Student: Joaquin Saldana
Week 6 / Lab 2
CS373 – Defense Against the Dark Arts
Winter 2018

In this week's lab we were asked to examine network traffic found in 2 .csv files. In order to analyze the data in the .csv files, we were asked to write code in a Python or Perl script to help us dissect the data.

While doing an initial run of the scancsv.py Python script to the R.csv file (the smaller file), I found it provided me the following data:

```
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python scancsv.py R.csv
numPackets:99142 numBytes:71683046
  1:          7
  2:          2
  6:      39138
 17:      59995
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$
```

```
~/network_security_unit/Lab2/CSVPacket.py - Sublime Text 2 (UNREGISTERED)
File  Edit  Selection  Find  View  Goto  Tools  Project  Preferences  Help
scancsv.py   CSVPacket.py
        r = ['Num:%4u length:%5u ' % (self.packetNum, self.length)]
        if self.proto == 1:
            r.append("ICMP type:%3u code:%3u" % (self.icmptype,self.icmpcode))
        elif self.proto == 6:
            r.append('TCP: %s:%-5u => %s:%-5u flags:%3u' % (self.ipsrc,self.tcpsport,self.ipdst
        elif self.proto == 17:
```

In doing some research and with the aide for the linked site ([https://technet.microsoft.com/en-us/library/cc959827.aspx](https://technet.microsoft.com/en-us/library/cc959827.aspx) and [https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml](https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml) ), I found that protocol 1 means ICMP (Internet Control Message Protocol), 2 equals IGMP (Internet Group Management), 6 equals TCP (Transmission Control Protocol) and 17 equals UDP (User Datagram Protocol).

Clearly from the data above the majority of the traffic captured is TCP and UDP, also the more commonly used network protocols.

I ran the same script against the O.csv file, since this file is much larger, and the following results were returned:

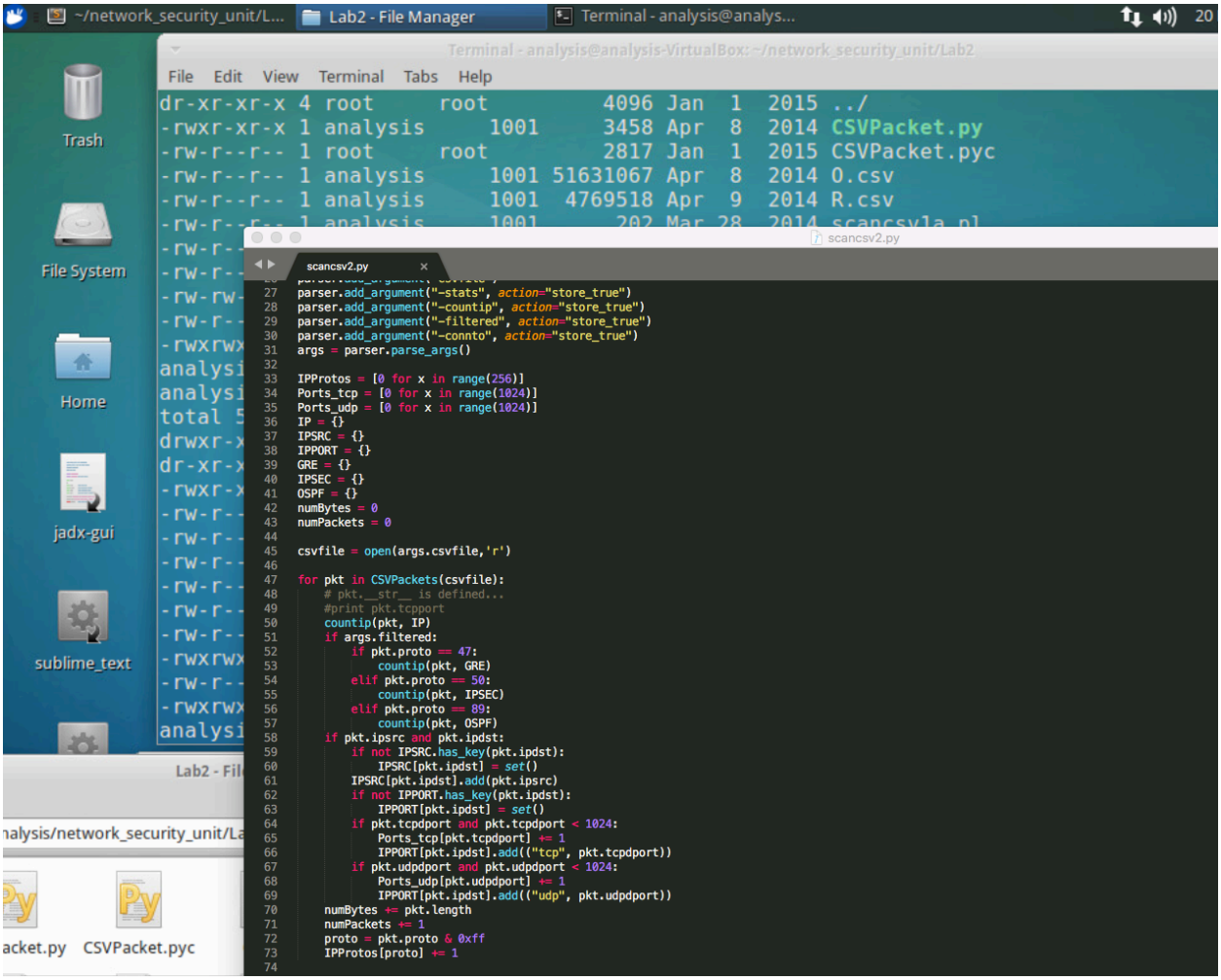
```
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$ python scancsv.py O.csv
numPackets:999914 numBytes:366325065
  1:      6794
  6:    950654
 17:     38332
 47:      2626
 50:      1484
 89:        24
analysis@analysis-VirtualBox:~/network_security_unit/Lab2$
```

```
~/network_security_unit/Lab2/CSVPacket.py - Sublime Text 2 (UNREGISTERED)
File  Edit  Selection  Find  View  Goto  Tools  Project  Preferences  Help
scancsv.py   CSVPacket.py
55          r = ['Num:%4u length:%5u ' % (self.packetNum, self.length)]
56          if self.proto == 1:
57              r.append("ICMP type:%3u code:%3u" % (self.icmptype,self.icmpcode))
58          elif self.proto == 6:
59              r.append('TCP: %s:%-5u => %s:%-5u flags:%3u' % (self.ipsrc,self.tcpsport,self.ipdst
60          elif self.proto == 17:
```

The meta data in the O.csv included protocols now found in the R.csv file. The protocols in particular were:

- 47 which equals GRE (Generic Routing Encapsulation)
- 50 which equals ESP (Encap Security Payload)
- 89 which means OSPFIGP which stands for Open Shortest Path First Interior Gateway Protocol which is a type of protocol used for exchanging routing information between routers within an autonomous system.

Afterwards I started to write my script with instructions as stated in the lab for commands such as -stats, -countip, -filtered and more




In my tests I found that the top 5 ports were Netbios sessions, HTTP, POP3, SSH, and DNS for the R.csv file. In the O.csv file I found that SMTP, HTTP, and DNS.

Also, in the R.csv there several private IP addresses as both the source and destination (addresses starting with 10.*). This suggests this is logs for a large network of internal machines exchanging information.

Also in the O.csv file, the largest set of connections were made to addresses starting at IP address 192.245 with TCP connections at ports 25, 135, and 22.