Nadeesha Liyanage – nadeeshadin637@gmail.com

Sample Input in command line

Fields: Date | Time | Action | Protocol | Src IP | Dst IP | Src Port | Dst Port | Size | TCP Flags | Info

2023-03-15 06:25:31 ALLOW TCP 192.168.1.105 93.184.216.34 44345 80 52 S - Client Hello

2023-03-15 06:26:45 BLOCK UDP 192.168.1.105 192.168.1.255 138 138 229 - - Local Broadcast

2023-03-15 06:27:02 ALLOW TCP 192.168.1.105 198.51.100.23 44346 443 60 S - Client Hello

2023-03-15 06:27:58 BLOCK TCP 192.168.1.105 203.0.113.5 44347 22 48 S - SSH Attempt

2023-03-15 06:28:16 ALLOW ICMP 192.168.1.105 8.8.8.8 - - 84 - - Echo request

2023-03-15 06:29:10 ALLOW UDP 192.168.1.105 8.8.4.4 53 53 72 - - DNS request

2023-03-15 06:30:05 BLOCK TCP 192.168.1.106 198.51.100.24 44348 80 52 S - Client Hello

2023-03-15 06:30:42 ALLOW TCP 192.168.1.107 192.168.1.200 44349 445 52 S - Internal Traffic

2023-03-15 06:31:19 BLOCK TCP 192.168.1.108 203.0.113.10 44350 1433 40 S - SQL Server Access Attempt

2023-03-15 06:32:00 ALLOW TCP 192.168.1.109 192.168.1.210 44351 22 60 S - Internal SSH Access

2023-03-15 06:33:45 BLOCK ICMP 192.168.1.110 10.10.10.10 - - 84 - - Destination Unreachable

2023-03-15 06:34:31 ALLOW TCP 192.168.1.111 192.168.1.220 44352 3306 52 S - Internal MySQL Access

2023-03-15 06:35:27 BLOCK UDP 192.168.1.112 192.168.1.230 44353 161 60 - - SNMP Access Attempt

End of log

Nadeesha Liyanage – nadeeshadin637@gmail.com

Output

Parsed Log Data Frame

```
     Date/Time Action Protocol     Source IP  Destination IP Source Port Destination Port Size flag                        Info
0   2023-03-15 06:25:31  ALLOW    TCP  192.168.1.105   93.184.216.34       44345              80   52    S              Client Hello
1   2023-03-15 06:26:45  BLOCK    UDP  192.168.1.105  192.168.1.255         138             138  229    -           Local Broadcast
2   2023-03-15 06:27:02  ALLOW    TCP  192.168.1.105   198.51.100.23       44346             443   60    S              Client Hello
3   2023-03-15 06:27:58  BLOCK    TCP  192.168.1.105    203.0.113.5        44347              22   48    S               SSH Attempt
4   2023-03-15 06:28:16  ALLOW   ICMP  192.168.1.105        8.8.8.8           -               -   84    -              Echo request
5   2023-03-15 06:29:10  ALLOW    UDP  192.168.1.105        8.8.4.4          53              53   72    -               DNS request
6   2023-03-15 06:30:05  BLOCK    TCP  192.168.1.106   198.51.100.24       44348              80   52    S              Client Hello
7   2023-03-15 06:30:42  ALLOW    TCP  192.168.1.107  192.168.1.200       44349             445   52    S           Internal Traffic
8   2023-03-15 06:31:19  BLOCK    TCP  192.168.1.108    203.0.113.10       44350            1433   40    S  SQL Server Access Attempt
9   2023-03-15 06:32:00  ALLOW    TCP  192.168.1.109  192.168.1.210       44351              22   60    S         Internal SSH Access
10  2023-03-15 06:33:45  BLOCK   ICMP  192.168.1.110    10.10.10.10           -               -   84    -     Destination Unreachable
11  2023-03-15 06:34:31  ALLOW    TCP  192.168.1.111  192.168.1.220       44352            3306   52    S       Internal MySQL Access
12  2023-03-15 06:35:27  BLOCK    UDP  192.168.1.112  192.168.1.230       44353             161   60    -        SNMP Access Attempt
```

Statistics

```
Statistics:
Total Number of Entries in the Log: 13

Action Statistics:
   Count   count
0  ALLOW      7
1  BLOCK      6

Protocol Distribution:
   Count   count
0   TCP       8
1   UDP       3
2  ICMP       2

Top Source IP Addresses:
          Count   count
0  192.168.1.105      6
1  192.168.1.106      1
2  192.168.1.107      1
3  192.168.1.108      1
4  192.168.1.109      1

Top Destination IP Addresses:
           Count   count
0   93.184.216.34      1
1   192.168.1.255      1
2   198.51.100.23      1
3     203.0.113.5      1
4         8.8.8.8      1

Top Blocked Ports:
   Count   count
0    138       1
1     22       1
2     80       1
3   1433       1
4      -       1
```

```
Top Blocked Ports:
   Count   count
0    138        1
1     22        1
2     80        1
3   1433        1
4      -        1

Top Allowed Ports:
   Count   count
0     80        1
1    443        1
2      -        1
3     53        1
4    445        1

Destination IP and Action Statistics:
Destination IP Action  Count
    10.10.10.10  BLOCK      1
 192.168.1.200  ALLOW      1
 192.168.1.210  ALLOW      1
 192.168.1.220  ALLOW      1
 192.168.1.230  BLOCK      1
 192.168.1.255  BLOCK      1
 198.51.100.23  ALLOW      1
 198.51.100.24  BLOCK      1
  203.0.113.10  BLOCK      1
   203.0.113.5  BLOCK      1
       8.8.4.4  ALLOW      1
       8.8.8.8  ALLOW      1
 93.184.216.34  ALLOW      1
```