

COMPUTER NETWORKS

PES UNIVERSITY

INDUSTRY PROBLEM - I

WEB SERVER PACKET CAPTURING AND MONITERING TO AUTOMATE STATISTICAL INFERENCESES.

NAME:	SRN:
SAMARTH RAJENDRA	PES1UG20CS370
SANATH N BHARGAV	PES1UG20CS372
SANJAY K N	PES1UG20CS379

SECTION: "G"

Abstract/ Overview:

One of the major tasks in our project is to connect to a web server and check all the network connections that establish with time outs and everything. Here in this part of our project, the connections are displayed in the terminal by executing commands like netstat and nmap. NYKAA's IP address is being monitored by us.

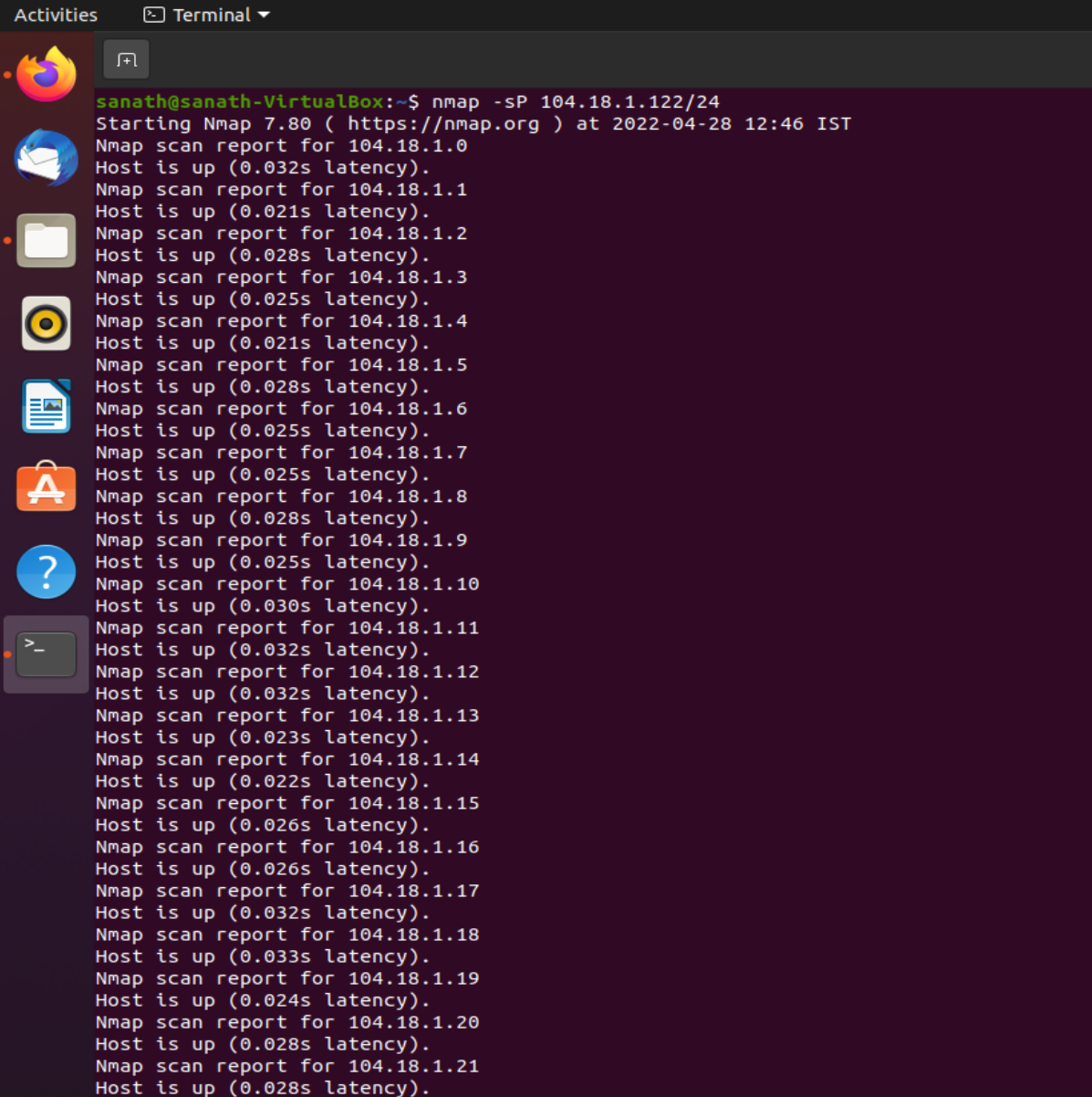
We have used tools like nmap to scan the network and server to obtain information about the target host. Netstat to analyze the TCP connections open (half or full) in the host and statistics on other parameters/protocols.

Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators use it for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. Netstat (network statistics) is a command-line network utility that displays network connections for Transmission Control Protocol (both incoming and outgoing), routing tables, and a number of network interface (network interface controller or software-defined network interface) and network protocol statistics. It is used for finding problems in the network and to determine the amount of traffic on the network as a performance measurement.

Reason For Analytics part:

If you are in IT or Security you have had to look at packets to troubleshoot or investigate an issue. Tools like Wireshark are great, but sometimes you need to automate or want to run something all on the terminal. This is a three-part post on monitoring network data with Python. We'll read a packet capture and plot the number of times each source IP is seen in the packet.

1. Scan the network for live systems / hosts



The screenshot shows a Linux desktop environment with a terminal window open. The terminal displays the output of an Nmap scan command. The command executed is `nmap -sP 104.18.1.122/24`. The output shows that all hosts in the range 104.18.1.0 to 104.18.1.21 are up, with varying latency times. The terminal window has a dark background and a sidebar on the left with various application icons.

```
sanath@sanath-VirtualBox:~$ nmap -sP 104.18.1.122/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-28 12:46 IST
Nmap scan report for 104.18.1.0
Host is up (0.032s latency).
Nmap scan report for 104.18.1.1
Host is up (0.021s latency).
Nmap scan report for 104.18.1.2
Host is up (0.028s latency).
Nmap scan report for 104.18.1.3
Host is up (0.025s latency).
Nmap scan report for 104.18.1.4
Host is up (0.021s latency).
Nmap scan report for 104.18.1.5
Host is up (0.028s latency).
Nmap scan report for 104.18.1.6
Host is up (0.025s latency).
Nmap scan report for 104.18.1.7
Host is up (0.025s latency).
Nmap scan report for 104.18.1.8
Host is up (0.028s latency).
Nmap scan report for 104.18.1.9
Host is up (0.025s latency).
Nmap scan report for 104.18.1.10
Host is up (0.030s latency).
Nmap scan report for 104.18.1.11
Host is up (0.032s latency).
Nmap scan report for 104.18.1.12
Host is up (0.032s latency).
Nmap scan report for 104.18.1.13
Host is up (0.023s latency).
Nmap scan report for 104.18.1.14
Host is up (0.022s latency).
Nmap scan report for 104.18.1.15
Host is up (0.026s latency).
Nmap scan report for 104.18.1.16
Host is up (0.026s latency).
Nmap scan report for 104.18.1.17
Host is up (0.032s latency).
Nmap scan report for 104.18.1.18
Host is up (0.033s latency).
Nmap scan report for 104.18.1.19
Host is up (0.024s latency).
Nmap scan report for 104.18.1.20
Host is up (0.028s latency).
Nmap scan report for 104.18.1.21
Host is up (0.028s latency).
```

```
Activities Terminal
Nmap scan report for 104.18.1.230
Host is up (0.030s latency).
Nmap scan report for 104.18.1.231
Host is up (0.042s latency).
Nmap scan report for 104.18.1.232
Host is up (0.030s latency).
Nmap scan report for 104.18.1.233
Host is up (0.030s latency).
Nmap scan report for 104.18.1.234
Host is up (0.030s latency).
Nmap scan report for 104.18.1.235
Host is up (0.042s latency).
Nmap scan report for 104.18.1.236
Host is up (0.030s latency).
Nmap scan report for 104.18.1.237
Host is up (0.030s latency).
Nmap scan report for 104.18.1.238
Host is up (0.030s latency).
Nmap scan report for 104.18.1.239
Host is up (0.030s latency).
Nmap scan report for 104.18.1.240
Host is up (0.042s latency).
Nmap scan report for 104.18.1.241
Host is up (0.042s latency).
Nmap scan report for 104.18.1.242
Host is up (0.031s latency).
Nmap scan report for 104.18.1.243
Host is up (0.029s latency).
Nmap scan report for 104.18.1.244
Host is up (0.032s latency).
Nmap scan report for 104.18.1.245
Host is up (0.032s latency).
Nmap scan report for 104.18.1.246
Host is up (0.032s latency).
Nmap scan report for 104.18.1.247
Host is up (0.032s latency).
Nmap scan report for 104.18.1.248
Host is up (0.032s latency).
Nmap scan report for 104.18.1.249
Host is up (0.032s latency).
Nmap scan report for 104.18.1.250
Host is up (0.032s latency).
Nmap scan report for 104.18.1.251
Host is up (0.032s latency).
Nmap scan report for 104.18.1.252
Host is up (0.032s latency).
Nmap scan report for 104.18.1.253
Host is up (0.032s latency).
Nmap scan report for 104.18.1.254
Host is up (0.032s latency).
Nmap scan report for 104.18.1.255
Host is up (0.032s latency).
Nmap done: 256 IP addresses (256 hosts up) scanned in 0.54 seconds
sanath@sanath-VirtualBox:~$
sanath@sanath-VirtualBox:~$
```

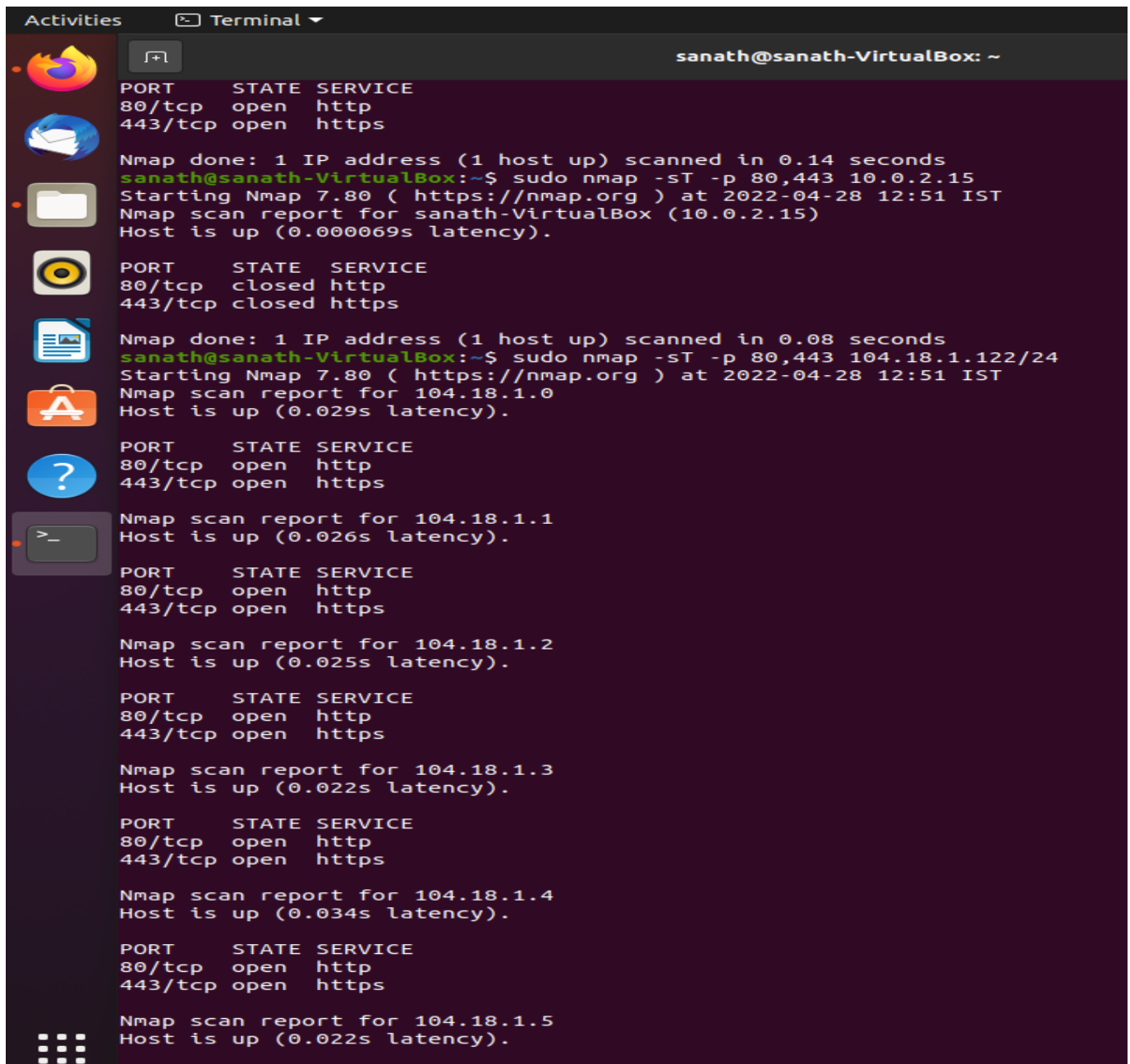
2.Port scanning a network / host

```
sanath@sanath-VirtualBox:~$
sanath@sanath-VirtualBox:~$
sanath@sanath-VirtualBox:~$ sudo nmap -d --packet-trace 104.18.1.122
[sudo] password for sanath:
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-28 12:47 IST
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0
-----
Initiating Ping Scan at 12:47
Scanning 104.18.1.122 [4 ports]
Packet capture filter (device enp0s3): dst host 10.0.2.15 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 104.18.1.122)))
SENT (0.0699s) ICMP [10.0.2.15 > 104.18.1.122 Echo request (type=8/code=0) id=8384 seq=0] IP [ttl=38 id=63528 iplen=28 ]
SENT (0.0701s) TCP 10.0.2.15:52390 > 104.18.1.122:443 S ttl=51 id=52790 iplen=44 seq=1026195140 win=1024 <mss 1460>
SENT (0.0702s) TCP 10.0.2.15:52390 > 104.18.1.122:80 A ttl=38 id=18057 iplen=40 seq=0 win=1024
SENT (0.0703s) ICMP [10.0.2.15 > 104.18.1.122 Timestamp request (type=13/code=0) id=26456 seq=0 orig=0 recv=0 trans=0] IP [ttl=47 id=53897 iplen=40
RCVD (0.0718s) TCP 104.18.1.122:80 > 10.0.2.15:52390 R ttl=255 id=9744 iplen=40 seq=1026195140 win=0
We got a TCP ping packet back from 104.18.1.122 port 80 (trynum = 0)
Completed Ping Scan at 12:47, 0.00s elapsed (1 total hosts)
Overall sending rates: 1069.80 packets / s, 40652.58 bytes / s.
mass_rdns: Using DNS server 127.0.0.53
NSOCK INFO [0.0720s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.0720s] nsock_connect_udp(): UDP connection requested to 127.0.0.53:53 (IOD #1) EID 8
NSOCK INFO [0.0720s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 18
Initiating Parallel DNS resolution of 1 host. at 12:47
NSOCK INFO [0.0720s] nsock_write(): Write request for 43 bytes to IOD #1 EID 27 [127.0.0.53:53]
NSOCK INFO [0.0720s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.53:53]
NSOCK INFO [0.0720s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 27 [127.0.0.53:53]
NSOCK INFO [0.1740s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [127.0.0.53:53] (43 bytes): .....122.1.18.104.in-addr
NSOCK INFO [0.1740s] nsock_read(): Read request from IOD #1 [127.0.0.53:53] (timeout: -1ms) EID 34
NSOCK INFO [0.1740s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1740s] nevent_delete(): nevent_delete on event #34 (type READ)
mass_rdns: 0.10s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 12:47, 0.10s elapsed
```

```
SENT (4.0577s) TCP 10.0.2.15:52647 > 104.18.1.122:1494 S ttl=52 id=18855 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0578s) TCP 10.0.2.15:52647 > 104.18.1.122:9 S ttl=49 id=21267 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0578s) TCP 10.0.2.15:52647 > 104.18.1.122:65000 S ttl=51 id=64834 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0579s) TCP 10.0.2.15:52647 > 104.18.1.122:544 S ttl=47 id=55206 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0579s) TCP 10.0.2.15:52647 > 104.18.1.122:2604 S ttl=40 id=32806 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0602s) TCP 10.0.2.15:52647 > 104.18.1.122:1863 S ttl=54 id=29130 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0602s) TCP 10.0.2.15:52647 > 104.18.1.122:52822 S ttl=39 id=41855 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0626s) TCP 10.0.2.15:52647 > 104.18.1.122:6100 S ttl=42 id=13034 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0627s) TCP 10.0.2.15:52647 > 104.18.1.122:9917 S ttl=37 id=19886 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0672s) TCP 10.0.2.15:52647 > 104.18.1.122:8000 S ttl=44 id=35979 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0673s) TCP 10.0.2.15:52647 > 104.18.1.122:38292 S ttl=47 id=43366 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0673s) TCP 10.0.2.15:52647 > 104.18.1.122:2399 S ttl=57 id=39060 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0674s) TCP 10.0.2.15:52647 > 104.18.1.122:55056 S ttl=52 id=7371 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0674s) TCP 10.0.2.15:52647 > 104.18.1.122:8200 S ttl=55 id=15566 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0674s) TCP 10.0.2.15:52647 > 104.18.1.122:7070 S ttl=46 id=38374 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0719s) TCP 10.0.2.15:52647 > 104.18.1.122:9220 S ttl=53 id=36660 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0719s) TCP 10.0.2.15:52647 > 104.18.1.122:1782 S ttl=53 id=47783 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0720s) TCP 10.0.2.15:52647 > 104.18.1.122:668 S ttl=40 id=53435 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0720s) TCP 10.0.2.15:52647 > 104.18.1.122:3211 S ttl=47 id=27689 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0720s) TCP 10.0.2.15:52647 > 104.18.1.122:2160 S ttl=46 id=10286 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0721s) TCP 10.0.2.15:52647 > 104.18.1.122:6666 S ttl=49 id=4153 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0721s) TCP 10.0.2.15:52647 > 104.18.1.122:666 S ttl=59 id=7231 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0721s) TCP 10.0.2.15:52647 > 104.18.1.122:5902 S ttl=44 id=2750 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0721s) TCP 10.0.2.15:52647 > 104.18.1.122:5560 S ttl=40 id=61002 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0748s) TCP 10.0.2.15:52647 > 104.18.1.122:2121 S ttl=42 id=63751 iplen=44 seq=3878212732 win=1024 <mss 1460>
SENT (4.0932s) TCP 10.0.2.15:52647 > 104.18.1.122:2869 S ttl=50 id=44785 iplen=44 seq=3878212732 win=1024 <mss 1460>
Completed SYN Stealth Scan at 12:47, 4.02s elapsed (1000 total ports)
Overall sending rates: 497.53 packets / s, 21888.25 bytes / s.
Nmap scan report for 104.18.1.122
Host is up, received reset ttl 255 (0.0073s latency).
Scanned at 2022-04-28 12:47:54 IST for 4s
Not shown: 998 filtered ports
Reason: 998 no-responses
PORT      STATE SERVICE REASON
80/tcp    open  http   syn-ack ttl 64
443/tcp   open  https  syn-ack ttl 64
Final times for host: srth: 7331 rttvar: 8869 to: 100000

Read from /usr/bin/./share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
Raw packets sent: 2005 (88.184KB) | Rcvd: 12 (488B)
sanath@sanath-VirtualBox:~$
```

3.TCP SYN Scan [syn,ack & rst Packets]



The screenshot shows a terminal window titled "Terminal" with the user "sanath@sanath-VirtualBox: ~". The terminal displays the output of Nmap TCP SYN scans for several IP addresses. The results are organized into sections, each starting with a table of open ports and services, followed by a summary line, the command used, and the scan report.

```
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
sanath@sanath-VirtualBox:~$ sudo nmap -sT -p 80,443 10.0.2.15
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-28 12:51 IST
Nmap scan report for sanath-VirtualBox (10.0.2.15)
Host is up (0.000069s latency).

PORT      STATE SERVICE
80/tcp    closed http
443/tcp   closed https

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
sanath@sanath-VirtualBox:~$ sudo nmap -sT -p 80,443 104.18.1.122/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-28 12:51 IST
Nmap scan report for 104.18.1.0
Host is up (0.029s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 104.18.1.1
Host is up (0.026s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 104.18.1.2
Host is up (0.025s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 104.18.1.3
Host is up (0.022s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 104.18.1.4
Host is up (0.034s latency).

PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for 104.18.1.5
Host is up (0.022s latency).
```



```
A Nmap scan report for 104.18.1.251
Host is up (0.011s latency).

? PORT      STATE SERVICE
80/tcp open  http
443/tcp open  https

> Nmap scan report for 104.18.1.252
Host is up (0.0085s latency).

PORT      STATE SERVICE
80/tcp open  http
443/tcp open  https

Nmap scan report for 104.18.1.253
Host is up (0.027s latency).

PORT      STATE SERVICE
80/tcp open  http
443/tcp open  https

Nmap scan report for 104.18.1.254
Host is up (0.010s latency).

PORT      STATE SERVICE
80/tcp open  http
443/tcp open  https

Nmap scan report for 104.18.1.255
Host is up (0.010s latency).

PORT      STATE SERVICE
80/tcp open  http
443/tcp open  https

Nmap done: 256 IP addresses (256 hosts up) scanned in 25.34 seconds
sanath@sanath-VirtualBox:~$
```

cnproject.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp && ip.addr ==104.18.1.122

No.	Time	Source	Destination	Protocol	Length	Info
156	4.365984	10.0.2.15	104.18.1.122	TLSv1.2	223	Application Data
157	4.367017	104.18.1.122	10.0.2.15	TCP	62	443 → 33114 [ACK] Seq=1 Ack=168 Win=65535 Len=0
181	4.516340	104.18.1.122	10.0.2.15	TLSv1.2	15994	Application Data
182	4.516377	10.0.2.15	104.18.1.122	TCP	56	33114 → 443 [ACK] Seq=168 Ack=15939 Win=65535 Len=0
187	4.517686	104.18.1.122	10.0.2.15	TLSv1.2	16116	Application Data, Application Data, Application Data,
188	4.517706	10.0.2.15	104.18.1.122	TCP	56	33114 → 443 [ACK] Seq=168 Ack=31999 Win=65535 Len=0
189	4.517791	104.18.1.122	10.0.2.15	TLSv1.2	15440	Application Data, Application Data, Application Data,
190	4.517804	10.0.2.15	104.18.1.122	TCP	56	33114 → 443 [ACK] Seq=168 Ack=47383 Win=65535 Len=0
300	4.914541	10.0.2.15	104.18.1.122	TLSv1.2	255	Application Data
301	4.915249	104.18.1.122	10.0.2.15	TCP	62	443 → 33114 [ACK] Seq=47383 Ack=367 Win=65535 Len=0
314	4.962557	104.18.1.122	10.0.2.15	TLSv1.2	8030	Application Data, Application Data
315	4.962589	10.0.2.15	104.18.1.122	TCP	56	33114 → 443 [ACK] Seq=367 Ack=55357 Win=65535 Len=0
447	5.805845	10.0.2.15	104.18.1.122	TLSv1.2	256	Application Data
448	5.806783	104.18.1.122	10.0.2.15	TCP	62	443 → 33114 [ACK] Seq=55357 Ack=567 Win=65535 Len=0
504	6.289042	104.18.1.122	10.0.2.15	TLSv1.2	154	Application Data

> Frame 156: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits)
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 10.0.2.15, Dst: 104.18.1.122
> Transmission Control Protocol, Src Port: 33114, Dst Port: 443, Seq: 1, Ack: 1, Len: 167
> Transport Layer Security

```
0000  00 04 00 01 00 06 08 00 27 cd 84 3d 00 00 08 00  .....'.=....
0010  45 00 00 cf fa 85 40 00 40 06 ca 08 0a 00 02 0f  E-...@. @.....
0020  68 12 01 7a 81 5a 01 bb 88 3e 71 13 34 ba d3 d0  h-z-Z...->q.4...
0030  50 18 ff ff 76 5c 00 00 17 03 03 00 a2 00 00 00  P...v\.....
0040  00 00 00 00 1d a7 c0 58 13 41 c2 f8 88 28 34 7e  ....X-A... (4~
```


4. Netstat to check TCP active connections

```
Nmap done: 256 IP addresses (256 hosts up) scanned in 25.34 seconds
sanath@sanath-VirtualBox:~$
sanath@sanath-VirtualBox:~$
sanath@sanath-VirtualBox:~$
sanath@sanath-VirtualBox:~$ netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 sanath-VirtualBox:57292 82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 sanath-VirtualBox:37276 ec2-54-187-160-31:https ESTABLISHED
tcp        0      0 sanath-VirtualBox:57290 82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 sanath-VirtualBox:57348 136.143.191.144:https  ESTABLISHED
tcp        0      0 sanath-VirtualBox:35784 maa05s24-in-f10.1:https ESTABLISHED
tcp        0      0 sanath-VirtualBox:49200 static.203.72.40.:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp      [::]:*                  LISTEN
sanath@sanath-VirtualBox:~$
```

5. Netstat to check TCP half open connections

```
sanath@sanath-VirtualBox:~$
sanath@sanath-VirtualBox:~$ netstat ss -a | grep "SYN"
sanath@sanath-VirtualBox:~$ netstat -tnal
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.15:57292        34.107.221.82:80        ESTABLISHED
tcp        0      0 10.0.2.15:37276        54.187.160.31:443       ESTABLISHED
tcp        0      0 10.0.2.15:57290        34.107.221.82:80        ESTABLISHED
tcp        0      0 10.0.2.15:57348        136.143.191.144:443     ESTABLISHED
tcp        0      0 10.0.2.15:35784        142.250.193.106:443     ESTABLISHED
tcp        0      0 10.0.2.15:49200        188.40.72.203:443       ESTABLISHED
tcp6       0      0 :::1:631               :::*                     LISTEN
sanath@sanath-VirtualBox:~$ netstat ss -a | grep "HTTP"
sanath@sanath-VirtualBox:~$ netstat -a http-method == "GET"
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp        0      0 sanath-VirtualBox:57292 82.221.107.34.bc.g:http TIME_WAIT
tcp        0      0 sanath-VirtualBox:37276 ec2-54-187-160-31:https ESTABLISHED
tcp        0      0 sanath-VirtualBox:57290 82.221.107.34.bc.g:http TIME_WAIT
tcp        0      0 sanath-VirtualBox:57348 136.143.191.144:https  ESTABLISHED
tcp        0      0 sanath-VirtualBox:35784 maa05s24-in-f10.1:https ESTABLISHED
tcp        0      0 sanath-VirtualBox:49200 static.203.72.40.:https ESTABLISHED
tcp6       0      0 ip6-localhost:ipp      [::]:*                  LISTEN
udp        0      0 0.0.0.0:631            0.0.0.0:*               LISTEN
udp        0      0 0.0.0.0:56188          0.0.0.0:*               LISTEN
udp        0      0 localhost:domain       0.0.0.0:*               LISTEN
udp        0      0 sanath-VirtualBo:bootpc _gateway:bootps         ESTABLISHED
udp        0      0 0.0.0.0:mdns            0.0.0.0:*               LISTEN
udp6       0      0 [::]:mdns               [::]:*                   LISTEN
udp6       0      0 [::]:46407              [::]:*                   LISTEN
raw6       0      0 [::]:ipv6-icmp          [::]:*                   LISTEN
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State       I-Node      Path
unix    2      [ ]         DGRAM      LISTENING   30784       /run/user/1000/systemd/notify
unix    2      [ ]         DGRAM      LISTENING   26163       /run/user/125/systemd/notify
unix    2      [ ACC ]     STREAM     LISTENING   30790       /run/user/1000/systemd/private
unix    2      [ ACC ]     STREAM     LISTENING   26166       /run/user/125/systemd/private
unix    2      [ ACC ]     STREAM     LISTENING   30817       /run/user/1000/bus
unix    2      [ ACC ]     STREAM     LISTENING   26172       /run/user/125/bus
unix    2      [ ACC ]     STREAM     LISTENING   30818       /run/user/1000/gnupg/S.dirmngr
unix    2      [ ACC ]     STREAM     LISTENING   26173       /run/user/125/gnupg/S.dirmngr
unix    2      [ ACC ]     STREAM     LISTENING   30819       /run/user/1000/gnupg/S.gpg-agent.browser
unix    2      [ ACC ]     STREAM     LISTENING   26174       /run/user/125/gnupg/S.gpg-agent.browser
unix    2      [ ACC ]     STREAM     LISTENING   30820       /run/user/1000/gnupg/S.gpg-agent.extra
unix    2      [ ACC ]     STREAM     LISTENING   26175       /run/user/125/gnupg/S.gpg-agent.extra
unix    2      [ ACC ]     STREAM     LISTENING   30821       /run/user/1000/gnupg/S.gpg-agent.ssh
unix    2      [ ACC ]     STREAM     LISTENING   26176       /run/user/125/gnupg/S.gpg-agent.ssh
unix    2      [ ACC ]     STREAM     LISTENING   30822       /run/user/1000/gnupg/S.gpg-agent
unix    2      [ ACC ]     STREAM     LISTENING   26177       /run/user/125/gnupg/S.gpg-agent
```

```

unix 3 [ ] STREAM CONNECTED 130536
unix 3 [ ] STREAM CONNECTED 35119 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 35068
unix 3 [ ] STREAM CONNECTED 161602 @/dbus-vfs-daemon/socket-ïFUaXCMg
unix 3 [ ] STREAM CONNECTED 41205 @/tmp/dbus-RsxRRdE0Dn
unix 3 [ ] STREAM CONNECTED 36982
unix 3 [ ] STREAM CONNECTED 26521
unix 3 [ ] STREAM CONNECTED 33416 @/tmp/dbus-RsxRRdE0Dn
unix 3 [ ] STREAM CONNECTED 31784 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 25496 /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 41200 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 33622 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 22251
unix 3 [ ] STREAM CONNECTED 35436
unix 3 [ ] STREAM CONNECTED 167200
unix 3 [ ] SEQPACKET CONNECTED 148042
unix 2 [ ] STREAM CONNECTED 135669
unix 3 [ ] STREAM CONNECTED 38897
unix 3 [ ] STREAM CONNECTED 36069
unix 3 [ ] STREAM CONNECTED 120858 /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 33527
unix 3 [ ] STREAM CONNECTED 33517 @/home/sanath/.cache/ibus/dbus-TBgd3Q0N
unix 3 [ ] STREAM CONNECTED 27133 /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 21359
unix 3 [ ] STREAM CONNECTED 178334
unix 3 [ ] STREAM CONNECTED 130595
unix 3 [ ] STREAM CONNECTED 27042
unix 3 [ ] STREAM CONNECTED 38817 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 23386
unix 3 [ ] STREAM CONNECTED 22816 /run/dbus/system_bus_socket
unix 3 [ ] STREAM CONNECTED 130839 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 38848 @/tmp/.X11-unix/X0
unix 2 [ ] DGRAM 36171
unix 3 [ ] STREAM CONNECTED 30188 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 36130
unix 3 [ ] STREAM CONNECTED 35491 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 33362 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 34564
unix 3 [ ] STREAM CONNECTED 33284 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 31164
unix 3 [ ] STREAM CONNECTED 21052
unix 3 [ ] STREAM CONNECTED 37092
unix 3 [ ] STREAM CONNECTED 26889
unix 3 [ ] STREAM CONNECTED 129674 /run/user/1000/pulse/native
unix 3 [ ] STREAM CONNECTED 35202 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 34657 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 33740 /run/user/1000/bus
unix 3 [ ] STREAM CONNECTED 33545
unix 3 [ ] STREAM CONNECTED 33418 @/tmp/.X11-unix/X0
unix 3 [ ] STREAM CONNECTED 31018 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 161610 @/dbus-vfs-daemon/socket-xXyqs0Tf
unix 3 [ ] STREAM CONNECTED 33450
unix 3 [ ] STREAM CONNECTED 30923 /run/systemd/journal/stdout
unix 3 [ ] STREAM CONNECTED 25817 /run/dbus/system_bus_socket
sanath@sanath-VirtualBox:~$ █

```