IT352: Information Assurance and Security

Lab Assignment 3

Name: Chinmayi C. Ramakrishna **Date of Submission:** 10th Feb, 2021

Roll No.: 181IT113

Objectives:

1. Use the sniff( ) function before capturing the real-time network traffic.
2. Display the entire captured packet in raw format onto the terminal of the host system and also display all the header fields of the captured packet (Ethernet, IP and ICMP/TCP/UDP) in human-understandable form onto the terminal of the host system.
3. Demonstrate the Packet Filtering Firewall operations by using appropriate extracted header fields of the captured packet as well as the given ACL file.

Screenshots

Test Case 1

Source IP: 20.20.20.20

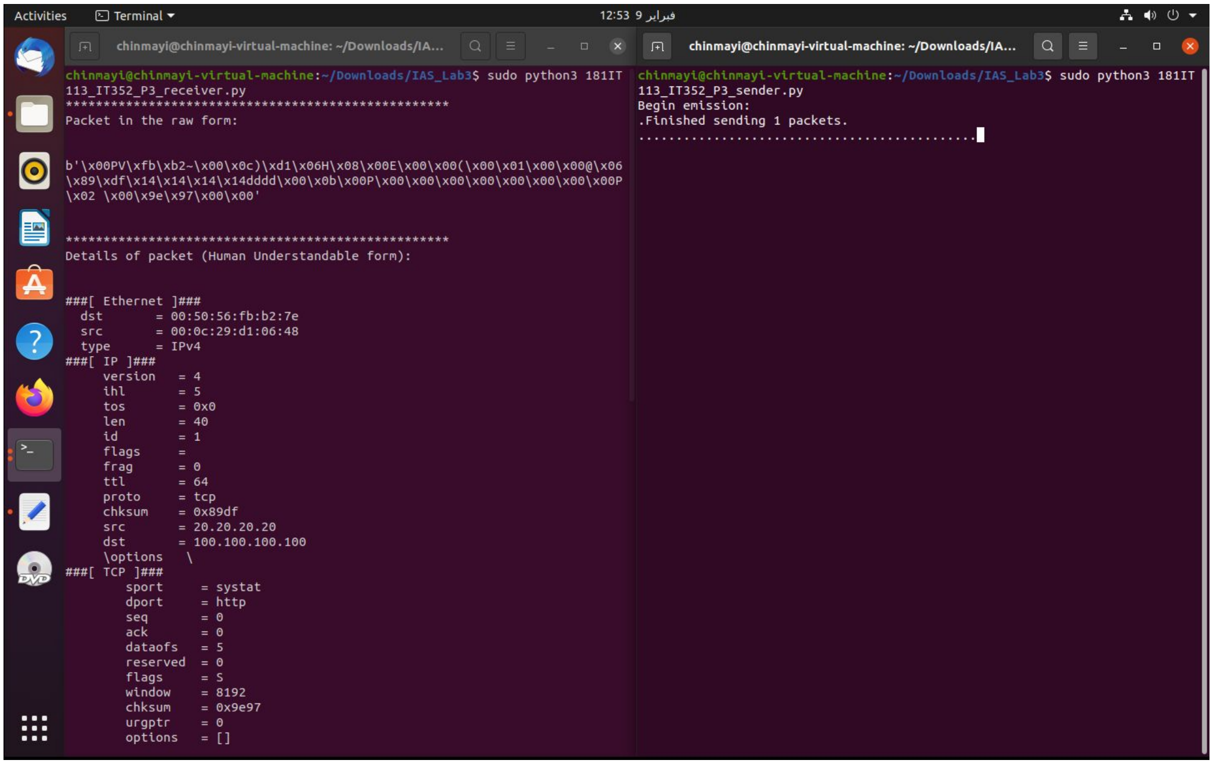
Destination IP: 100.100.100.100

Source port: 11

Destination port: 80.

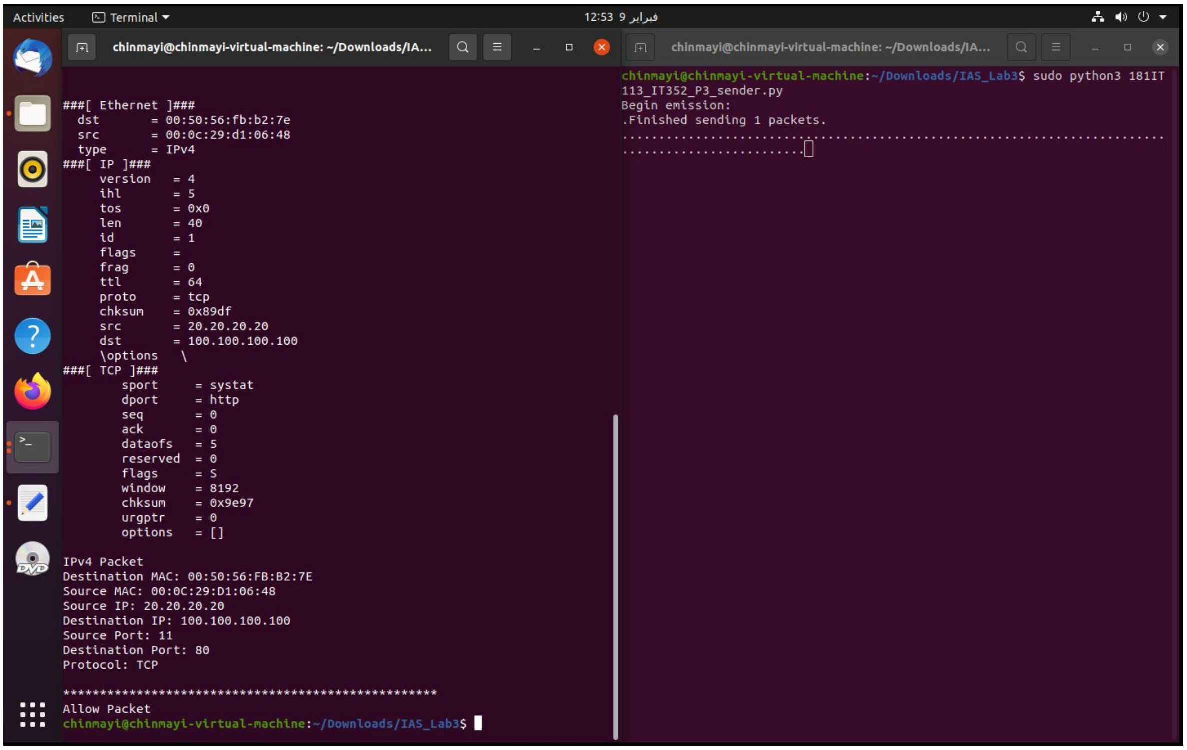
Function used: sr1()

Destination IP to set the filter option in sniff() function: 100.100.100.100


Activities
Terminal
12:53 9 فبراير
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_receiver.py
**************************************************
Packet in the raw form:


b'\x00PV\xfb\xb2~\x00\x0c)\xd1\x06H\x08\x00E\x00\x00(\x00\x01\x00\x00@\x06
\x89\xdf\x14\x14\x14\x14dddd\x00\x0b\x00P\x00\x00\x00\x00\x00\x00\x00\x00P
\x02 \x00\x9e\x97\x00\x00'


**************************************************
Details of packet (Human Understandable form):


###[ Ethernet ]###
  dst       = 00:50:56:fb:b2:7e
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x89df
     src       = 20.20.20.20
     dst       = 100.100.100.100
     \options   \
###[ TCP ]###
        sport     = systat
        dport     = http
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0x9e97
        urgptr    = 0
        options   = []
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
Begin emission:
.Finished sending 1 packets.
.............................................
```


Activities
Terminal
12:53 9 فبراير
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...

```
###[ Ethernet ]###
  dst       = 00:50:56:fb:b2:7e
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x89df
     src       = 20.20.20.20
     dst       = 100.100.100.100
     \options   \
###[ TCP ]###
        sport     = systat
        dport     = http
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0x9e97
        urgptr    = 0
        options   = []

IPv4 Packet
Destination MAC: 00:50:56:FB:B2:7E
Source MAC: 00:0C:29:D1:06:48
Source IP: 20.20.20.20
Destination IP: 100.100.100.100
Source Port: 11
Destination Port: 80
Protocol: TCP

***************************************************
Allow Packet
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
Begin emission:
.Finished sending 1 packets.
..........................................................................
.........................
```

Test Case 2

Source IP: 200.200.200.200

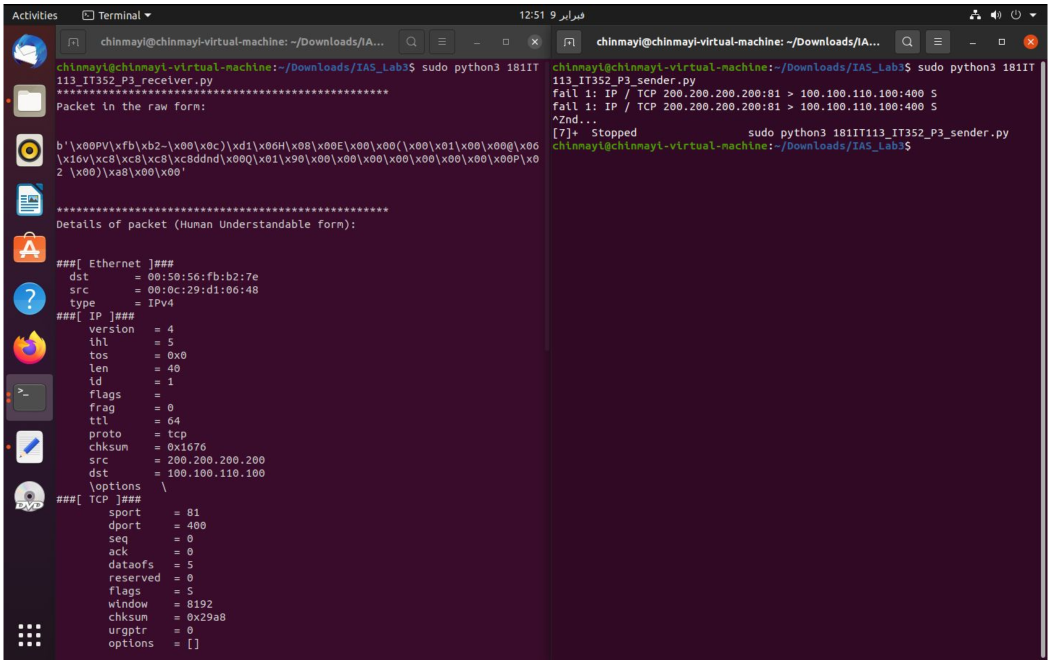
Destination IP: 100.100.110.100

Source port: 81

Destination port: 400

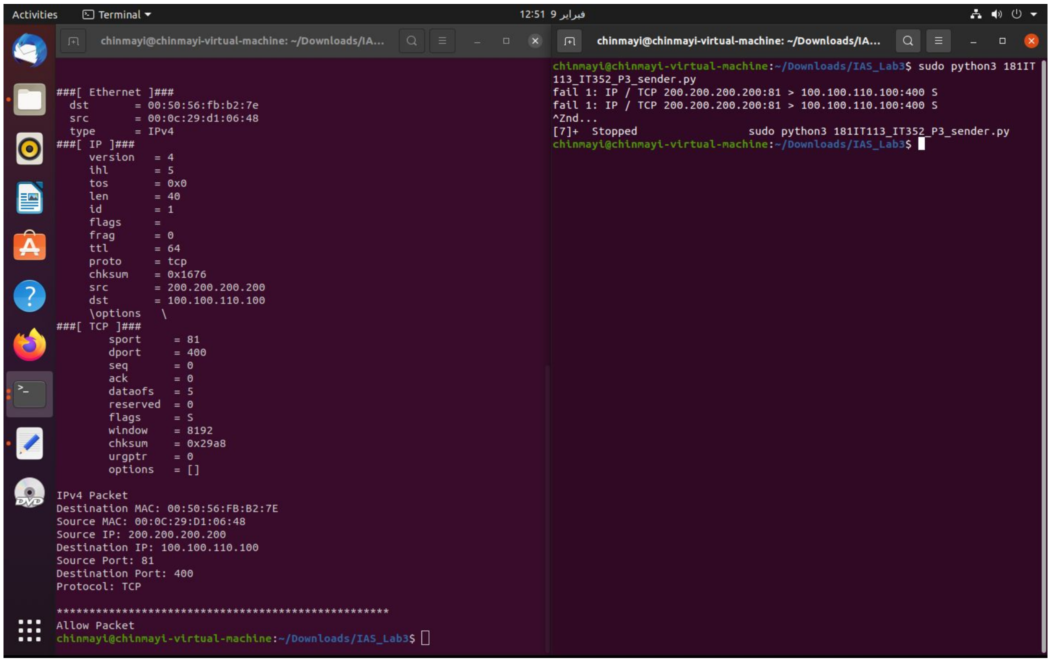
Function used: srloop()

Destination IP to set the filter option in sniff() function: 100.100.110.100



```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_receiver.py
***************************************************
Packet in the raw form:


b'\x00PV\xfb\xb2~\x00\x0c)\xd1\x06H\x08\x00E\x00\x00(\x00\x01\x00\x00@\x06
\x16v\xc8\xc8\xc8\xc8ddnd\x00Q\x01\x90\x00\x00\x00\x00\x00\x00\x00\x00P\x0
2 \x00)\xa8\x00\x00'


***************************************************
Details of packet (Human Understandable form):


###[ Ethernet ]###
  dst       = 00:50:56:fb:b2:7e
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x1676
     src       = 200.200.200.200
     dst       = 100.100.110.100
     \options   \
###[ TCP ]###
        sport     = 81
        dport     = 400
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0x29a8
        urgptr    = 0
        options   = []
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
fail 1: IP / TCP 200.200.200.200:81 > 100.100.110.100:400 S
fail 1: IP / TCP 200.200.200.200:81 > 100.100.110.100:400 S
^Znd...
[7]+  Stopped                 sudo python3 181IT113_IT352_P3_sender.py
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$
```

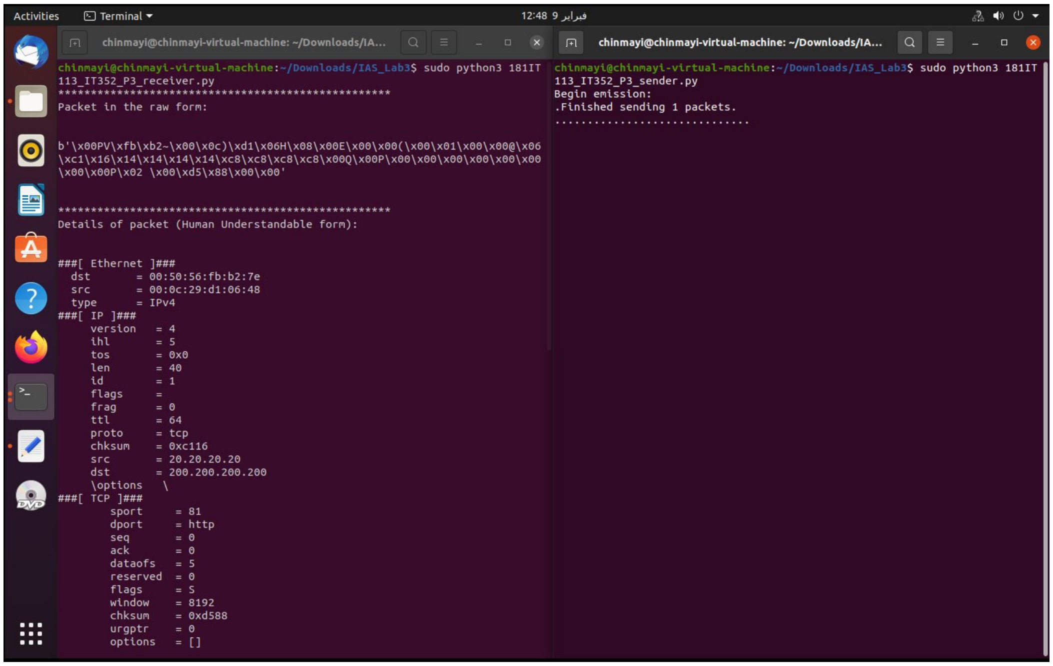


```
###[ Ethernet ]###
  dst       = 00:50:56:fb:b2:7e
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x1676
     src       = 200.200.200.200
     dst       = 100.100.110.100
     \options   \
###[ TCP ]###
        sport     = 81
        dport     = 400
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0x29a8
        urgptr    = 0
        options   = []

IPv4 Packet
Destination MAC: 00:50:56:FB:B2:7E
Source MAC: 00:0C:29:D1:06:48
Source IP: 200.200.200.200
Destination IP: 100.100.110.100
Source Port: 81
Destination Port: 400
Protocol: TCP

***************************************************
Allow Packet
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
fail 1: IP / TCP 200.200.200.200:81 > 100.100.110.100:400 S
fail 1: IP / TCP 200.200.200.200:81 > 100.100.110.100:400 S
^Znd...
[7]+  Stopped                 sudo python3 181IT113_IT352_P3_sender.py
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$
```

Test Case 3

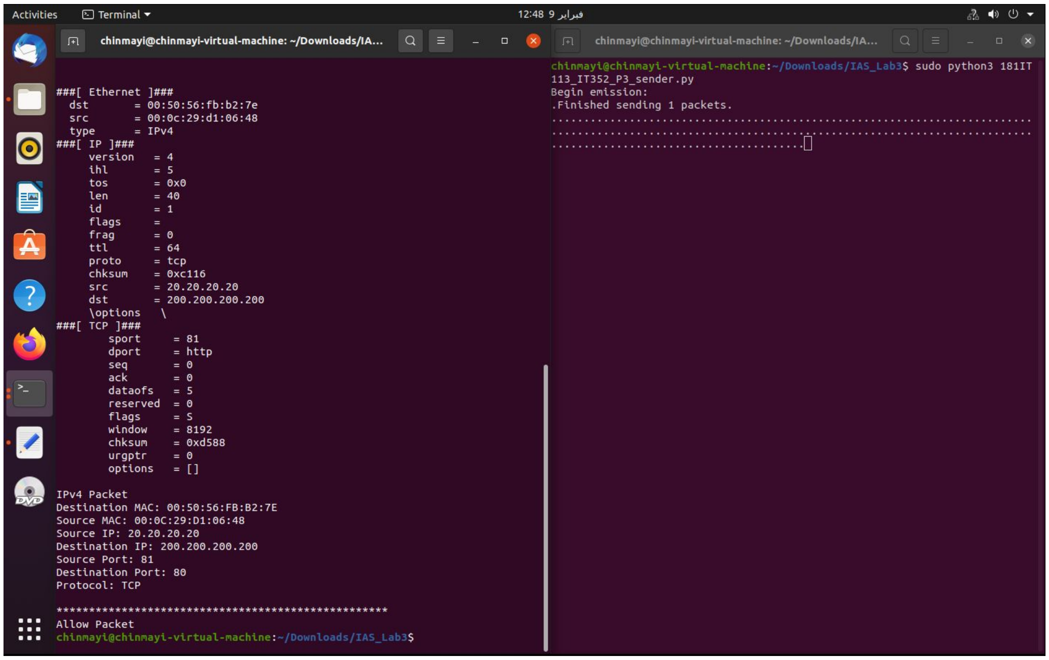
Source IP: 20.20.20.20
Destination IP: 200.200.200.200
Source port: 81
Destination port: 80.
Function used: sr()
Destination IP to set the filter option in sniff() function: 200.200.200.200



Activities
Terminal
12:48 9 فبراير
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_receiver.py
***************************************************
Packet in the raw form:


b'\x00PV\xfb\xb2~\x00\x0c)\xd1\x06H\x08\x00E\x00\x00(\x00\x01\x00\x00@\x06
\xc1\x16\x14\x14\x14\x14\xc8\xc8\xc8\xc8\x00Q\x00P\x00\x00\x00\x00\x00\x00
\x00\x00P\x02 \x00\xd5\x88\x00\x00'


***************************************************
Details of packet (Human Understandable form):


###[ Ethernet ]###
  dst       = 00:50:56:fb:b2:7e
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xc116
     src       = 20.20.20.20
     dst       = 200.200.200.200
     \options   \
###[ TCP ]###
        sport     = 81
        dport     = http
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0xd588
        urgptr    = 0
        options   = []
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
Begin emission:
.Finished sending 1 packets.
.............................
```



Activities
Terminal
12:48 9 فبراير
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...

```
###[ Ethernet ]###
  dst       = 00:50:56:fb:b2:7e
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0xc116
     src       = 20.20.20.20
     dst       = 200.200.200.200
     \options   \
###[ TCP ]###
        sport     = 81
        dport     = http
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0xd588
        urgptr    = 0
        options   = []

IPv4 Packet
Destination MAC: 00:50:56:FB:B2:7E
Source MAC: 00:0C:29:D1:06:48
Source IP: 20.20.20.20
Destination IP: 200.200.200.200
Source Port: 81
Destination Port: 80
Protocol: TCP

***************************************************
Allow Packet
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
Begin emission:
.Finished sending 1 packets.
..........................................................................
..........................................................................
.......................................
```

Test Case 4

Source IP: 200.20.202.20

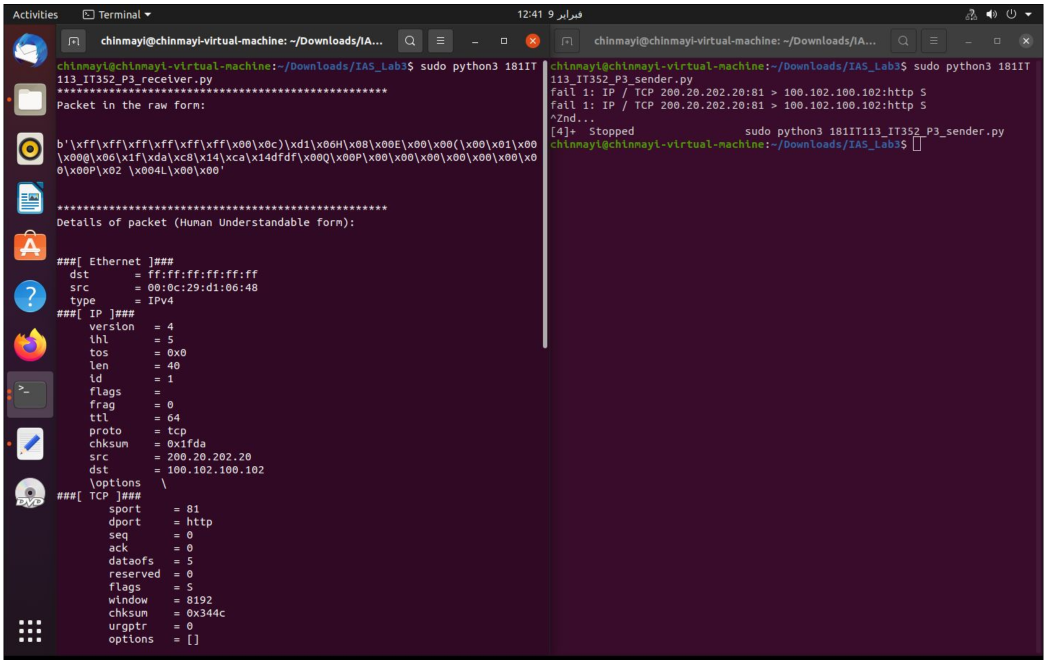
Destination IP: 100.102.100.102

Source port: 81

Destination port: 80.

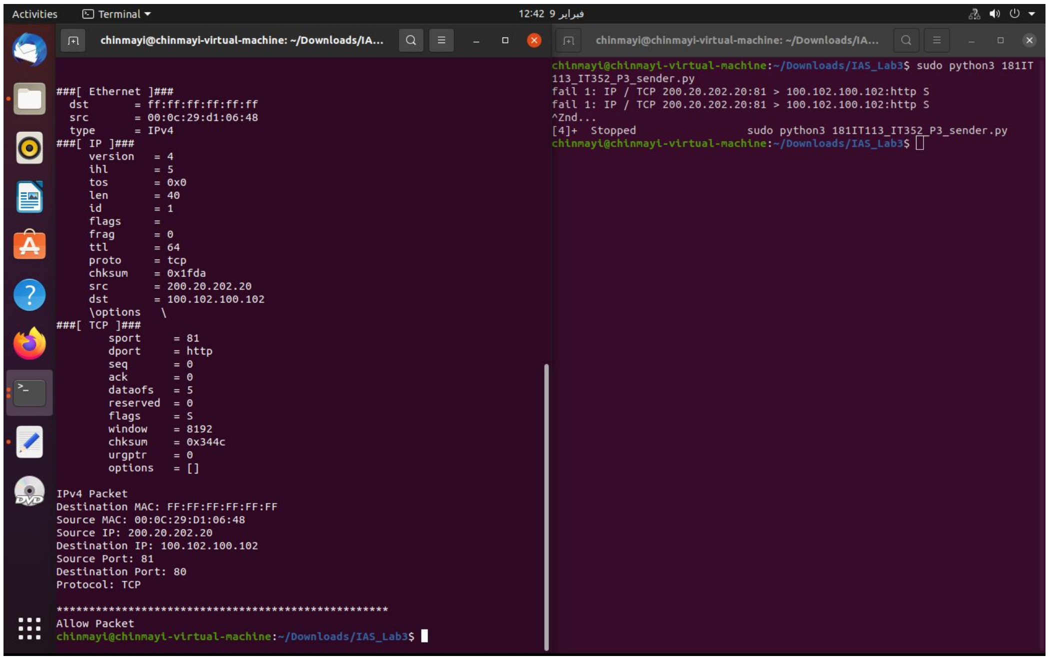
Function used: srloop()

Destination IP to set the filter option in sniff() function: 100.102.100.102


Activities
Terminal
12:41 9 فبراير
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_receiver.py
****************************************************
Packet in the raw form:


b'\xff\xff\xff\xff\xff\xff\x00\x0c)\xd1\x06H\x08\x00E\x00\x00(\x00\x01\x00
\x00@\x06\x1f\xda\xc8\x14\xca\x14dfdf\x00Q\x00P\x00\x00\x00\x00\x00\x00\x0
0\x00P\x02 \x004L\x00\x00'


****************************************************
Details of packet (Human Understandable form):


###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x1fda
     src       = 200.20.202.20
     dst       = 100.102.100.102
     \options   \
###[ TCP ]###
        sport     = 81
        dport     = http
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0x344c
        urgptr    = 0
        options   = []
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
fail 1: IP / TCP 200.20.202.20:81 > 100.102.100.102:http S
fail 1: IP / TCP 200.20.202.20:81 > 100.102.100.102:http S
^Znd...
[4]+  Stopped                 sudo python3 181IT113_IT352_P3_sender.py
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ 
```


Activities
Terminal
12:42 9 فبراير
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...
chinmayi@chinmayi-virtual-machine: ~/Downloads/IA...

```
###[ Ethernet ]###
  dst       = ff:ff:ff:ff:ff:ff
  src       = 00:0c:29:d1:06:48
  type      = IPv4
###[ IP ]###
     version   = 4
     ihl       = 5
     tos       = 0x0
     len       = 40
     id        = 1
     flags     =
     frag      = 0
     ttl       = 64
     proto     = tcp
     chksum    = 0x1fda
     src       = 200.20.202.20
     dst       = 100.102.100.102
     \options   \
###[ TCP ]###
        sport     = 81
        dport     = http
        seq       = 0
        ack       = 0
        dataofs   = 5
        reserved  = 0
        flags     = S
        window    = 8192
        chksum    = 0x344c
        urgptr    = 0
        options   = []

IPv4 Packet
Destination MAC: FF:FF:FF:FF:FF:FF
Source MAC: 00:0C:29:D1:06:48
Source IP: 200.20.202.20
Destination IP: 100.102.100.102
Source Port: 81
Destination Port: 80
Protocol: TCP

****************************************************
Allow Packet
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ 
```

```
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ sudo python3 181IT
113_IT352_P3_sender.py
fail 1: IP / TCP 200.20.202.20:81 > 100.102.100.102:http S
fail 1: IP / TCP 200.20.202.20:81 > 100.102.100.102:http S
^Znd...
[4]+  Stopped                 sudo python3 181IT113_IT352_P3_sender.py
chinmayi@chinmayi-virtual-machine:~/Downloads/IAS_Lab3$ 
```