**Program to implement packet capturing in Python:**

#Packet sniffer in python #For Linux - Sniffs all incoming and outgoing packets :)

import socket, sys

from struct import \*

#Convert a string of 6 characters of ethernet address into a dash separated hex string

def eth\_addr (a) :

b = "%.2x:%.2x:%.2x:%.2x:%.2x:%.2x" % (ord(a[0]) , ord(a[1]) , ord(a[2]), ord(a[3]), ord(a[4]) , ord(a[5]))

return b

#create a AF\_PACKET type raw socket (thats basically packet level)

#define ETH\_P\_ALL 0x0003 /\* Every packet (be careful!!!) \*/

try:

s = socket.socket( socket.AF\_PACKET , socket.SOCK\_RAW , socket.ntohs(0x0003))

except socket.error , msg:

print 'Socket could not be created. Error Code : ' + str(msg[0]) + ' Message ' + msg[1]

sys.exit()

x=input("Enter the number of packets you want: ")

count=tcp=icmp=udp=others=0

# receive a packet

while count<x:

packet = s.recvfrom(65565)

packet = packet[0] #packet string from tuple

#parse ethernet header

eth\_length = 14

eth\_header = packet[:eth\_length]

eth = unpack('!6s6sH' , eth\_header)

eth\_protocol = socket.ntohs(eth[2])

print 'Packet Number: ' + str(count)

count = count+1

print 'Destination MAC : ' + eth\_addr(packet[0:6]) + ' Source MAC : ' + eth\_addr(packet[6:12]) + ' Protocol : ' + str(eth\_protocol)

#Parse IP packets, IP Protocol number = 8

if eth\_protocol == 8 :

#Parse IP header

#take first 20 characters for the ip header

ip\_header = packet[eth\_length:20+eth\_length]

#now unpack them :)

iph = unpack('!BBHHHBBH4s4s' , ip\_header)

version\_ihl = iph[0]

version = version\_ihl >> 4

ihl = version\_ihl & 0xF

iph\_length = ihl \* 4

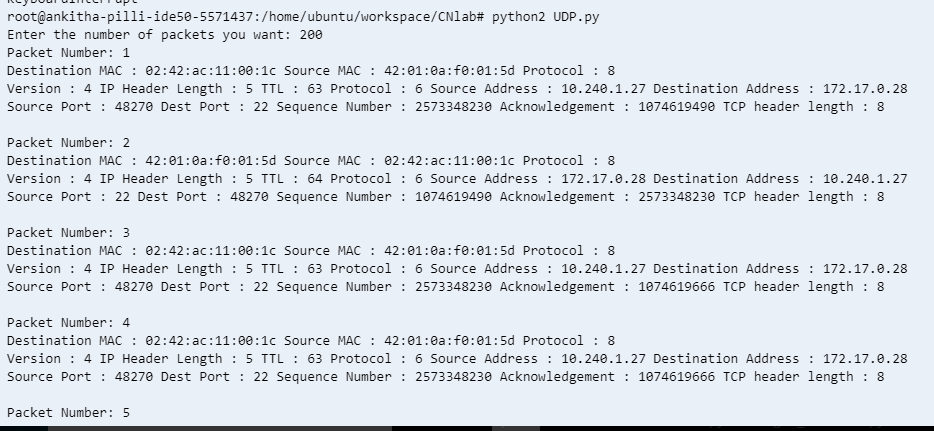
ttl = iph[5]

protocol = iph[6]

s\_addr = socket.inet\_ntoa(iph[8]);

d\_addr = socket.inet\_ntoa(iph[9]);

print 'Version : ' + str(version) + ' IP Header Length : ' + str(ihl) + ' TTL : ' + str(ttl) + ' Protocol : ' + str(protocol) + ' Source Address : ' + str(s\_addr) + ' Destination Address : ' + str(d\_addr)



#TCP protocol

if protocol == 6 :

t = iph\_length + eth\_length

tcp\_header = packet[t:t+20]

#now unpack them :)

tcph = unpack('!HHLLBBHHH' , tcp\_header)

source\_port = tcph[0]

dest\_port = tcph[1]

sequence = tcph[2]

acknowledgement = tcph[3]

doff\_reserved = tcph[4]

tcph\_length = doff\_reserved >> 4

print 'Source Port : ' + str(source\_port) + ' Dest Port : ' + str(dest\_port) + ' Sequence Number : ' + str(sequence) + ' Acknowledgement : ' + str(acknowledgement) + ' TCP header length : ' + str(tcph\_length)

tcp=tcp+1

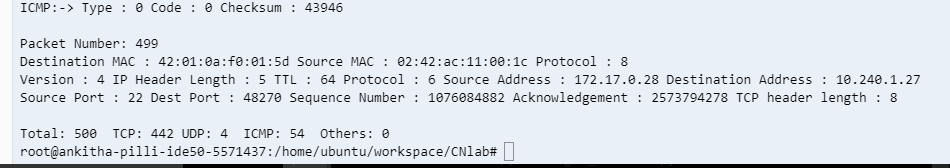
"""h\_size = eth\_length + iph\_length + tcph\_length \* 4

data\_size = len(packet) - h\_size

#get data from the packet

data = packet[h\_size:]

print 'Data : ' + data"""



#ICMP Packets

elif protocol == 1 :

u = iph\_length + eth\_length

icmph\_length = 4

icmp\_header = packet[u:u+4]

#now unpack them :)

icmph = unpack('!BBH' , icmp\_header)

icmp\_type = icmph[0]

code = icmph[1]

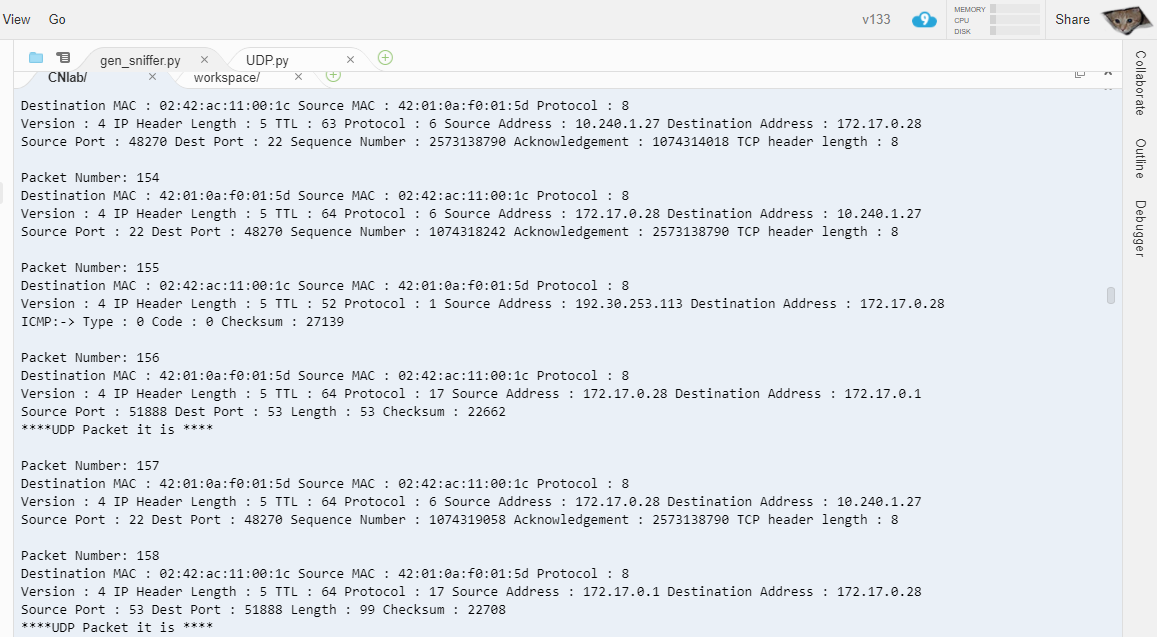
checksum = icmph[2]

print 'ICMP:-> Type : ' + str(icmp\_type) + ' Code : ' + str(code) + ' Checksum : ' + str(checksum)

icmp=icmp+1

"""h\_size = eth\_length + iph\_length + icmph\_length

data\_size = len(packet) - h\_size"""



#UDP packets

elif protocol == 17 :

u = iph\_length + eth\_length

udph\_length = 8

udp\_header = packet[u:u+8]

#now unpack them :)

udph = unpack('!HHHH' , udp\_header)

source\_port = udph[0]

dest\_port = udph[1]

length = udph[2]

checksum = udph[3]

print 'Source Port : ' + str(source\_port) + ' Dest Port : ' + str(dest\_port) + ' Length : ' + str(length) + ' Checksum : ' + str(checksum)

udp=udp+1

print '\*\*\*\*UDP Packet it is \*\*\*\*'

#some other IP packet like IGMP

else :

print 'Protocol other than TCP/UDP/ICMP'

others=others+1

print

print 'Total: '+str(count)+' TCP: '+str(tcp)+' UDP: '+str(udp)+ ' ICMP: '+str(icmp)+' Others: '+str(others)