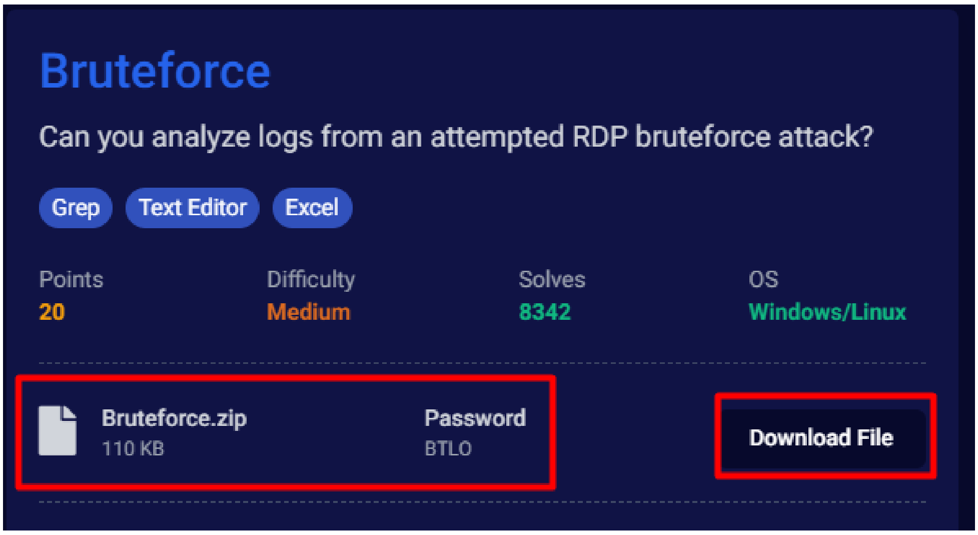
Challenge URL: https://blueteamlabs.online/home/challenge/bruteforce-16629bf9a2



Bruteforce

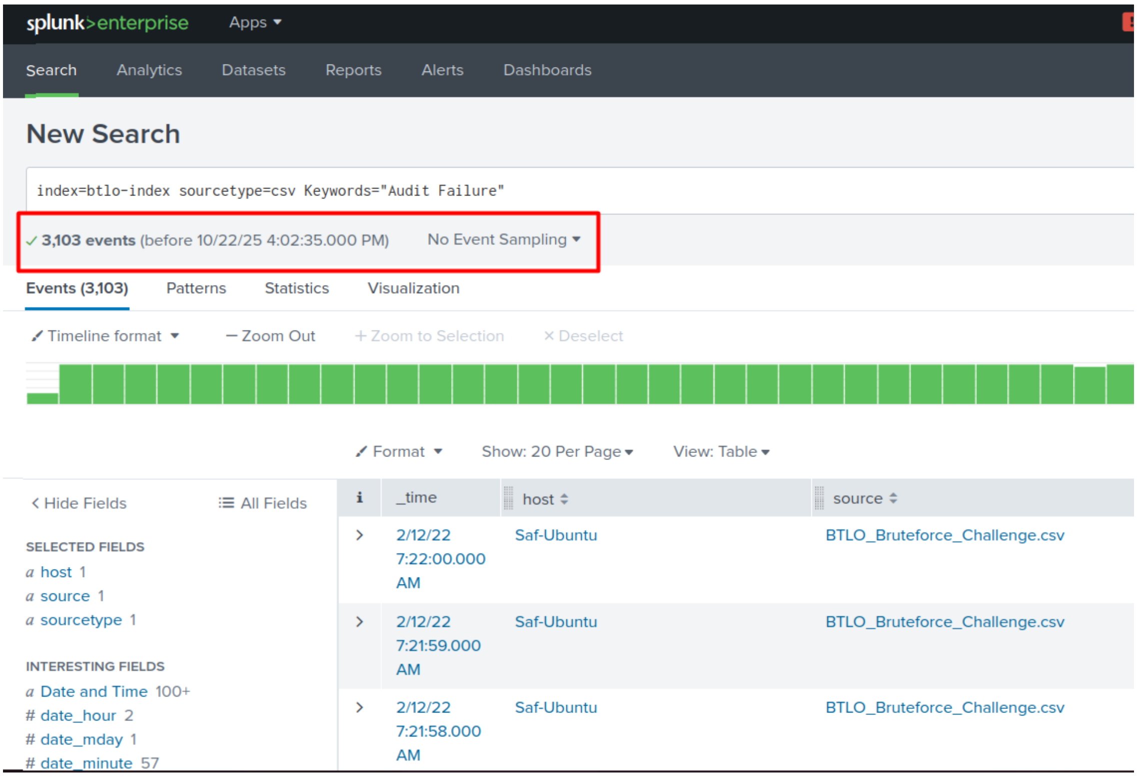
Can you analyze logs from an attempted RDP bruteforce attack?

Points	Difficulty	Solves	OS
20	Medium	8342	Windows/Linux

Bruteforce.zip 110 KB — Password BTLO

Download the zip file to analyze the log file.

Question 1) How many Audit Failure events are there? (Format: Count of Events)



New Search

```
index=btlo-index sourcetype=csv Keywords="Audit Failure"
```

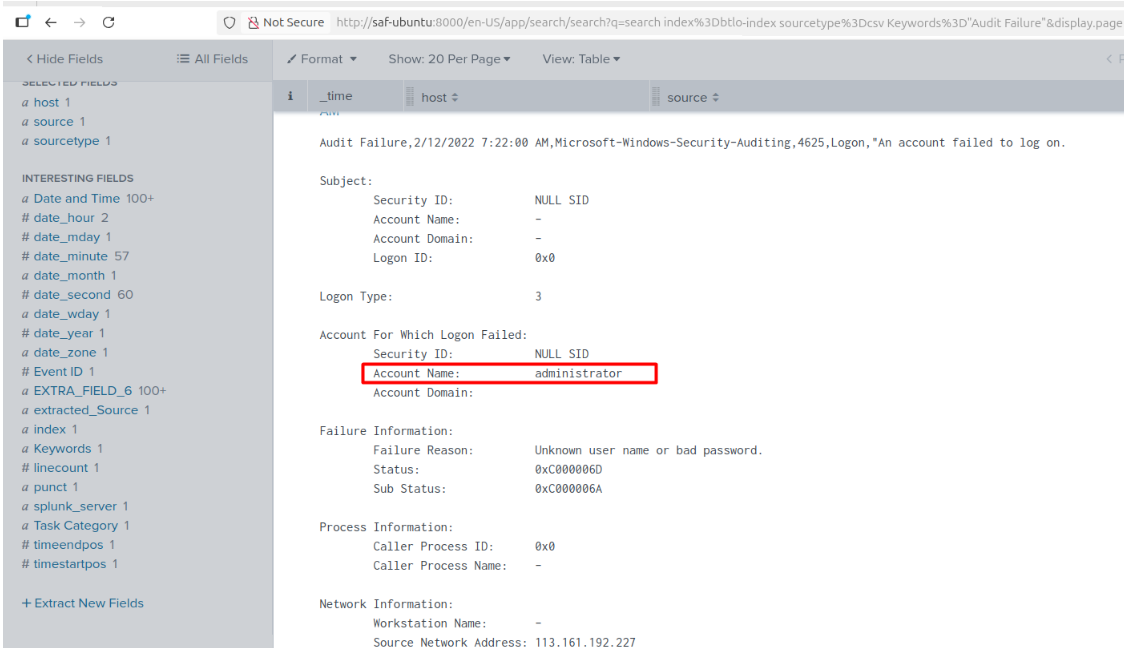
✓ 3,103 events (before 10/22/25 4:02:35.000 PM) No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a Date and Time 100+
- # date_hour 2
- # date_mday 1
- # date_minute 57

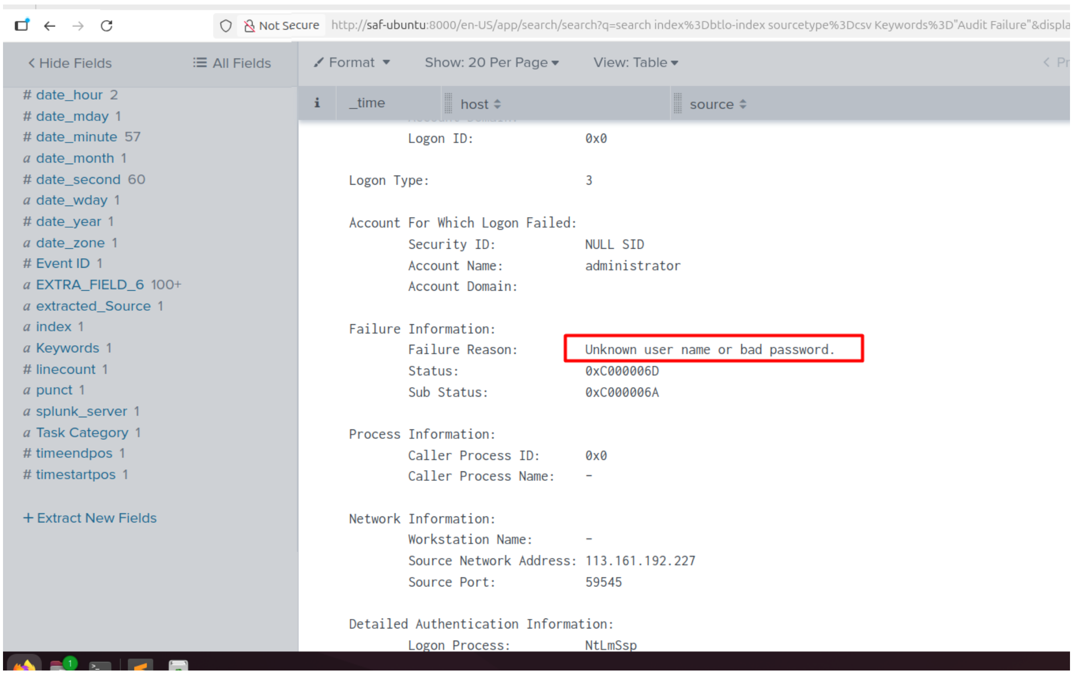
i	_time	host	source
>	2/12/22 7:22:00.000 AM	Saf-Ubuntu	BTLO_Bruteforce_Challenge.csv
>	2/12/22 7:21:59.000 AM	Saf-Ubuntu	BTLO_Bruteforce_Challenge.csv
>	2/12/22 7:21:58.000 AM	Saf-Ubuntu	BTLO_Bruteforce_Challenge.csv

Question 2) What is the username of the local account that is being targeted? (Format: Username)



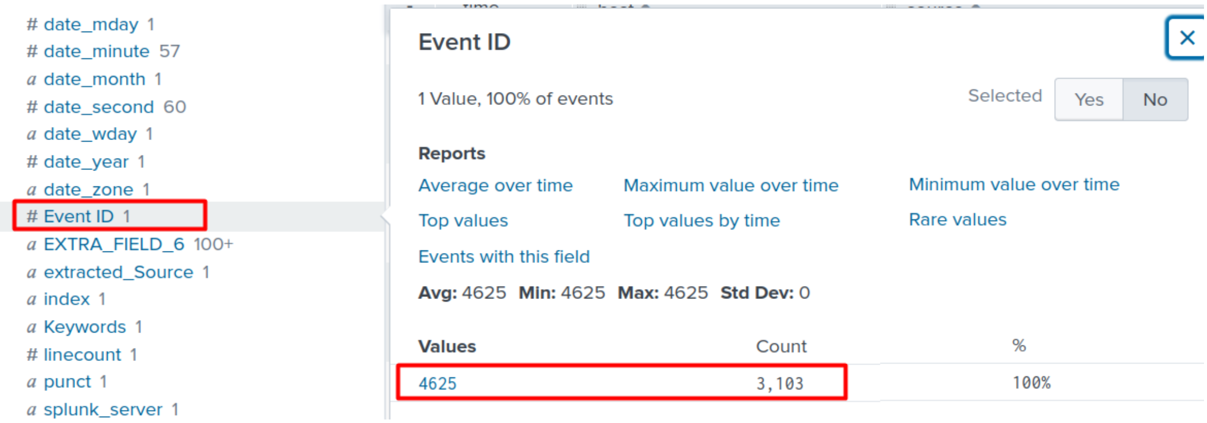
```
Audit Failure,2/12/2022 7:22:00 AM,Microsoft-Windows-Security-Auditing,4625,Logon,"An account failed to log on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           administrator
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       -
        Source Network Address: 113.161.192.227
```

Question 3) What is the failure reason related to the Audit Failure logs? (Format: String)



```
        Logon ID:               0x0

Logon Type:                     3

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           administrator
        Account Domain:

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC000006A

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       -
        Source Network Address: 113.161.192.227
        Source Port:            59545

Detailed Authentication Information:
        Logon Process:          NtLmSsp
```

Question 4) What is the Windows Event ID associated with these logon failures? (Format: ID)



#	date_mday	1
#	date_minute	57
a	date_month	1
#	date_second	60
a	date_wday	1
#	date_year	1
a	date_zone	1
#	Event ID	1
a	EXTRA_FIELD_6	100+
a	extracted_Source	1
a	index	1
a	Keywords	1
#	linecount	1
a	punct	1
a	splunk_server	1

Event ID

1 Value, 100% of events

Selected Yes No

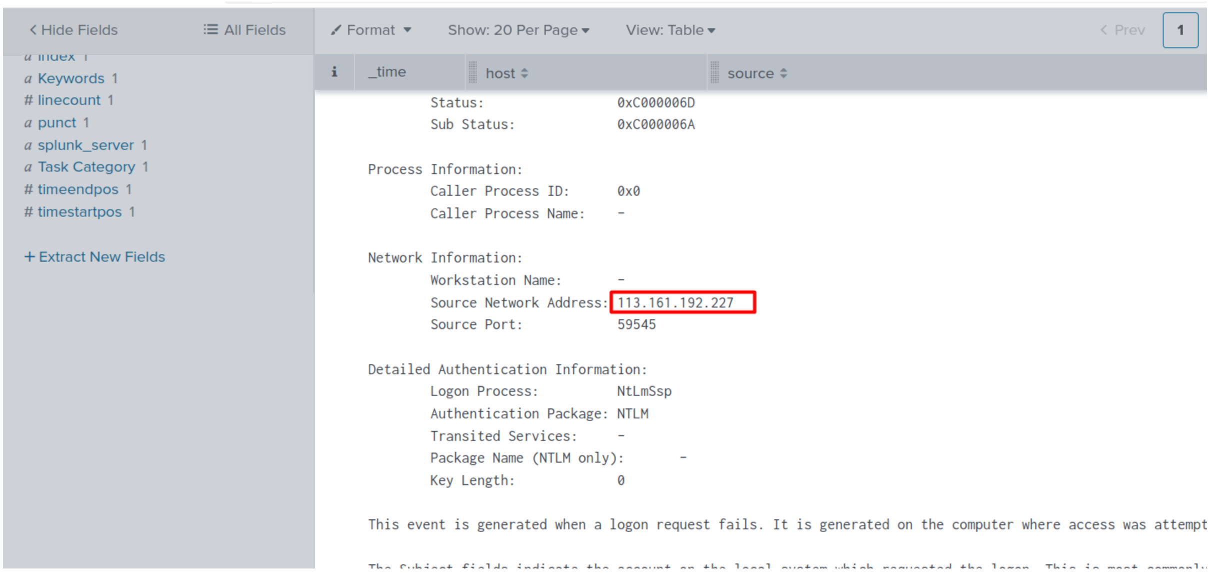
Reports

Average over time Maximum value over time Minimum value over time
Top values Top values by time Rare values
Events with this field

Avg: 4625 **Min:** 4625 **Max:** 4625 **Std Dev:** 0

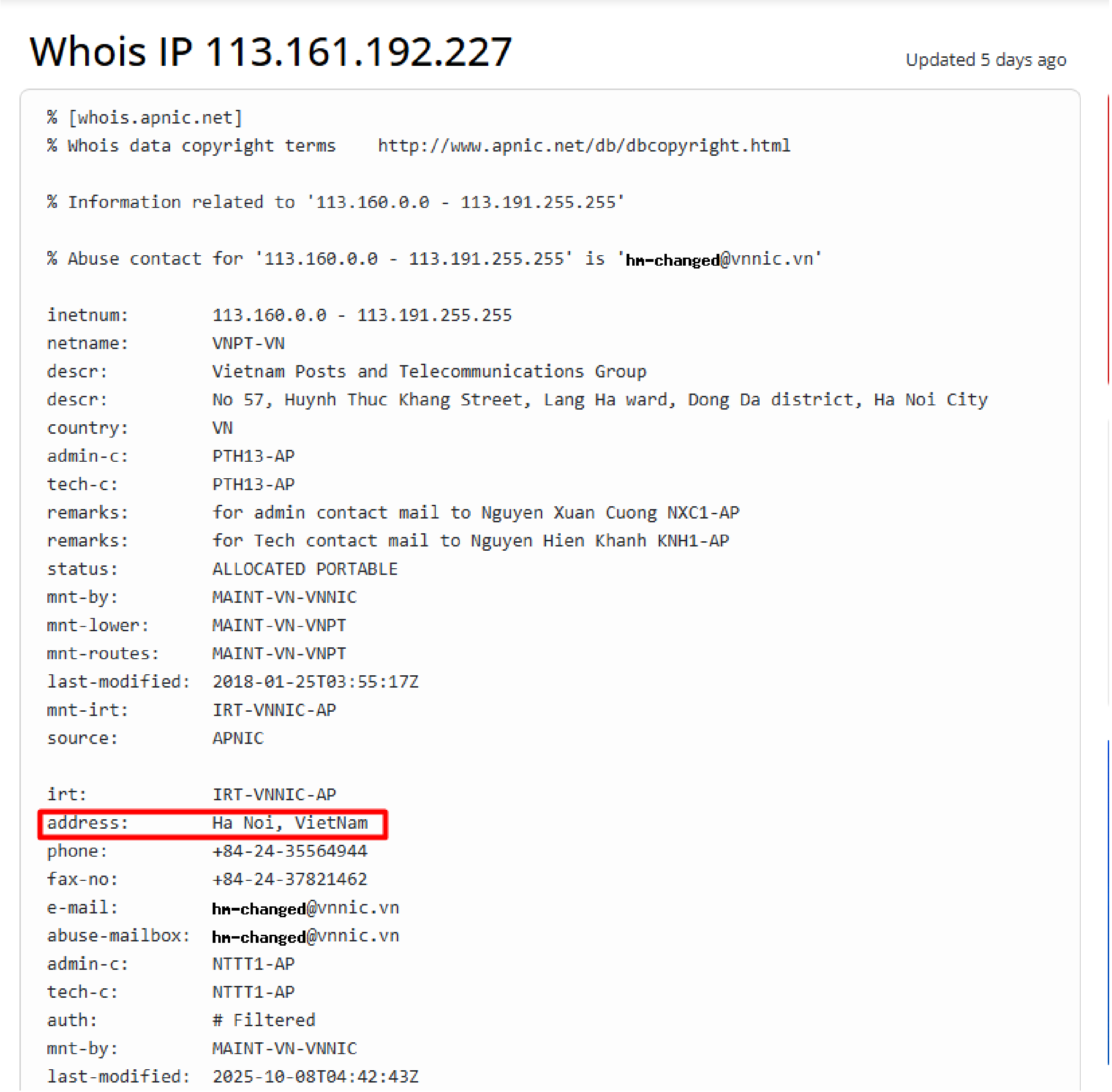
Values	Count	%
4625	3,103	100%

Question 5) What is the source IP conducting this attack? (Format: X.X.X.X)



```
          Status:                 0xC000006D
          Sub Status:             0xC000006A

Process Information:
          Caller Process ID:      0x0
          Caller Process Name:    -

Network Information:
          Workstation Name:       -
          Source Network Address: 113.161.192.227
          Source Port:            59545

Detailed Authentication Information:
          Logon Process:          NtLmSsp
          Authentication Package: NTLM
          Transited Services:     -
          Package Name (NTLM only):       -
          Key Length:             0

This event is generated when a logon request fails. It is generated on the computer where access was attempt

The Subject fields indicate the account on the local system which requested the logon. This is most commonly
```

Question 6) What country is this IP address associated with? (Format: Country)

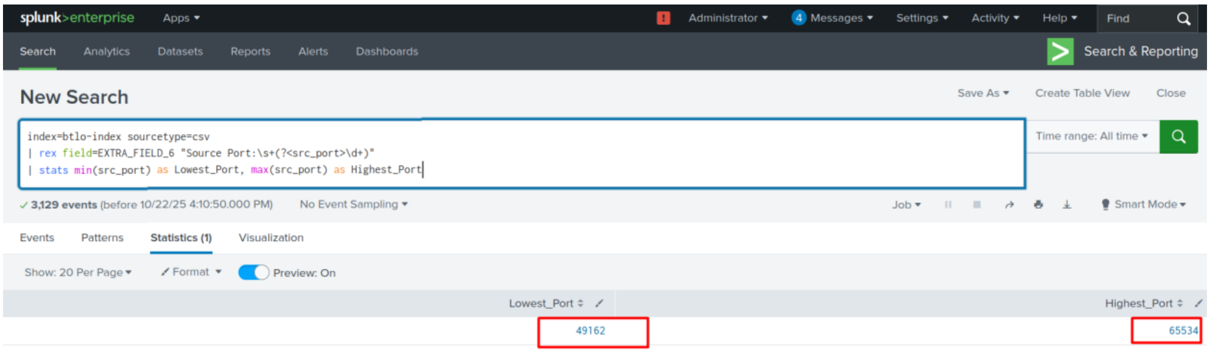


Whois IP 113.161.192.227

Updated 5 days ago

```
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '113.160.0.0 - 113.191.255.255'

% Abuse contact for '113.160.0.0 - 113.191.255.255' is 'hm-changed@vnnic.vn'

inetnum:        113.160.0.0 - 113.191.255.255
netname:        VNPT-VN
descr:          Vietnam Posts and Telecommunications Group
descr:          No 57, Huynh Thuc Khang Street, Lang Ha ward, Dong Da district, Ha Noi City
country:        VN
admin-c:        PTH13-AP
tech-c:         PTH13-AP
remarks:        for admin contact mail to Nguyen Xuan Cuong NXC1-AP
remarks:        for Tech contact mail to Nguyen Hien Khanh KNH1-AP
status:         ALLOCATED PORTABLE
mnt-by:         MAINT-VN-VNNIC
mnt-lower:      MAINT-VN-VNPT
mnt-routes:     MAINT-VN-VNPT
last-modified:  2018-01-25T03:55:17Z
mnt-irt:        IRT-VNNIC-AP
source:         APNIC

irt:            IRT-VNNIC-AP
address:        Ha Noi, VietNam
phone:          +84-24-35564944
fax-no:         +84-24-37821462
e-mail:         hm-changed@vnnic.vn
abuse-mailbox:  hm-changed@vnnic.vn
admin-c:        NTTT1-AP
tech-c:         NTTT1-AP
auth:           # Filtered
mnt-by:         MAINT-VN-VNNIC
last-modified:  2025-10-08T04:42:43Z
```

What is the range of source ports that were used by the attacker to make these login requests? (LowestPort-HighestPort - Ex: 100-541)



New Search

```
index=btlo-index sourcetype=csv
| rex field=EXTRA_FIELD_6 "Source Port:\s+(?<src_port>\d+)"
| stats min(src_port) as Lowest_Port, max(src_port) as Highest_Port
```

✓ 3,129 events (before 10/22/25 4:10:50.000 PM) No Event Sampling

Lowest_Port	Highest_Port
49162	65534

To see the lowest and highest port

```
index=btlo-index sourcetype=csv
| rex field=EXTRA_FIELD_6 "Source Port:\s+(?<src_port>\d+)"
| stats min(src_port) as Lowest_Port, max(src_port) as Highest_Port
```

To see all the ports with event

```
index=btlo-index sourcetype=csv
| rex field=EXTRA_FIELD_6 "Source Port:\s+(?<src_port>\d+)"
| table _time src_port host source
```

Country Extraction and visualization

```
index=btlo-index sourcetype=csv
| rex field=EXTRA_FIELD_6 "Source Network
Address:\s+(?<src_ip>\d{1,3}(?:\.\d{1,3}){3})"
| iplocation src_ip
| stats count by Country
| sort -count
```

With Username and success failure

```
index=btlo-index sourcetype=csv
| eval Status=if(match(EXTRA_FIELD_6, "An account failed to log on"),
"Failure", "Success")
| rex field=EXTRA_FIELD_6 "Account Name:\s+(?<username>\S+)"
| stats count by Status, username
| sort - count
```