
24/tcp filtered priv-mail
25/tcp filtered smtp
MAC Address: 00:0C:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
```


Here we can see that none of the packets got the reply

	Time	Source	Destination	Protocol	Length	Info
31	14.864709909	192.168.1.105	192.168.1.104	TCP	58	60709 → 22 [SYN]
32	14.864898127	192.168.1.105	192.168.1.104	TCP	58	60709 → 25 [SYN]
33	14.865011886	192.168.1.105	192.168.1.104	TCP	58	60709 → 23 [SYN]
34	14.865108287	192.168.1.105	192.168.1.104	TCP	58	60709 → 21 [SYN]
35	14.865243830	192.168.1.105	192.168.1.104	TCP	58	60709 → 24 [SYN]
36	15.967381795	192.168.1.105	192.168.1.104	TCP	58	60710 → 24 [SYN]
37	15.967592422	192.168.1.105	192.168.1.104	TCP	58	60710 → 21 [SYN]
38	15.967706625	192.168.1.105	192.168.1.104	TCP	58	60710 → 23 [SYN]
39	15.967835030	192.168.1.105	192.168.1.104	TCP	58	60710 → 25 [SYN]
40	15.967931326	192.168.1.105	192.168.1.104	TCP	58	60710 → 22 [SYN]

Bypass Aggressive T4, Normal T3 & Polite T2 Firewall filter

To bypass this kind of rule we have to use a Timing Template which is slower than -T4

```
nmap -T1 -p21-25 192.168.1.104
```

```
root@kali:~# nmap -T1 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 07:26 EST
Nmap scan report for 192.168.1.104
Host is up (0.0013s 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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 103.25 seconds
```

Here we can see that all the packets got a reply because the time interval in T1 is almost 15 seconds.

	Time	Source	Destination	Protocol	Length	Info
99	44.893943225	192.168.1.105	192.168.1.104	TCP	58	61287 → 23 [SYN] Seq
101	44.895843158	192.168.1.105	192.168.1.104	TCP	54	61287 → 23 [RST]
131	59.909434397	192.168.1.105	192.168.1.104	TCP	58	61287 → 21 [SYN] Seq
133	59.910248531	192.168.1.105	192.168.1.104	TCP	54	61287 → 21 [RST]
172	74.910835140	192.168.1.105	192.168.1.104	TCP	58	61287 → 22 [SYN] Seq
174	74.911630312	192.168.1.105	192.168.1.104	TCP	54	61287 → 22 [RST]
209	89.926127003	192.168.1.105	192.168.1.104	TCP	58	61287 → 25 [SYN] Seq
211	89.926878490	192.168.1.105	192.168.1.104	TCP	54	61287 → 25 [RST]
243	104.947879330	192.168.1.105	192.168.1.104	TCP	58	61287 → 24 [SYN] Seq
245	104.952729714	192.168.1.105	192.168.1.104	TCP	54	61287 → 24 [RST]

Block Sneaky (-T1) Scan

Now, this rule is to block TCP packets from an IP address if the packet count goes more than 1. In other words, only the first packet will be responded from an IP address in 200 seconds.

```
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 20
```

```
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 200 --hitcount 1 -j DROP
xander@ubuntu:~$
```

Now repeat the T1 scan again as given below and this time you will found that firewall is blocking our Nmap probes for identifying the open/closed state of any port.

```
nmap -T1 -p21-25 192.168.1.104
```

Results of T1 scan can be as **either** all port will be filtered **or** anyone port can show open/closed state. From given below image you can observe that it has shown **all 4 ports** are **filtered**.

```
root@kali:~# nmap -T1 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-26 06:46 EST
Nmap scan report for 192.168.1.104
Host is up (0.0022s 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: 14:2D:27:E8:C1:07 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 179.31 seconds
```

Here we can see that only one of the packets got the reply rest are drop by the firewall.

	Time	Source	Destination	Protoco	Length	Info
57	42.129504671	192.168.1.107	192.168.1.104	TCP	58	55955 → 23 [SYN] Seq=
58	42.131450675	192.168.1.104	192.168.1.107	TCP	60	23 → 55955 [SYN, ACK]
59	42.131690614	192.168.1.107	192.168.1.104	TCP	54	55955 → 23 [RST] Seq=
75	57.145022951	192.168.1.107	192.168.1.104	TCP	58	55955 → 22 [SYN] Seq=
85	73.163272713	192.168.1.107	192.168.1.104	TCP	58	55956 → 22 [SYN] Seq=
114	88.173139326	192.168.1.107	192.168.1.104	TCP	58	55955 → 25 [SYN] Seq=
134	103.185529085	192.168.1.107	192.168.1.104	TCP	58	55956 → 25 [SYN] Seq=
158	118.201747923	192.168.1.107	192.168.1.104	TCP	58	55955 → 21 [SYN] Seq=
178	133.216936340	192.168.1.107	192.168.1.104	TCP	58	55956 → 21 [SYN] Seq=
203	148.229065468	192.168.1.107	192.168.1.104	TCP	58	55955 → 24 [SYN] Seq=
224	163.244223214	192.168.1.107	192.168.1.104	TCP	58	55956 → 24 [SYN] Seq=

Bypass Sneaky (-T1) Scan

To bypass this kind of rule we have to use a Timing Template which has time difference in packets for more than 200 seconds, therefore use paranoid time scan because the time difference between two packets is near about 5 mints as discussed above.

```
nmap -T0 -p21-25 192.168.1.104
```

From given below image you can observe that it has taken **1813.61 sec** which is close to 30 mints for scanning 5 ports and found **open state** for all 5 ports.

```
root@kali:~# nmap -T0 -p21-25 192.168.1.104

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-23 13:45 EST
Nmap scan report for 192.168.1.104
Host is up (0.0027s 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:29:48:22:FD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1813.61 seconds
```

Here we can see that we have got the response of every packet even though the firewall had the security rules set.

To evade any type of IPS or Firewall, you need to remember that it will take much longer time than usual to scan the target system using a slower timing template. So try to specify a small number of ports, where the slow scans don't take time to scan the ports that you don't intend to.

	Time	Source	Destination	Protocol	Length	Info
248	2497.0006454…	192.168.1.5	192.168.1.104	TCP	58	48908 → 25 [SYN] Seq=
250	2497.0267467…	192.168.1.5	192.168.1.104	TCP	54	48908 → 25 [RST]
291	2797.0801653…	192.168.1.5	192.168.1.104	TCP	58	48908 → 23 [SYN] Seq=
293	2797.0813546…	192.168.1.5	192.168.1.104	TCP	54	48908 → 23 [RST]
313	3097.1607989…	192.168.1.5	192.168.1.104	TCP	58	48908 → 22 [SYN] Seq=
315	3097.1618679…	192.168.1.5	192.168.1.104	TCP	54	48908 → 22 [RST]
395	3397.2406533…	192.168.1.5	192.168.1.104	TCP	58	48908 → 21 [SYN] Seq=
397	3397.2414966…	192.168.1.5	192.168.1.104	TCP	54	48908 → 21 [RST]
419	3697.2930061…	192.168.1.5	192.168.1.104	TCP	58	48908 → 24 [SYN] Seq=
421	3697.2937272…	192.168.1.5	192.168.1.104	TCP	54	48908 → 24 [RST]