Lab 7 Assignment AWK

Kruthi M S

241059049

Timestamp,Src_IP,Dest_IP,Protocol,Source_Port,Destination_Port,Packet_Size,Status

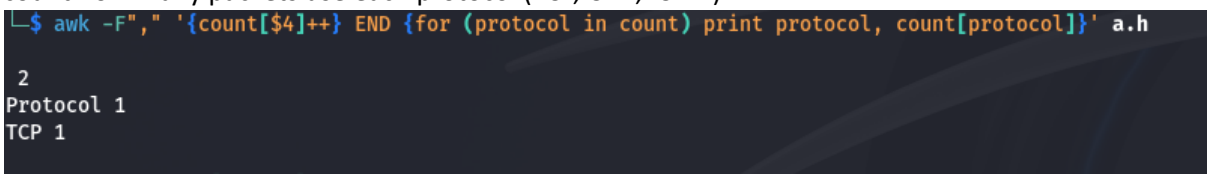
2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30 10:15:12,192.168.1.15,203.0.113.5,UDP,53,55432,512,Dropped 2024-09-30 10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30 10:15:16,172.16.0.5,192.168.1.15,ICMP,64,Dropped 2024-09-30 10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30 10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30 10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped

Src IP – Source Ip

Dest Ip – Destination Ip

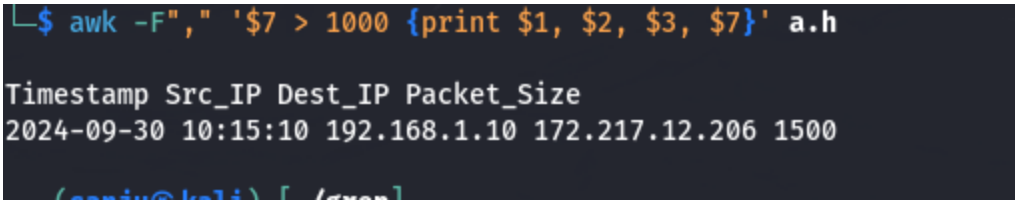
Write a awk script to

1. count how many packets use each protocol (TCP, UDP, ICMP)



2. filter and print only the dropped packets.

3. print the Timestamp, Source_IP, Destination_IP, and Packet_Size for packets that have a size greater than 1000 bytes.



4. display traffic that is directed to destination port 443.

```
└─$ awk -F"," '!seen[$2]++ {print $2}' k.h

Src_IP

192.168.1.10
192.168.1.15
10.0.0.2
172.16.0.5
198.51.100.23
203.0.113.5
```

5. print all unique Source_IP addresses from the network_traffic.csv file.

```
└─$ awk -F"," '!seen[$2]++ {print $2}' k.h

Src_IP

192.168.1.10
192.168.1.15
10.0.0.2
172.16.0.5
198.51.100.23
203.0.113.5
```

6. filter only TCP traffic and calculate the average packet size.

```
└─$ awk -F"," '$4 == "TCP" {total+=$7; count++} END {if (count > 0) print "Average Packet Size:", total/count}' k.h

Average Packet Size: 1455
```

7. Count invalid records

```
└─$ awk -F"," 'NF != 8 {invalid++} END {print "Invalid Records:", invalid+0}' k.h

Invalid Records: 4
```

8. extract and print all rows where the Source_IP is in the 192.168.x.x range.

```
└─$ awk -F"," '$2 ~ /^192\.168\./ {print}' k.h

2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30
10:15:12,192.168.1.15,203.0.113.5,UDP,53,55432,512,Dropped 2024-09-30
10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30
```

9. match traffic directed to either port 80 (HTTP) or port 443 (HTTPS).

```
└─$ awk -F"," '$6 !~ /[a-zA-Z]/ {print}' k.h


2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30
10:15:12,192.168.1.15,203.0.113.5,UDP,53,55432,512,Dropped 2024-09-30
10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30
10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30
10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30
10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped
Src IP - Source Ip
Dest Ip - Destination Ip
```

10. filter out rows where the Destination_Port contains any alphanumeric characters (letters or numbers).

```
└─$ awk -F"," '$6 !~ /[a-zA-Z]/ {print}' k.h


2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30
10:15:12,192.168.1.15,203.0.113.5,UDP,53,55432,512,Dropped 2024-09-30
10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30
10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30
10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30
10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped
Src IP - Source Ip
Dest Ip - Destination Ip
```

11. filter out traffic where the protocol is TCP AND the destination port is 443 (HTTPS traffic).

```
└─$ awk -F"," '!($4 == "TCP" && $6 == 443) {print}' k.h

Timestamp,Src_IP,Dest_IP,Protocol,Source_Port,Destination_Port,Packet_Size,Status

2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30
10:15:12,192.168.1.15,203.0.113.5,UDP,53,55432,512,Dropped 2024-09-30
10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30
10:15:16,172.16.0.5,192.168.1.15,ICMP,64,Dropped 2024-09-30
10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30
10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30
10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped
Src IP - Source Ip
Dest Ip - Destination Ip
```

12. filter out and print traffic where the Packet_Size is greater than 1000 OR the Status is Dropped.

```
└─$ awk -F"," '$7 > 1000 || $8 == "Dropped" {print}' k.h

Timestamp,Src_IP,Dest_IP,Protocol,Source_Port,Destination_Port,Packet_Size,Status
2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30
10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30
10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30
10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30
10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped
```

13. print traffic NOT originating from 192.168.x.x IP addresses.

```
└─$ awk -F"," '$2 !~ /^192\.168\./ {print}' k.h

Timestamp,Src_IP,Dest_IP,Protocol,Source_Port,Destination_Port,Packet_Size,Status

10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30
10:15:16,172.16.0.5,192.168.1.15,ICMP,64,Dropped 2024-09-30
10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30
10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped
Src IP – Source Ip
Dest Ip – Destination Ip
```

14. filter rows where both Source_IP and Destination_IP are within the 192.168.x.x range.

```
└─$ awk -F"," '!($6 == 22 || $7 < 100) {print}' k.h

Timestamp,Src_IP,Dest_IP,Protocol,Source_Port,Destination_Port,Packet_Size,Status
2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30
10:15:12,192.168.1.15,203.0.113.5,UDP,53,55432,512,Dropped 2024-09-30
10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30
10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30
10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30
10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped
```

15. filter out traffic where the destination port is 22 OR the packet size is less than 100 bytes.

```
└─$ awk -F"," '!($6 == 22 || $7 < 100) {print}' k.h

Timestamp,Src_IP,Dest_IP,Protocol,Source_Port,Destination_Port,Packet_Size,Status
2024-09-30 10:15:10,192.168.1.10,172.217.12.206,TCP,443,51413,1500,Accepted 2024-09-30
10:15:12,192.168.1.15,203.0.113.5,UDP,53,55432,512,Dropped 2024-09-30
10:15:14,10.0.0.2,192.168.1.10,TCP,80,61324,1420,Accepted 2024-09-30
10:15:18,192.168.1.10,198.51.100.23,TCP,443,1025,1500,Accepted 2024-09-30
10:15:20,198.51.100.23,192.168.1.10,TCP,443,1025,1400,Accepted 2024-09-30
10:15:22,203.0.113.5,192.168.1.15,UDP,123,49152,512,Dropped
```