Nolan Flatt

IFT 383

Lab 1

Question 1

```
nflatt@generall:~/ift383/lab1$ cat firewall.log | head
#Version 1.5
#Software: Microsoft Windows Firewall
#Time Format: local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size

2018-05-25 11:47:02 FORWARD TCP 11.100.6.64 10.202.41.103 2176 7 953880
2018-02-22 03:34:00 FORWARD UDP 11.102.7.64 10.202.40.101 2075 65 116445
2018-03-20 04:47:11 REJECT UDP 9.102.8.65 10.202.41.101 2189 97 985631
2018-11-08 14:14:47 REJECT TCP 10.101.8.64 10.202.40.103 2158 63 164259
2018-07-24 22:46:54 REJECT TCP 11.100.6.65 10.202.41.103 2089 61 991882
nflatt@generall:~/ift383/lab1$ wc -l firewall.log
100006 firewall.log
nflatt@generall:~/ift383/lab1$ sed -i '1,10d' firewall.log
nflatt@generall:~/ift383/lab1$ wc -l firewall.log
99996 firewall.log
nflatt@generall:~/ift383/lab1$ cat firewall.log | head
2018-01-01 19:27:19 DROP TCP 11.101.7.64 10.202.40.100 2210 44 354300
2018-04-17 01:35:12 FORWARD UDP 10.102.6.65 10.202.41.103 2135 83 231775
2018-05-05 04:26:05 DROP UDP 11.101.6.65 10.202.40.103 2160 104 209447
2018-08-20 15:43:16 DROP TCP 10.102.6.64 10.202.41.100 2212 113 960460
2018-02-10 02:28:02 FORWARD UDP 11.101.6.65 10.202.41.102 2089 68 117449
2018-03-22 00:05:32 DROP TCP 9.101.8.65 10.202.41.101 2129 92 435203
2018-04-24 19:32:47 REJECT TCP 9.100.8.65 10.202.40.103 2115 93 682002
2018-05-19 01:43:06 FORWARD TCP 10.100.7.64 10.202.41.100 2107 29 70746
2018-04-13 03:51:33 DROP TCP 9.102.8.64 10.202.40.103 2219 32 984581
2018-08-16 21:02:36 FORWARD UDP 11.100.8.65 10.202.40.102 2190 17 965652
```

Question 2

Commands used:

awk '{print $5}' firewallq2.log

sort firewallq2v1.log > firewallq2v1sort.log

Nano firewallq2v1sort.log (Counted 54 different values)

grep -e '10.100.6.64' firewallq2v1sort.log; grep -e '10.100.6.65' firewallq2v1sort.log; grep -e '10.100.7.64' firewallq2v1sort.log; grep -e '10.100.7.65' firewallq2v1sort.log; grep -e '10.100.8.64' firewallq2v1sort.log; grep -e '10.100.8.65' firewallq2v1sort.log; grep -e '10.101.6.64' firewallq2v1sort.log; grep -e '10.101.6.64' firewallq2v1sort.log; grep -e '10.101.7.64' firewallq2v1sort.log; grep -e '10.101.7.65' firewallq2v1sort.log; grep -e '10.101.8.64' firewallq2v1sort.log; grep -e '10.101.8.65' firewallq2v1sort.log; grep -e '10.102.6.64' firewallq2v1sort.log; grep -e '10.102.6.65' firewallq2v1sort.log; grep -e '10.102.7.64' firewallq2v1sort.log; grep -e '10.102.7.65' firewallq2v1sort.log; grep -e '10.102.8.64' firewallq2v1sort.log; grep -e '10.102.8.65' firewallq2v1sort.log; grep -e '11.100.6.64' firewallq2v1sort.log; grep -e '11.100.6.65' firewallq2v1sort.log; grep -e '11.100.7.64' firewallq2v1sort.log; grep -e '11.100.7.65' firewallq2v1sort.log; grep -e '11.100.8.64' firewallq2v1sort.log; grep -e '11.100.8.65' firewallq2v1sort.log; grep -e '11.101.6.64' firewallq2v1sort.log; grep -e '11.101.6.65' firewallq2v1sort.log; grep -e '11.101.7.64' firewallq2v1sort.log; grep -e '11.101.7.65' firewallq2v1sort.log;

grep -e '11.101.8.64' firewallq2v1sort.log; grep -e '11.101.8.65' firewallq2v1sort.log; grep -e '11.102.6.64' firewallq2v1sort.log; grep -e '11.102.6.65' firewallq2v1sort.log; grep -e '11.102.7.64' firewallq2v1sort.log; grep -e '11.102.7.65' firewallq2v1sort.log; grep -e '11.102.8.64' firewallq2v1sort.log; grep -e '11.102.8.65' firewallq2v1sort.log; grep -e '9.100.6.64' firewallq2v1sort.log; grep -e '9.100.6.65' firewallq2v1sort.log; grep -e '9.100.7.64' firewallq2v1sort.log; grep -e '9.100.7.65' firewallq2v1sort.log; grep -e '9.100.8.64' firewallq2v1sort.log; grep -e '9.100.8.65' firewallq2v1sort.log; grep -e '9.101.6.64' firewallq2v1sort.log; grep -e '9.101.6.65' firewallq2v1sort.log; grep -e '9.101.7.64' firewallq2v1sort.log; grep -e '9.101.7.65' firewallq2v1sort.log; grep -e '9.101.8.64' firewallq2v1sort.log; grep -e '9.101.8.65' firewallq2v1sort.log; grep -e '9.102.6.64' firewallq2v1sort.log; grep -e '9.102.6.65' firewallq2v1sort.log; grep -e '9.102.7.64' firewallq2v1sort.log; grep -e '9.102.7.65' firewallq2v1sort.log; grep -e '9.102.8.64' firewallq2v1sort.log; grep -e '9.102.8.65' firewallq2v1sort.log

Output (video link):

There are 54 unique values.

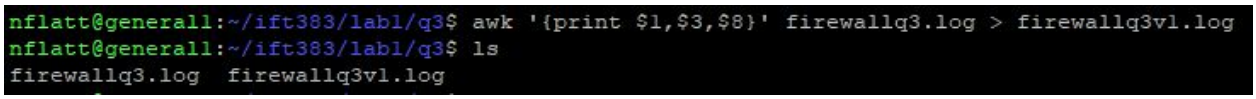
I included a video link since the output would be too long to include in this document.

IFT 383 Lab 1 Question 2 grep commands and result

Question 3

The commands used and the results are below.

First, I counted the occurrences of 2018-08-01 to 2018-08-31 for both ports 80 and 443 with an action field of accept. Second, I counted the occurrences of 2017-07-04 for both ports 80 and 443 with an action field of accept. I will include a table below of the occurrences of each.



```
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-01 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-02 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-03 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-04 ACCEPT 80' firewallq3v1.log
2
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-05 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-06 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-07 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-08 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-09 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-10 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-11 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-12 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-13 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-14 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-15 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-16 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-17 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-18 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-19 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-20 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-21 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-22 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-23 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-24 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-25 ACCEPT 80' firewallq3v1.log
0
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-26 ACCEPT 80' firewallq3v1.log
1
nflatt@generall:~/ift383/lab1/q3$ grep -c '2018-08-27 ACCEPT 80' firewallq3v1.log
1
```

```
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-28 ACCEPT 80' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-29 ACCEPT 80' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-30 ACCEPT 80' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-31 ACCEPT 80' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-01 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-02 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-03 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-04 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-05 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-06 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-07 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-08 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-09 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-10 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-11 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-12 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-13 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-14 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-15 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-16 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-17 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-18 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-19 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-20 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-21 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-22 ACCEPT 443' firewallq3vl.log
1
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-23 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-24 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-25 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-26 ACCEPT 443' firewallq3vl.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-27 ACCEPT 443' firewallq3vl.log
0
```

```
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-28 ACCEPT 443' firewallq3v1.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-29 ACCEPT 443' firewallq3v1.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-30 ACCEPT 443' firewallq3v1.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-08-31 ACCEPT 443' firewallq3v1.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-07-04 ACCEPT 443' firewallq3v1.log
0
nflatt@generall:~/ift383/labl/q3$ grep -c '2018-07-04 ACCEPT 80' firewallq3v1.log
0
```

Total number of occurrences based on given filters

Question 4

```
nflatt@generall:~/ift383/labl/q4$ awk '{print $2,$3,$4,$8}' firewallq4.log > firewallq4v1.log
nflatt@generall:~/ift383/labl/q4$ ls
firewallq4.log  firewallq4v1.log
```

```
nflatt@generall:~/ift383/labl/q4$ grep -c 'DROP TCP 22' firewallq4v1.log
235
```

```
nflatt@generall:~/ift383/labl/q4$ grep -c '00* DROP TCP 22' firewallq4v1.log
26
nflatt@generall:~/ift383/labl/q4$ grep -c '01* DROP TCP 22' firewallq4v1.log
30
nflatt@generall:~/ift383/labl/q4$ grep -c '02* DROP TCP 22' firewallq4v1.log
30
nflatt@generall:~/ift383/labl/q4$ grep -c '03:00:00 DROP TCP 22' firewallq4v1.log
0
```

There are a total of 86 events that occurred from 00:00:00 to 03:00:00 with the filters dst-port 22, drop action and TCP protocol.

Question 5

```
nflatt@generall:~/ift383/labl/q5$ grep -E "\<((500)|[0-4]{3})$" ./firewallnew.log | grep -E '(10.202.40)'
2018-05-18 09:34:47 DROP UDP 11.101.6.64 10.202.40.103 2164 124 421
2018-01-18 14:42:45 ACCEPT TCP 9.100.6.65 10.202.40.101 2125 51 140
2018-06-24 13:32:57 FORWARD UDP 10.100.8.65 10.202.40.103 2095 78 312
2018-06-22 17:52:58 FORWARD TCP 9.101.6.64 10.202.40.102 2050 54 221
2018-10-18 01:24:01 DROP UDP 11.101.6.65 10.202.40.100 2062 8 441
```

Question 6 (parts 1 and 2)

```
nflatt@generall:~/ift383/labl/q6pt1$ awk '{print $1, $2}' firewallq6pt1.log > test.log
nflatt@generall:~/ift383/labl/q6pt1$ sort test.log | head


2018-01-01 00:00:23
2018-01-01 00:02:07
2018-01-01 00:12:42
2018-01-01 00:22:27
2018-01-01 00:25:53
2018-01-01 00:31:13
2018-01-01 00:31:49
2018-01-01 00:35:33
nflatt@generall:~/ift383/labl/q6pt1$ sort test.log | tail
2018-11-27 22:39:53
2018-11-27 22:45:51
2018-11-27 22:46:39
2018-11-27 22:46:40
2018-11-27 22:52:28
2018-11-27 22:53:56
#Fields: date
#Software: Microsoft
#Time Format:
#Version 1.5
nflatt@generall:~/ift383/labl/q6pt1$ grep -e "2018-01-01 00:00" test.log
2018-01-01 00:00:23
nflatt@generall:~/ift383/labl/q6pt1$ grep -e "2018-11-27 22:53" test.log
2018-11-27 22:53:56
```

Part 1: 2018-01-01 00:00:23

Part 2: 2018-11-27 22:53:56