Computer Security 353 -Professor Heckathorn

Final Project – Application Development

Packet Sniffer

Bennett Lawrenz

Moustapha Said

Joe Vanacore

Our application project was to create a packet sniffer that captures network traffic over a wi-fi connection and then parses the raw data from the packets into human readable format. Python was used as our development language. The program first extracts pertinent data from the packet. The information is then parsed into split into three different headers:

1. Ethernet Header
2. IP Header
3. TCP Header

<u>The Ethernet parser includes:</u>

- Destination MAC Address
- Source MAC Address
- Protocol #

<u>The IP parser includes:</u>

- Version #
- TOS
- Length of packet
- Identification #
- Fragment
- TTL
- Protocol
- Header CheckSum
- Source IP Address
- Destination IP Address

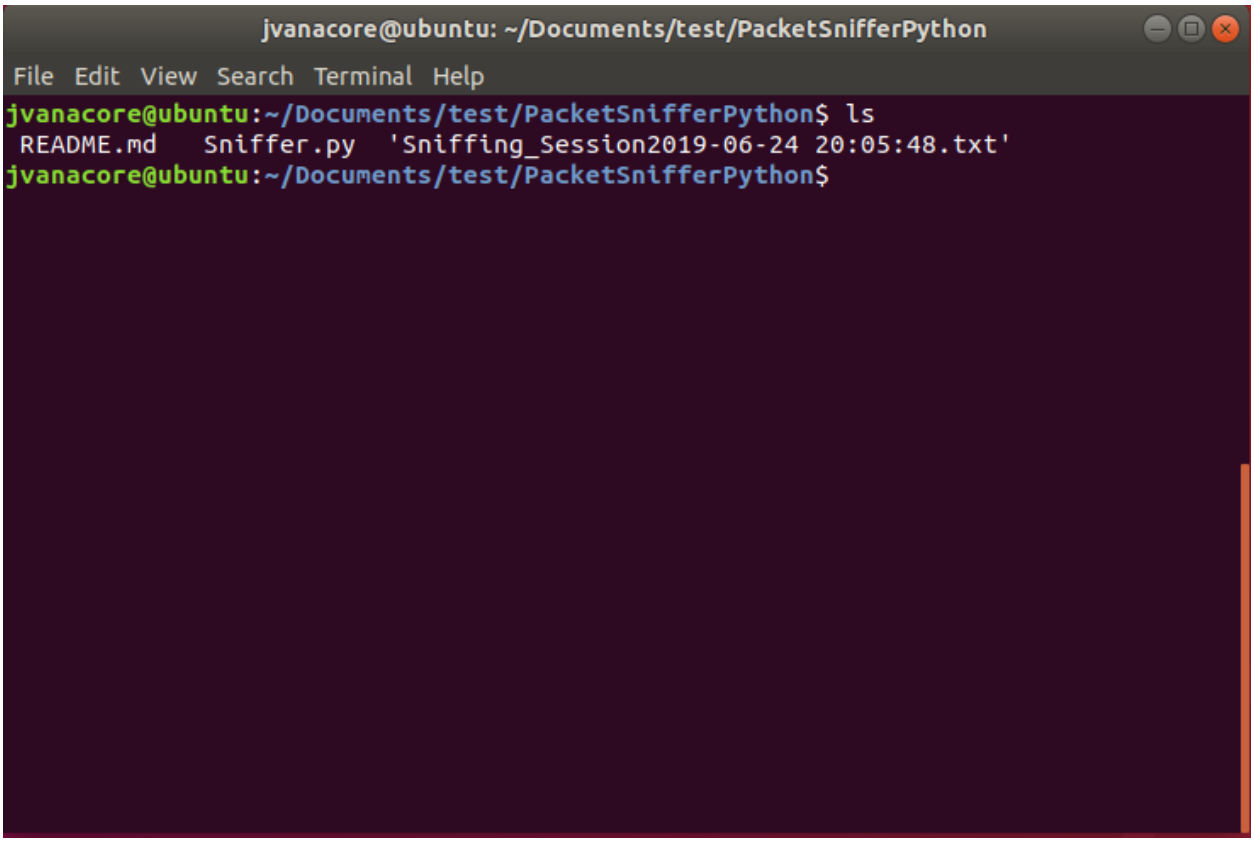
<u>The TCP parser includes:</u>

- Source port #
- Destination port #
- Sequence #
- Acknowledge #
- Offset and Reserved
- TCP Flag
- Window
- CheckSum

The program will then keep a log file of the packet sniffing session that is stored within the directory of the python file.

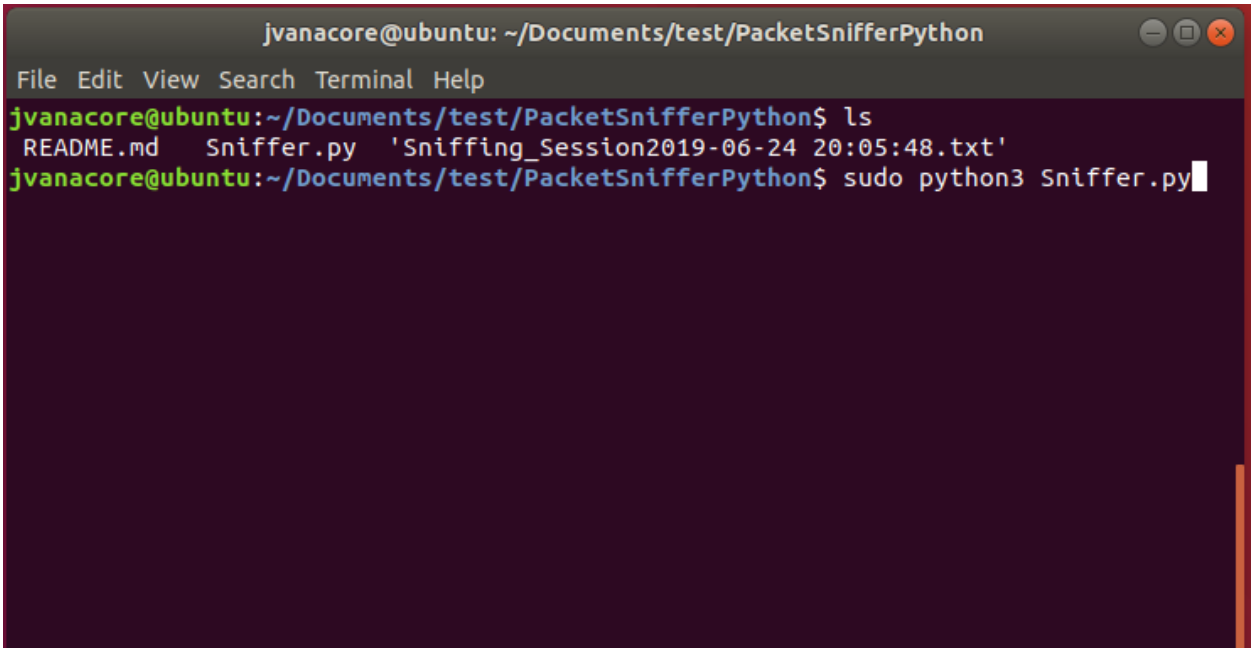
Execution

1. Navigate to the directory of the packet sniffer application.



2. Type in the following command to run the application:

   sudo python3 Sniffer.py



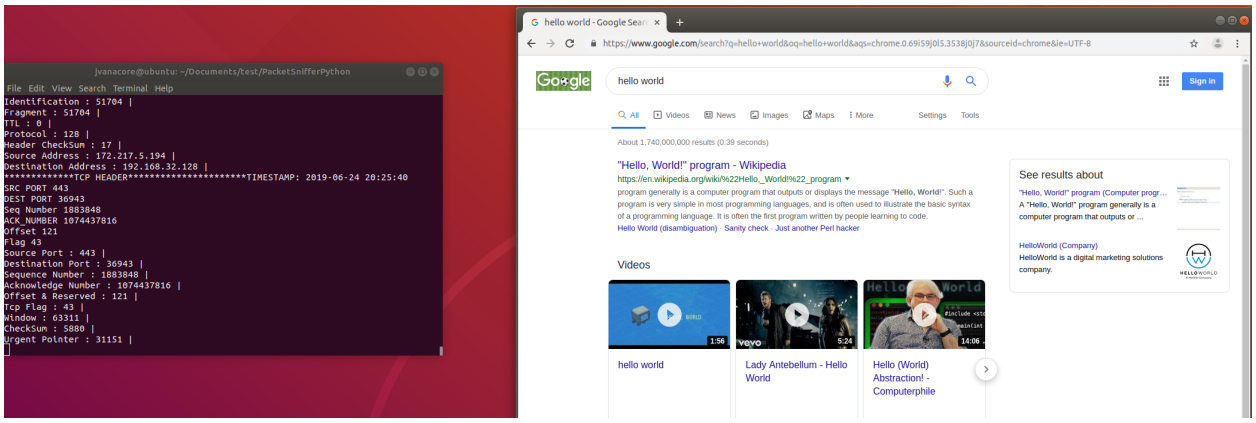
3. Verify that the application has started:

```
jvanacore@ubuntu:~/Documents/test/PacketSnifferPython$ ls
 README.md   Sniffer.py  'Sniffing_Session2019-06-24 20:05:48.txt'
jvanacore@ubuntu:~/Documents/test/PacketSnifferPython$ sudo python3 Sniffer.py
[sudo] password for jvanacore:
Starting Sniffing Session
2019-06-24 20:22:38
```

4. Verify the application will now start to passively parse incoming traffic.

```
jvanacore@ubuntu: ~/Documents/test/PacketSnifferPython
File  Edit  View  Search  Terminal  Help
Identification : 50673 |
Fragment : 50673 |
TTL : 0 |
Protocol : 128 |
Header CheckSum : 6 |
Source Address : 173.194.167.42 |
Destination Address : 192.168.32.128 |
*************TCP HEADER*********************TIMESTAMP: 2019-06-24 20:23:43
SRC PORT 80
DEST PORT 36980
Seq Number 52840098
ACK_NUMBER 308743058
Offset 80
Flag 16
Source Port : 80 |
Destination Port : 36980 |
Sequence Number : 52840098 |
Acknowledge Number : 308743058 |
Offset & Reserved : 80 |
Tcp Flag : 16 |
Window : 64240 |
CheckSum : 34376 |
Urgent Pointer : 0 |
```

5. Lets try to surf the web and see what kind of traffic we get, do a quick Google search.



6. The packet sniffer will being to parse a large amount of inbound and outbound traffic.

```
Dest_Mac_addr : b'\x00\x0c)@\x88\xb3' |
Src_Mac_addr : b'\x00PV\xe8\x9a\xad' |
Protocol : 2048 |
*************IP HEADER**********************TIMESTAMP: 2019-06-24 20:26:20
source_addr  216.58.193.196
dest_addr  192.168.32.128
sproto  128
Version : 69 |
Tos : 0 |
Total Length : 202 |
Identification : 51757 |
Fragment : 51757 |
TTL : 0 |
Protocol : 128 |
Header CheckSum : 17 |
Source Address : 216.58.193.196 |
Destination Address : 192.168.32.128 |
*************TCP HEADER**********************TIMESTAMP: 2019-06-24 20:26:20
SRC PORT 443
DEST PORT 49238
Seq Number 11959131
ACK_NUMBER 1074189922
Offset 174
Flag 104
Source Port : 443 |
Destination Port : 49238 |
Sequence Number : 11959131 |
Acknowledge Number : 1074189922 |
Offset & Reserved : 174 |
Tcp Flag : 104 |
Window : 391 |
CheckSum : 42901 |
Urgent Pointer : 48977 |
*************ETHERNAET HEADER**********************TIMESTAMP: 2019-06-24 20:26:20
Source Mac_addr:  b'\x00PV\xe8\x9a\xad'
ethernetT proto : 2048
Dest_Mac_addr : b'\x00\x0c)@\x88\xb3' |
Src_Mac_addr : b'\x00PV\xe8\x9a\xad' |
Protocol : 2048 |
*************IP HEADER**********************TIMESTAMP: 2019-06-24 20:26:20
source_addr  216.58.193.196
dest_addr  192.168.32.128
sproto  128
Version : 69 |
Tos : 0 |
Total Length : 44 |
Identification : 51758 |
Fragment : 51758 |
TTL : 0 |
Protocol : 128 |
Header CheckSum : 17 |
Source Address : 216.58.193.196 |
Destination Address : 192.168.32.128 |
*************TCP HEADER**********************TIMESTAMP: 2019-06-24 20:26:20
SRC PORT 443
DEST PORT 49238
Seq Number 1605209
ACK_NUMBER 1074241863
Offset 108
Flag 255
Source Port : 443 |
Destination Port : 49238 |
Sequence Number : 1605209 |
Acknowledge Number : 1074241863 |
Offset & Reserved : 108 |
Tcp Flag : 255 |
Window : 20548 |
CheckSum : 20527 |
Urgent Pointer : 49043 |
```

7. Finally, the program stores a log of the current packet sniffing session within the directory of the application along with the timestamp of every packet.