

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

The image shows two terminal windows from a virtual machine. The left window displays the output of a packet capture using the '181IT' tool. It shows the raw packet data in hexadecimal and ASCII, followed by a human-readable summary of the packet headers. The summary includes Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol details. The right window shows the output of a script named '113_IT352_P3_sender.py', which indicates that it has begun an emission and finished sending 1 packet.

```
chinnmayi@chinnmayi-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\x00H\x00\x00E\x00\x00(\x00\x01\x00\x00@\x00
\x89\xdf\x14\x14\x14\x14\x14\x14\x14\x14\x14\x14\x14\x14\x14\x14\x14\x14
\x02 \x00 \x9e\x97\x00\x00'
*****
Details of packet (Human Understandable form):
###[ Ethernet ]###
dst      = 00:50:56:fb:b2:7e
src      = 00:0c:29:d1:00:48
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  = []

chinnmayi@chinnmayi-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 2020
chinnmayi@chinnmayi-virtual-machine: ~/Downloads/IA...
chinnmayi@chinnmayi-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    = 5
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
chinnmayi@chinnmayi-virtual-machine:~/Downloads/IAS_Lab3$

chinnmayi@chinnmayi-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

The image shows two terminal windows side-by-side, both running on a Linux system (Ubuntu 20.04 LTS). The left window shows the output of the command `sudo python3 1811T113_ITS2_P3_receiver.py`, which displays the raw packet data for an ICMP Echo (ping) request. The right window shows the output of the command `sudo python3 1811T113_ITS2_P3_sender.py`, which displays the packet data after being processed by a script, showing the destination IP and port.

```

chinnmayi@chinnmayi-virtual-machine: ~/Downloads/IA...
chinnmayi@chinnmayi-virtual-machine:~/Downloads/IAS_Labs$ sudo python3 1811T
113 ITS2_P3_receiver.py
*****
Packet in the raw form:

b'\x00Pv\xfb\x2-\x00\xc'\xd1\x06H\x00\x0E\x00\x00(\x00\x01\x00\x00)\x06
\x16v\xcc\x08\x08\xdd\x00\x00Q\x01\x00\x00\x00\x00\x00\x00\x00P\x00
2 \x00)\xa0\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      = 0x00
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   = 65535
chksum   = 0x29a8
urgptr   = 0
options  = []
  
```

The image shows a Kali Linux desktop environment. In the foreground, a terminal window displays the output of a network traffic analysis tool, likely Wireshark's packet details pane. The output shows an Ethernet II packet, an IP packet, and a TCP packet. The IP packet details include version, length, flags, and source/destination addresses. The TCP packet details include source/destination ports and flags. The output is as follows:

```
###[ 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
dataoffs = 5
reserved = 0
flags    = 5
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
chinmay@chinmay-virtual-machine:~/Downloads/IAS_Lab3$
```

In the background, a file manager window is open, showing the contents of the directory ~/Downloads/IAS_Lab3. The files listed are:

- 113_IT352_P3_sender.py
- 181IT113_IT352_P3_sender.py
- IAS_Lab3\$

Test Case 3

Source IP: 20.20.20.20

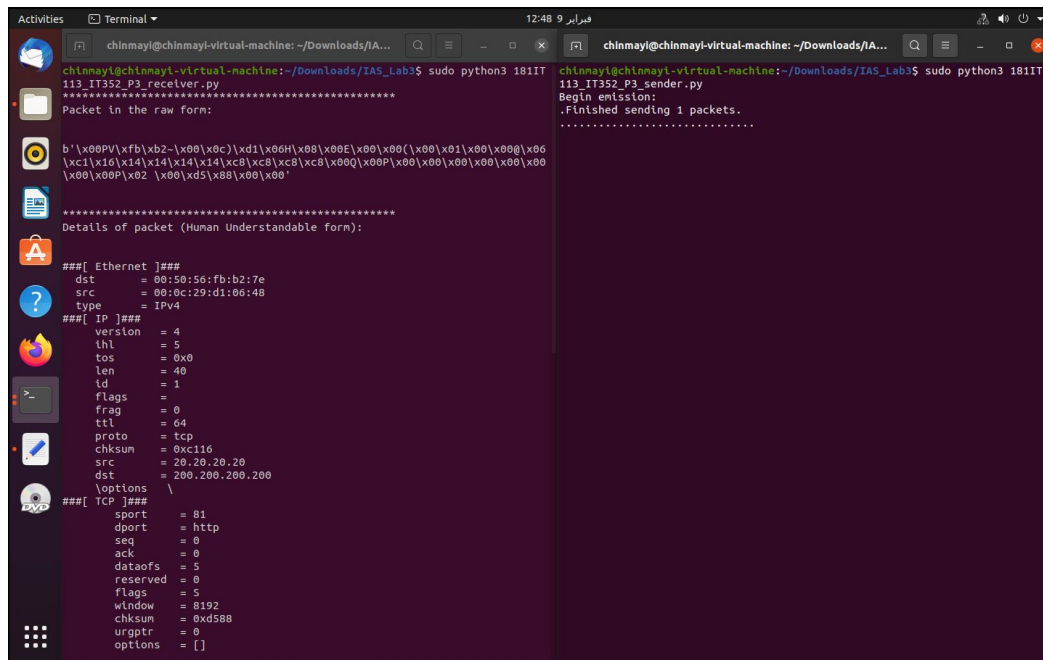
Destination IP: 200.200.200.200

Source port: 81

Destination port: 80.

Function used: sr()

Destination IP to set the filter option in sniff() function: 200.200.200.200



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

b'\x00PV\xfb\xb2-\x00\x0c\xdi\x00H\x00\x00E\x00\x00(\x00\x01\x00\x00@\x06
\x01\x16\x14\x14\x14\x14\x0c\x0c\x0c\x0c\x0c\x00P\x00\x00\x00\x00\x00
\x00\x00P\x02 \x00\x05\x08\x00\x00'

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

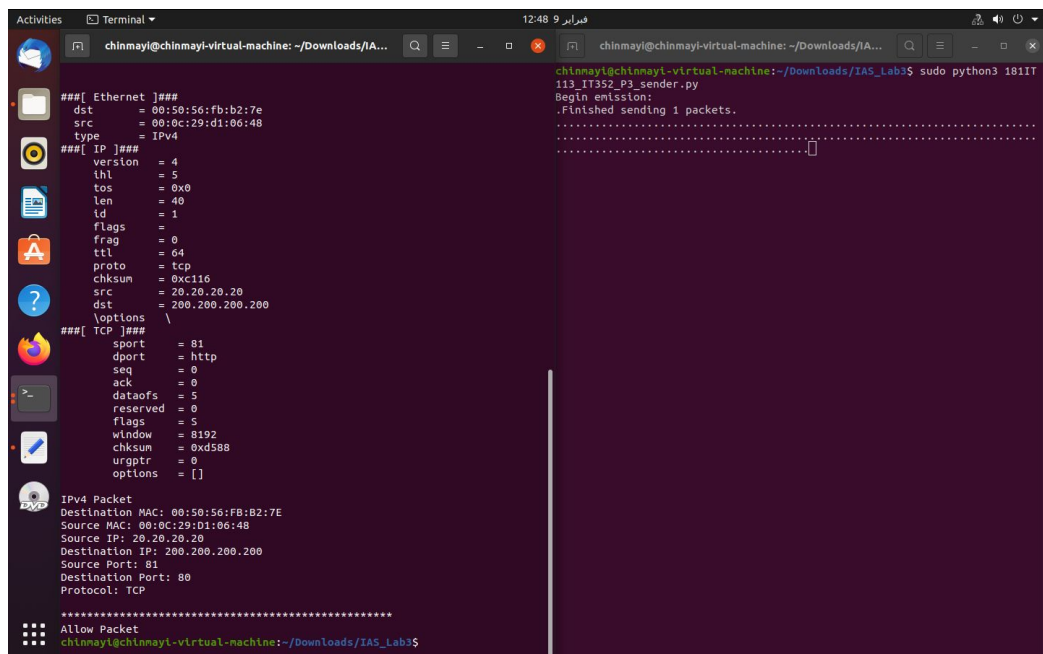
###[ Ethernet ]###
dst      = 00:50:56:fb:b2:7e
src      = 00:0c:29:d1:06:48
type     = IPv4

###[ IP ]###
version  = 4
ihl      = 5
tos      = 0x0
len      = 40
id       = 1
flags    = 0
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    = 5
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
chinnmayi@chinnmayi-virtual-machine: ~/Downloads/IAS_Lab3$
```



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

###[ 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    = 0
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    = 5
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
chinnmayi@chinnmayi-virtual-machine: ~/Downloads/IAS_Lab3$
```

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 9  
chinmay@chinmay-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\xff\xff\x00\x0c\xd1\x06:\x00\x00\x00\x00\x01\x00  
\x00\x06\x1f\xda\xc8\x14\kca\x14dfrf\x00\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 = []  
  
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  
chinmay@chinmay-virtual-machine:~/Downloads/IAS_Lab3$
```